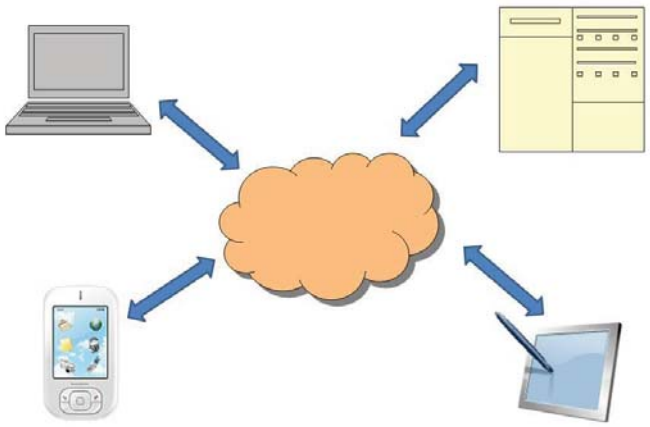
ADVANCED COPYRIGHT ISSUES ON THE INTERNET



David L. Hayes, Esq.[*]
FENWICK & WEST LLP

[*] Chairman of Intellectual Property Practice Group, Fenwick & West LLP, Mountain View & San Francisco, California. B.S.E.E. (Summa Cum Laude), Rice University (1978); M.S.E.E., Stanford University (1980); J.D. (Cum Laude), Harvard Law School (1984). An earlier version of this paper appeared in David L. Hayes, "Advanced Copyright Issues on the Internet," 7 Tex. Intell. Prop. L.J. 1 (Fall 1998). The author expresses appreciation to Matthew Becker for significant contributions to Section III.E ("Streaming and Downloading").

© 1997-2013 David L. Hayes. All Rights Reserved.
(Updated as of March 2013)

TABLE OF CONTENTS

I. INTRODUCTION 13

II. RIGHTS IMPLICATED BY TRANSMISSION AND USE OF WORKS ON THE INTERNET 14

A. The Right of Reproduction 14

1. The Ubiquitous Nature of "Copies" on the Internet 15
2. Whether Images of Data Stored in RAM Qualify as "Copies" 15
3. The WIPO Treaties & the European Copyright Directive Are Unclear With Respect to Interim "Copies" 22
   (a) Introduction to the WIPO Treaties & the European Copyright Directive 22
   (b) The WIPO Copyright Treaty 24
   (c) The WIPO Performances and Phonograms Treaty 27
4. The Requirement of Volition for Direct Liability 29
   (a) The Netcom Case 30
   (b) The MAPHIA Case 32
   (c) The Sabella Case 33
   (d) The Frena Case 34
   (e) The Webbworld Case 35
   (f) The Sanfilippo Case 36
   (g) The Free Republic Case 37
   (h) The MP3.com Cases 39
   (i) The CoStar Case 42
   (j) The Ellison Case 43
   (k) Perfect 10 v. Cybernet Ventures 43
   (l) Field v. Google 44
   (m) Parker v. Google 45
   (n) The Cablevision Case 45
   (o) Arista Records v. Usenet.com 48
   (p) Quantum Systems v. Sprint Nextel 49
   (q) Disney Enterprises v. Hotfile 50
   (r) Perfect 10 v. Megaupload 51
   (s) Wolk v. Kodak Imaging Network 52
   (t) Fox Broadcasting v. Dish Network 52
   (u) Summary of Case Law 56
5. The Reproduction Right Under WIPO Implementing Legislation 57
   (a) United States Legislation 57
      (1) The Digital Millennium Copyright Act 57
      (2) Legislation Not Adopted 57
   (b) The European Copyright Directive 59
6. Peer-to-Peer File Sharing 64
   (a) BMG Music v. Gonzalez 64

(b) Columbia Pictures v. Bunnell 65
(c) Sony BMG Music Entertainment v. Tenenbaum 65
(d) Capitol Records v. Thomas-Rasset 70
7. The Immunity of the Audio Home Recording Act (AHRA) 73
(a) The Napster Cases 73
(b) The Aimster Case 74
(c) Atlantic Recording Corp. v. XM Satellite Radio 74
B. The Right of Public Performance 77
1. Isochronous Versus Asynchronous Transmissions 78
2. The Meaning of "Publicly" 79
3. Live Nation Motor Sports v. Davis 79
4. United States v. ASCAP 80
5. The Cablevision Case 82
6. Ringtones – In re Application of Cellco Partnership 83
7. Warner Bros. v. WTV Systems 85
8. Capitol Records v. MP3tunes 88
9. The Aereo Case 88
C. The Right of Public Display 93
1. The Frena, Marobie-FL, Hardenburgh and Webbworld Cases 93
2. Kelly v. Arriba Soft 95
3. Ticketmaster v. Tickets.com 98
4. Perfect 10 v. Google (aka Perfect 10 v. Amazon) 99
5. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey 111
6. ICG-Internet Commerce Group, Inc. v. Wolf 112
D. The Right of Public Distribution 112
1. The Requirement of a "Copy" 112
(a) Cases Addressing Whether Mere Posting Is a Distribution 113
(1) Cases Holding That Mere Posting Is a Distribution 114
(2) Cases Holding That Mere Posting Is Not a Distribution 118
(3) Cases Refusing To Decide the Issue 127
2. The Requirement of a "Public" Distribution 127
3. The Requirement of a Rental or Transfer of Ownership 128
4. The Right of Distribution Under the WIPO Treaties 128
5. The Right of Distribution Under WIPO Implementing Legislation 129
(a) United States Legislation 129
(b) The European Copyright Directive 130
E. The Right of Importation 130
F. The New Right of Transmission and Access Under the WIPO Treaties 131
1. The Right of Communication to the Public in the WIPO Copyright Treaty 131
2. The Right of Making Available to the Public in the WIPO Performances and Phonograms Treaty 133
3. The Right of Transmission and Access Under WIPO Implementing Legislation 135

(a) United States Legislation 135
(b) The European Copyright Directive 135
G. New Rights and Provisions Under The Digital Millennium Copyright Act, the European Copyright Directive & Legislation That Did Not Pass 138
1. Circumvention of Technological Measures and Rights Management Information Under the DMCA 138
(a) Circumvention of Technological Protection Measures 139
(1) Prohibition on Conduct 139
(i) Exemptions Adopted by the Librarian of Congress 140
a. Scope of the Network Connection Exemption – The TracFone Cases 146
(ii) Epic Games v. Altmeyer 149
(iii) Facebook v. Power Ventures 149
(iv) Bose v. Zavala 150
(v) MGE UPS Systems v. GE 150
(vi) Granger v. One Call Lender Services 151
(2) Prohibition on Devices 151
(i) Sony Computer Entertainment America v. Gamemasters 152
(ii) The DirecTV Cases 153
a. DirecTV, Inc. v. Borow 153
b. DirecTV, Inc. v. Carrillo 153
(iii) Sony Computer Entertainment America v. Divineo 153
(iv) Ticketmaster L.L.C. v. RMG Technologies, Inc. 155
(v) The Tracfone Cases 155
(vi) Movida Communications, Inc. v. Haifa 156
(vii) Microsoft Corp. v. EEE Business Inc. 156
(viii) MDY Industries v. Blizzard Entertainment 156
(ix) Coupons, Inc. v. Stottlemire 161
(x) CoxCom, Inc. v. Chafee 162
(xi) The DISH Network Cases 163
a. Dish Network v. Sonicview 163
b. Dish Network v. SatFTA 163
c. Dish Network v. Dimarco 164
d. Dish Network v. Sonicview 165
e. Dish Network v. Alejandri 166
(xii) Realnetworks v. DVD Copy Control Association. 166
(xiii) Apple v. Psystar 168
(xiv) Blizzard Entertainment v. Reeves 171
(xv) The Craigslist Cases 171
a. Craigslist v. Naturemarket 171
b. Craigslist v. Mesiab 172
c. Craigslist v. Hubert 173
d. Craigslist v. Branley 173
e. Craigslist v. Kerbel 173
(xvi) Echostar v. Viewtech 174

(xvii) Adobe Systems v. Feather 174
(3) What Constitutes an Effective Technological Measure 175
(i) Auto Inspection Services v. Flint Auto Auction 175
(ii) Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey 175
(iii) Apple v. Psystar 178
(4) No Requirements With Respect to Design of a Product 178
(5) Other Rights Not Affected 178
(6) Exemption for Nonprofit Organizations and Law Enforcement 179
(7) Reverse Engineering for Interoperability 180
(i) Universal City Studios Inc. v. Reimerdes 185
(ii) Storage Technology Corporation v. Custom Hardware Engineering & Consulting 186
(iii) Chamberlain Group, Inc. v. Skylink Technologies, Inc. 186
(iv) Lexmark International, Inc. v. Static Control Components, Inc. 187
(v) Davidson Assocs. v. Internet Gateway 187
(vi) Sony Computer Entertainment America v. Divineo 191
(8) Encryption Research 191
(9) Protection of Minors 192
(10) Protection of Personally Identifying Information 192
(11) Security Testing 192
(12) Copy Restrictions To Be Built Into VCRs and Camcorders 192
(13) Other Cases Filed Under the Anti-Circumvention Provisions 193
(i) Sony Computer Entertainment, Inc. v. Connectix, Inc. 193
(ii) RealNetworks, Inc. v. Streambox Inc. 194
(iii) Universal City Studios, Inc. v. Reimerdes 198
(iv) A Related DVD Case Involving Trade Secret Claims – DVD Copy Control Association, Inc. v. McLaughlin (the Bunner case) 203
(v) A Related DVD Case – Norwegian Prosecution of Jon Johansen 207
(vi) Another Challenge to the DMCA – The Felten Case. 207
(vii) Pearl Investments, LLC v. Standard I/O, Inc. 208
(viii) 321 Studios v. Metro Goldwyn Mayer Studios, Inc. 209
(ix) I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc. 210
(x) Paramount Pictures Corp. v. 321 Studios. 211
(xi) Macrovision Corp. v. 321 Studios 211
(xii) Comcast of Illinois X v. Hightech Electronics, Inc. 211
(xiii) Davidson & Assocs. v. Internet Gateway 212
(xiv) Agfa Monotype Corp. v. Adobe Sys. 212
(xv) Egilman v. Keller & Heckman 215
(xvi) Macrovision v. Sima Products Corp. 215
(xvii) Nordstrom Consulting, Inc. v. M&S Technologies, Inc. 216

(xviii) R.C. Olmstead v. CU Interface 217
(xix) Avaya v. Telecom Labs 217
(xx) Actuate v. IBM 218
(xxi) Navistar v. New Baltimore Garage 219
(xxii) Dice Corp. v. Bold Technologies 219
(14) Criminal Prosecutions Under the DMCA 220
(i) The Sklyarov/Elcomsoft Case 220
(ii) Other Criminal Prosecutions Under the DMCA 221
(15) Other Uses of the Anti-Circumvention Provisions as a Sword 222
(i) Lexmark International, Inc. v. Static Control Components, Inc. 222
(ii) Chamberlain Group, Inc. v. Skylink Technologies, Inc. 228
(iii) In re Certain Universal Transmitters for Garage Door Openers 234
(iv) Storage Technology Corporation v. Custom Hardware Engineering & Consulting 235
(b) Integrity of Copyright Management Information 240
(1) Definition of CMI 240
(i) Cases Requiring CMI to be Part of a Technological System or Process 240
a. The IQ Group, Ltd. v. Wiesner Publishing, LLC 240
b. Textile Secrets Int'l, Inc. v. Ya-Ya Brand Inc. 243
c. Jacobsen v. Katzer 244
d. Silver v. Lavadeira 245
(ii) Cases Not Requiring CMI to be Part of a Technological System or Process 245
a. McClatchey v. The Associated Press 245
b. Associated Press v. All Headline News Corp. 246
c. Fox v. Hildebrand 246
d. Faulkner Press v. Class Notes 247
e. Agence France Presse v. Morel 247
f. Murphy v. Millennium Radio 248
g. William Wade Waller Co. v. Nexstar Broadcasting 249
(2) Prohibitions on False CMI and Removal/Alteration of CMI 250
(i) Cases re Removal or Alteration of CMI 250
a. Kelly v. Arriba Soft Corp. 250
b. Thron v. Harper Collins Publishers 251
c. Gordon v. Nextel Communications 252
d. Monotype Imaging, Inc. v. Bitstream Inc. 253
e. Keogh v. Big Lots Corp. 255
f. Goldman v. Healthcare Management Systems 255
g. Thomas M Gilbert Architects v. Accent Builders 255
h. Banxcorp v. Costco 256
i. Agence France Presse v. Morel 256
j. Scholz Design v. Custom Homes 257

k. Personal Keepsakes v. PersonalizationMall.com 257
(ii) Cases re False CMI 258
a. Schiffer Publishing, Ltd. v. Chronicle Books, LLC 258
b. Agence France Presse v. Morel 259
c. Personal Keepsakes v. PersonalizationMall.com 260
(3) Exceptions and Limitations 260
(c) Remedies for Violations of Sections 1201 and 1202 260
(1) Statutory Damages and Disgorgement of Profits 261
(i) Sony Computer Entertainment America v. Filipiak 261
(ii) Sony Computer Entertainment v. Divineo 262
(iii) McClatchey v. The Associated Press 262
(iv) Goldman v. Healthcare Management Systems 263
(v) Stockwire Research Group v. Lebed 263
(vi) MDY Industries, LLC v. Blizzard Entertainment, Inc. 264
(vii) Stockart.com v. Engle 264
(viii) Nexon America v. Kumar 265
(ix) Point 4 Data Corp. v. Tri-State Surgical Supply 265
(x) Granger v. One Call Lender Services 269
(xi) Pacific Stock v. Macarthur & Co. 269
(2) Jurisdictional Issues – Blueport Co. v. United States 270
(d) Alternative Approaches to the DMCA That Did Not Pass 270
(e) The Battle Between Content Owners and Technology Companies Over Built-In Technological Measures 271
2. Anticircumvention Provisions Under the European Copyright Directive 271
3. Anti-Circumvention Provisions in Other Foreign Countries 275
4. Fair Use 276
(a) United States Legislation That Did Not Pass 276
(b) The European Copyright Directive 276
5. Expansion of Library/Archives Exemptions 277
6. Distance Education 277
7. Copying in the Course of Computer Maintenance or Repair 278
8. Other Provisions of the DMCA 279
(a) Evaluation of Impact of Copyright Law on Electronic Commerce 279
(b) Clarification of the Authority of the Copyright Office 279
(c) Ephemeral Recordings 280
(d) Statutory Licenses With Respect to Performances of Sound Recordings 281
(e) Assumption of Contractual Obligations Related to Transfers of Rights in Motion Pictures 281
(f) Protection of Certain Industrial Designs 281
(1) Protection of Designs Embodied in Useful Articles 282
(2) Originality 282
(3) Exclusions from Protection 283
(4) Adaptations of Unprotectable Elements 283
(5) Duration of Protection and Design Notice 284

(6) Rights of a Design Owner and Limitations 284
(7) Standard of Infringement 284
(8) Benefit of Foreign Filing Date 285
(9) Vesting and Transfer of Ownership 285
(10) Remedies of Injunctive Relief, Damages, Attorneys' Fees and Destruction 285
(11) Private Rights of Action Against Pirated Designs 286
(12) Relation to Design Patents and Retroactive Effect 286
(g) Limitation of Liability of Online Service Providers 286
(h) Subpoenas to Service Providers 286
(1) Jurisdictional Issues 287
(2) RIAA v. Verizon Internet Services 287
(3) The Charter Communications Litigation 290
(4) Fatwallet v. Best Buy 291
(5) In re Subpoena to University of North Carolina at Chapel Hill 292
(6) Subpoenas in John Doe Actions 292
(7) Interscope Records v. Does 1-7 293
(8) In re Maximized Living 293
9. Proposed Limitation of Scope of Shrinkwrap and Clickwrap Licenses That Did Not Pass 293

III. APPLICATION OF COPYRIGHT RIGHTS TO SPECIFIC ACTS ON THE INTERNET 295

A. Browsing 295

B. Caching 297

1. Types of Caching 297
2. The Detriments of Caching 298
3. The Netcom Case and Application of the Fair Use Doctrine 300
(a) Purpose and Character of the Use 300
(b) Nature of the Copyrighted Work 301
(c) Amount and Substantiality of the Portion Used 301
(d) Effect of Use on the Potential Market 302
4. Cases Adjudicating Caching Under the Fair Use and Implied License Doctrines 304
(a) Field v. Google 304
(b) Perfect 10 v. Google (aka Perfect 10 v. Amazon) 307
(c) Ticketmaster L.L.C. v. RMG Technologies, Inc. 308
(d) Parker v. Yahoo!, Inc. 309
5. Other Caching Cases 310
(a) Facebook v. Power Ventures 310

C. Liability of Online Service Providers 311

1. Direct Liability 311
(a) Louis Vuitton v. Akanoc Solutions 312
(b) Flava Works v. Gunter 313

2. Contributory Liability 314
(a) The Netcom Case 314
(b) The MAPHIA Case 315
(c) The Peer-to-Peer Filing Sharing Cases 316
(1) The Napster Cases 316
(2) The Scour.com Lawsuit 351
(3) The Aimster/Madster Lawsuits 352
(4) The StreamCast/Kazaa/Grokster Lawsuits 358
(5) The Supreme Court's Grokster Decision 365
(6) The Grokster Decision on Remand 380
(i) The Ruling on Liability 380
(ii) The Permanent Injunction 384
(7) The Audiogalaxy Case 387
(8) The Hummer Winblad/Bertelsmann Litigation 388
(9) Arista Records v. Lime Group 391
(d) The CoStar Case 391
(e) Ellison v. Robertson 392
(f) Perfect 10 v. Cybernet Ventures 393
(g) Perfect 10 v. Visa International 394
(h) Parker v. Google 396
(i) MDY Industries v. Blizzard Entertainment 396
(j) Louis Vuitton v. Akanoc Solutions, Inc. 399
(k) Arista Records v. Usenet.com 402
(l) Hermeris v. Brandenburg 402
(m) Flava Works v. Gunter 404
(n) Summary 406
3. Vicarious Liability 408
(a) The Netcom Case and its Progeny 408
(b) The Napster Cases 409
(c) Ellison v. Robertson 409
(d) Perfect 10 v. Cybernet Ventures 409
(e) The Aimster/Madster Lawsuits 410
(f) The StreamCast/Kazaa/Grokster Lawsuits 411
(g) Perfect 10 v. Visa International 413
(h) Parker v. Google 415
(i) Louis Vuitton v. Akanoc Solutions 415
(j) Live Face on Web v. Howard Stern Productions 416
(k) Arista Records v. Usenet.com 416
(l) Corbis v. Starr 417
(m) Arista Records v. Lime Group 418
(n) Hermeris v. Brandenburg 418
(o) Luvdarts v. AT&T Mobility 418
(p) Flava Works v. Gunter 418
4. Inducement Liability 419
(a) The Supreme Court's Grokster Decision 419

(b) Arista Records v. Usenet.com 419
(c) Columbia Pictures v. Fung 420
(d) Arista Records v. Lime Group 423
(e) Flava Works v. Gunter 428
5. Adequacy of Pleadings of Secondary Liability Against Service Providers 428
(a) Miller v. Facebook 428
(b) Williams v. Scribd 429
6. Limitations of Liability of Online Service Providers in the DMCA 430
(a) History of the Various Legislative Efforts 430
(b) The OSP Liability Provisions of the DMCA 432
(1) Safe Harbors – Definition of a "Service Provider" 432
(i) Acting as a Mere Conduit for Infringing Information – Section 512(a) 433
a. The Napster Case 434
b. Ellison v. Robertson 436
c. The Aimster/Madster Lawsuits 441
d. Perfect 10 v. CCBill 442
e. Columbia Pictures v. Fung 449
(ii) Caching – Section 512(b) 450
a. Field v. Google 451
b. Parker v. Google 453
c. Perfect 10 v. Google 453
(iii) Innocent Storage of Infringing Information – Section 512(c) 457
a. The ALS Scan Case – What Constitutes a "Substantially" Compliant Notice 460
b. Hendrickson v. eBay 464
c. CoStar v. LoopNet 468
d. Perfect 10 v. Cybernet Ventures 476
e. The Aimster/Madster Lawsuits 479
f. Hendrickson v. Amazon.com 479
g. Rossi v. MPAA 481
h. Perfect 10 v. CCBill 482
i. Corbis Corp. v. Amazon.com, Inc. 484
j. Tur v. YouTube, Inc. 489
k. Io Group v. Veoh Networks 490
l. UMG Recordings v. Veoh Networks 494
m. Perfect 10 v. Amazon 505
n. Louis Vuitton v. Akanoc Solutions 507
o. Viacom v. YouTube 507
p. Perfect 10 v. Google 516
q. Wolk v. Kodak Imaging Network 517
r. Flava Works v. Gunter 520
s. Capitol Records v. MP3tunes 520
t. Obodai v. Demand Media 525

(iv) Referral or Linking to Infringing Material (Information Location Tools) – Section 512(d) 526
a. The Napster Case 527
b. Perfect 10 v. Cybernet Ventures 529
c. The MP3Board Case 529
d. The Aimster/Madster Lawsuits 529
e. The Diebold Lawsuit 530
f. Perfect 10 v. CCBill 532
g. Columbia Pictures v. Fung 533
h. Perfect 10 v. Google 534
(2) General Requirements for Limitations of Liability 534
(3) Special Provisions for Nonprofit Educational Institutions 535
(4) Filing of False DMCA Notices – Section 512(f) 535
(i) Rossi v. MPAA 536
(ii) Online Policy Group v. Diebold, Inc. 536
(iii) Dudnikov v. MGA Entertainment 536
(iv) Novotny v. Chapman 536
(v) BioSafe-One, Inc. v. Hawks 537
(vi) Lenz v. Universal Music Corp. 538
(vii) UMG Recordings v. Augusto 541
(viii) Capitol Records v. MP3tunes, LLC 542
(ix) Brave New Films v. Weiner 542
(x) Design Furnishings v. Zen Path 543
(xi) Amaretto Ranch Breedables v. Ozimals 543
(xii) Shropshire v. Canning 544
(xiii) Rock River Communications v. Universal Music Group 545
(xiv) Smith v. Summit Entertainment 546
(xv) Ouellette v. Viacom 546
(5) Other Provisions 547
(6) Injunctions Against Service Providers 548
(7) Designation of Agent to Receive Notification of Claimed Infringement 548
(8) Whether the Safe Harbors Apply to Pre-1972 Sound Recordings 549
7. Limitations of Liability of Online Service Providers under the Communications Decency Act 550
(a) Stoner v. eBay 550
(b) Perfect 10 v. CCBill 552
8. Secondary Liability of Investors 552
(a) The Hummer Winblad/Bertelsmann Litigation 552
(b) UMG Recordings v. Veoh Networks 552
D. Linking and Framing 554
1. The Shetland Times Case 557
2. The Total News Case 558
3. The Seattle Sidewalk Case 559
4. The Futuredontics Case 561

5. The Bernstein Case 561
6. The Intellectual Reserve Case 562
7. Ticketmaster v. Tickets.com 563
8. The MP3Board Case 566
9. Kelly v. Arriba Soft 569
10. Batesville Services, Inc. v. Funeral Depot, Inc. 569
11. Live Nation Sports v. Davis 571
12. Perfect 10 v. Google (aka Perfect 10 v. Amazon) 572

E. Streaming and Downloading 572

1. The Digital Performance Right – The Section 114(d)(1) Exemption and Streaming by FCC-Licensed Broadcasters 572
2. The Digital Performance Right – Statutory Licenses Under Section 114 for Certain Nonsubscription and Subscription Services 576
   (a) Preexisting Subscription Services 579
   (b) Eligible Nonsubscription Services (Webcasters) 582
   (c) New Subscription Services 591
3. The Digital Performance Right – What Constitutes an "Interactive" Service 594
   (a) Arista Records v. Launch Media 596
4. The Reproduction Right – Mechanical Licenses and Streaming/Downloading 598
   (a) Applicability of the Section 115 Compulsory License to Streaming 600
   (b) The Copyright Office's Position – The 2001 DMCA Report and Comment Proceedings 602
   (c) The NMPA/HFA/RIAA Agreement of 2001 604
   (d) The Interactive Streaming and Limited Download Agreement of 2008 606
   (e) 2008 Interim Regulation re Compulsory DPD License 607
   (f) Applicability of the Section 115 Compulsory License to Ringtones 609
5. The Section 111 Compulsory License for Cable Systems 609
   (a) WPIX v. ivi 610
6. International Licensing Efforts 610

F. First Sales in Electronic Commerce 610

G. Pop-Up Advertising 613

1. The Gator Litigations 613
2. The WhenU Litigations 614
   (a) U-Haul v. WhenU.com 615
   (b) Wells Fargo v. WhenU.com 616
   (c) 1-800 Contacts v. WhenU.com 618
3. The MetroGuide Litigation 621
4. The D Squared Litigation 621
5. International Decisions 622

H. Harvesting of Web Data 622

1. The FatWallet Dispute 622
2. Nautical Solutions Marketing v. Boats.com 623

IV. CONCLUSION 624

ADVANCED COPYRIGHT ISSUES ON THE INTERNET

I. INTRODUCTION

Over the years, the Internet has become the basic foundational infrastructure for the global movement of data of all kinds. With continued growth at a phenomenal rate, the Internet has moved from a quiet means of communication among academic and scientific research circles into ubiquity in both the commercial arena and private homes. The Internet is now a major global data pipeline through which large amounts of intellectual property are moved. As this pipeline is increasingly used in the mainstream of commerce to sell and deliver creative content and information across transnational borders, issues of intellectual property protection for the material available on and through the Internet have taken on great importance.

Copyright law provides one of the most important forms of intellectual property protection on the Internet for at least two reasons. First, much of the material that moves in commerce on the Internet is works of authorship, such as musical works, multimedia works, audiovisual works, movies, software, database information and the like, which are within the usual subject matter of copyright. Second, because the very nature of an electronic online medium requires that data be "copied" as it is transmitted through the various nodes of the network, copyright rights are obviously at issue.

Traditional copyright law was designed to deal primarily with the creation, distribution and sale of protected works in tangible copies.[1] In a world of tangible distribution, it is generally easy to know when a "copy" has been made. The nature of the Internet, however, is such that it is often difficult to know precisely whether a "copy" of a work has been made and, if so, where it resides at any given time within the network. As described further below, information is sent through the Internet using a technology known as "packet switching," in which data is broken up into smaller units, or "packets," and the packets are sent as discrete units. As these packets pass through the random access memory (RAM) of each interim computer node on the network, are "copies" of the work being made?

The case of MAI Systems Corp. v. Peak Computer[2] held that loading a computer program into the RAM of a computer constituted the making of a "copy" within the purview of copyright law. This case has been followed by a number of other courts. Under the rationale of this case, a "copy" may be created under United States law at each stage of transmission of a work through the Internet. The language of two treaties discussed extensively in this paper – the WIPO Copyright Treaty[3] and the WIPO Performances and Phonograms Treaty[4] – leave unclear the

---

1 For example, under United States law, copyright protection subsists only in "works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 102(a).

2 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

3 World Intellectual Property Organization Copyright Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17 (1997).

crucial question whether the MAI approach will be internationalized. In any event, these two treaties would strengthen copyright holders' rights of "distribution" and would create new rights of "making available to the public" a copyrighted work, both of which are implicated by transmissions through the Internet nearly as broadly as the right of reproduction.

The ubiquitous nature of "copying" in the course of physical transmission gives the copyright owner potentially very strong rights with respect to the movement of copyrighted material through the Internet, and has moved copyright to the center of attention as a form of intellectual property on the Internet. If the law categorizes all interim and received transmissions as "copies" for copyright law purposes, or treats all such transmissions as falling within the right of distribution of the copyright owner, then activities that have been permissible with respect to traditional tangible copies of works, such as browsing and transfer, may now fall within the control of the copyright holder.

This paper discusses the multitude of areas in which copyright issues arise in an online context. Although the issues will, for simplicity of reference, be discussed in the context of the Internet, the analysis applies to any form of online usage of copyrighted works. Part II of this paper discusses the various copyright rights that may be implicated by transmissions and use of works on the Internet, including new rights and remedies, as well as certain limitations on liability for online service providers afforded under federal statutes. Part III then analyzes the application of those rights to various activities on the Internet, such as browsing, caching, operation of an online service or bulletin board, linking to other sites, creation of derivative works, and resale or subsequent transfer of works downloaded from the Internet. Part III also analyzes the application of the fair use doctrine and the implied license doctrine to various Internet activities. Because the law is still developing with respect to many of these issues, a great deal of uncertainty is likely to exist as the issues are worked out over time through the courts and the various relevant legislative bodies and industry organizations.

II. RIGHTS IMPLICATED BY TRANSMISSION AND USE OF WORKS ON THE INTERNET

This Part discusses the various rights of the copyright holder – the right of reproduction, the right of public performance, the right of public display, the right of public distribution, the right of importation, and the new rights of transmission and access – that are implicated by the transmission and use of works on the Internet.

A. The Right of Reproduction

The single most important copyright right implicated by the transmission and use of works on the Internet is the right of reproduction. As elaborated below, if the law categorizes all interim and received transmissions as "copies" for copyright law purposes, then a broad range of ordinary activities on the Internet, such as browsing, caching, and access of information, may fall within the copyright holder's monopoly rights.

---

[4] World Intellectual Property Organization Performances and Phonograms Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17 (1997).

1. The Ubiquitous Nature of "Copies" on the Internet

Under current technology, information is transmitted through the Internet using a technique known broadly as "packet switching." Specifically, data to be transmitted through the network is broken up into smaller units or "packets" of information, which are in effect labeled as to their proper order. The packets are then sent through the network as discrete units, often through multiple different paths and often at different times. As the packets are released and forwarded through the network, each "router" computer makes a temporary (ephemeral) copy of each packet and transmits it to the next router according to the best path available at that instant, until it arrives at its destination. The packets, which frequently do not arrive in sequential order, are then "reassembled" at the receiving end into proper order to reconstruct the data that was sent.[5] Thus, only certain subsets (packets) of the data being transmitted are passing through the RAM of a node computer at any given time, although a complete copy of the transmitted data may be created and/or stored at the ultimate destination computer, either in the destination computer's RAM, on its hard disk, or in portions of both.

To illustrate the number of interim "copies," in whole or in part, that may be made when transmitting a work through the Internet, consider the example of downloading a picture from a website. During the course of such transmission, no less than seven interim copies of the picture may be made: the modem at the receiving and transmitting computers will buffer each byte of data, as will the router, the receiving computer itself (in RAM), the Web browser, the video decompression chip, and the video display board.[6] These copies are in addition to the one that may be stored on the recipient computer's hard disk.[7]

2. Whether Images of Data Stored in RAM Qualify as "Copies"

Do these interim and final copies of a work (many of which are only partial) being transmitted through the Internet qualify as "copies" within the meaning of United States copyright law? The copyright statute defines "copies" as:

> material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a

---

[5] If any packet is lost along the way, the originating computer automatically resends it, likely along a different path than the lost packet was originally sent.

[6] Mark A. Lemley, "Dealing with Overlapping Copyrights on the Internet," 22 U. Dayton L. Rev. 547, 555 (1997).

[7] Even if a complete copy of the picture is not intentionally stored on the recipient computer's hard disk, most computers enhance performance of their memory by swapping certain data loaded in RAM onto the hard disk to free up RAM for other data, and retrieving the swapped data from the hard disk when it is needed again. Some of this swapped data may be left on the hard disk when the computer is turned off, even though the copy in RAM has been destroyed.

> machine or device. The term "copies" includes the material object, other than a phonorecord, in which the work is first fixed.[8]

The language of the definition raises two issues concerning whether images[9] of transmitted data in RAM qualify as "copies." First, depending upon where the data is in transit through the Internet, only a few packets – or indeed perhaps only a single byte – of the data may reside in a given RAM at a given time. For example, the modem at the receiving and transmitting computers may buffer only one or a few bytes of data at a time. A node computer may receive only a few packets of the total data, the other packets being passed through a different route and therefore a different node computer's RAM. Should the law consider these partial images a "copy" of the work? Should the outcome turn on whether all or most of the packets of data comprising the work pass through a given RAM, or only a portion? How can interim partial images of data stored in RAM be deemed a "copy" of a work, in the case where there is no point in time at which the entire work is available in a single RAM?

The White Paper published by the Working Group on Intellectual Property Rights of President Clinton's Information Infrastructure Task Force (referred to herein as the "NII White Paper") implicitly suggests that at least interim, partial copies of a work created in RAM in interim node computers during transmission may not themselves constitute a "fixed" copy:

> A transmission, in and of itself, is not a fixation. While a transmission may result in a fixation, a work is not fixed by virtue of the transmission alone. Therefore, "live" transmissions via the NII [National Information Infrastructure] will not meet the fixation requirement, and will be unprotected by the Copyright Act, unless the work is being fixed at the same time as it is being transmitted.[10]

The second general issue raised by the definition of "copies" is whether images of data stored in RAM are sufficiently "permanent" to be deemed "copies" for copyright purposes. The definition of "copies" speaks of "material objects," suggesting an enduring, tangible embodying medium for a work. With respect to an image of data stored in RAM, is the RAM itself to be considered the "material object"? The image of the data in RAM disappears when the computer is turned off. In addition, most RAM is "dynamic" (DRAM), meaning that even while the computer is on, the data must be continually refreshed in order to remain readable. So the data is in every sense "fleeting." Is its embodiment in RAM sufficiently permanent to be deemed a "copy"?

The legislative history of the Copyright Act of 1976 would suggest that data stored in RAM is not a "copy." As noted above, a "copy" is defined as a material object in which a work is "fixed." The statute defines a work to be "fixed in a tangible medium of expression when its

---

[8] 17 U.S.C. § 101.

[9] The word "image" is being used here to refer to an image of data stored in RAM to avoid use of the word "copy," which is a legal term of art. Whether an image of data in RAM should be deemed a "copy" for copyright law purposes is the question at issue.

[10] Information Infrastructure Task Force, "Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights" at 27 (1995).

embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."[11] The legislative history states:

> [T]he definition of "fixation" would exclude from the concept purely evanescent or transient reproductions such as those projected briefly on a screen, shown electronically on a television or other cathode ray tube, or captured momentarily in the "memory" of a computer.[12]

This language suggests that images of data temporarily stored in RAM do not constitute "copies."[13]

Several cases, however, have held to the contrary. The leading case is MAI Systems Corp. v. Peak Computer, Inc.,[14] which held that loading an operating system into RAM for maintenance purposes by an unlicensed third party maintenance organization created an illegal "copy" of the program fixed in RAM.[15] When the MAI decision first came down, it was unclear whether that decision would support a legal principle that any storage of a copyrighted work in RAM, no matter how transiently, constituted a "copy" within the purview of copyright law, for the Ninth Circuit's opinion in MAI seemed somewhat qualified. The court in MAI noted that the "copy" of the operating system was stored in RAM for several minutes (rather than only a few seconds). In addition, the court emphasized that while in RAM, output of the program was viewed by the user, which confirmed the conclusion that the RAM "copy" was capable of being perceived with the aid of a machine:

> [B]y showing that Peak loads the software into the RAM and is then able to view the system error log and diagnose the problem with the computer, MAI has adequately shown that the representation created in the RAM is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."[16]

In addition, a decision from the Seventh Circuit handed down shortly after MAI, NLFC, Inc. v. Devcom Mid-Am., Inc.,[17] although somewhat unclear on both the facts involved in the case and whether the court really understood the issue, contains language that may suggest that

---

[11] 17 U.S.C. § 101 (definition of "fixed in a tangible medium of expression").

[12] H.R. Rep. No. 94-1476, at 53 (1976), reprinted in U.S.C.C.A.N. 5659, 5666.

[13] But see R. Nimmer, Information Law ¶ 4.02[2], at 4-6 (2001) ("This language refers to subject matter protection and not whether particular acts create an infringing copy. The exclusion of transient works refers to the work itself, not a copy. It presumes that there was no copy of the work other than the transient display or memory.")

[14] 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

[15] Id. at 518.

[16] 991 F.2d at 518.

[17] 45 F.3d 231 (7th Cir. 1995).

merely proving that the defendant has remotely accessed the plaintiff's software through a terminal emulation program is not sufficient to prove that a "copy" has been made.[18] Moreover, an earlier Ninth Circuit decision in the case of Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.[19] implied that an image of data stored in RAM may not qualify as a "copy." At issue in that case was whether a device that altered certain bytes of data of a video game "on the fly" as such information passed through RAM created an infringing derivative work. The court held that it did not, because although a derivative work need not be fixed, it must have some "form" or "permanence," which were lacking in the enhanced displays created by the device. The court stated, however, that even if a derivative work did have to be fixed, the changes in the displayed images wrought on the fly by the accused device did not constitute a fixation because the transitory images it created were not "embodied" in any form.

Notwithstanding these earlier decisions, however, a great many courts have now followed MAI,[20] and some earlier decisions also support its conclusion.[21] Although the opinion in one of

---

[18] Id. at 236.

[19] 964 F.2d 965 (9th Cir. 1992).

[20] See Carson v. Verismart Software, 2012 U.S. Dist. LEXIS 4166 (N.D. Cal. Mar. 27, 2012) at *8-9 (pleading alleging that defendants were "using" plaintiff's software without authorization was sufficient to state a copyright claim because the software had to be loaded into RAM to run, which constitutes the making of a fixed copy under MAI); Costar Realty Information, Inc. v. Field, 2010 U.S. Dist. LEXIS 135016 at *19 (D. Md. Dec. 20, 2010) (copies of web pages stored automatically in a computer's cache or RAM upon a viewing of the web page fall within the definition of "copy"); DocMagic, Inc. v. Ellie Mae, Inc., 745 F. Supp. 2d 1148 (N.D. Cal. 2010) (unauthorized loading of software into RAM constitutes an act of copying and thus of infringement); Apple, Inc. v. Psystar Corp., 673 F. Supp. 2d 931, 935 (N.D. Cal. 2009) (turning on computers that loaded into RAM copies of Apple's Mac OS X operating system containing unauthorized modifications constitute direct infringement of Apple's reproduction right); Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp., 2009 U.S. App. LEXIS 14766 at *18-19 (4th Cir. July 7, 2009) (loading of software into RAM from unauthorized copies on hard disk was sufficiently fixed for purposes of copyright infringement); SimplexGrinnell LP v. Integrated Sys. & Power, Inc., 2009 U.S. Dist. LEXIS 30657 at *42 (S.D.N.Y. Apr. 8, 2009) (embodiment requirement is satisfied when a program is loaded for use into a computer's RAM and the duration requirement is satisfied when the program remains in RAM for several minutes or until the computer is shut off); MDY Industries, LLC v. Blizzard Entertainment, Inc., 2008 U.S. Dist. LEXIS 53988 (D. Ariz. July 14, 2008) (under MAI, copying software into RAM constitutes making a "copy" within the purview of copyright law, so that if a person is not authorized by the copyright holder through a license or by law (e.g. Section 117) to copy the software to RAM, the person commits copyright infringement when using the software in an unauthorized way); Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096, 1005 (C.D. Cal. 2007) (copies of web pages stored in a computer's cache or RAM upon a viewing of the web page fall within the Copyright Act's definition of a "copy"); Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc., 2004 U.S. Dist. LEXIS 12391 at *11-12 (D. Mass. July 2, 2004) (unauthorized copying of a program into RAM for use of the program infringes the copyright in the program); Lowry's Reports, Inc. v. Legg Mason, Inc., 271 F. Supp. 2d 737, 745 (D. Md. 2003) ("Unauthorized electronic transmission of copyrighted text, from the memory of one computer into the memory of another, creates an infringing 'copy' under the Copyright Act."); Stenograph L.L.C. v. Bossard Assocs., 144 F.3d 96 (D.C. Cir. 1998) (holding that an infringing copy of a computer program was made when that program was loaded into RAM upon boot up and used for its principal purposes); Triad Sys. v. Southeastern Express Co., 64 F.3d 1330 (9th Cir. 1995), cert. denied, 116 S. Ct. 1015 (1996); Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 53 U.S.P.Q.2d 1425 (D. Utah 1999); Tiffany Design, Inc. v. Reno-Tahoe Specialty, Inc., 55 F. Supp. 1113 (D. Nev. 1999); Marobie-FL Inc. v. National Association of Fire Equipment Distributors, 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997); Advanced Computer Servs. v.

these decisions suggests that only copies that exist for several minutes should constitute a "copy" within the purview of copyright law,[22] the others appear not to focus on how transitorily an image may be stored in RAM in ruling that such an image constitutes a "copy" for purposes of copyright law.

One of these decisions, Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,[23] was the first decision to focus on whether the act of browsing on the Internet involves the creation of "copies" that implicate the copyright owner's rights. In that case, the court, citing the MAI decision, flatly stated, "When a person browses a website, and by so doing displays the [copyrighted material], a copy of the [copyrighted material] is made in the computer's random access memory (RAM), to permit viewing of the material. And in making a copy, even a temporary one, the person who browsed infringes the copyright."[24] This decision, although quite direct in its holding, appears to address only the final "copy" that is made in the RAM of a Web surfer's computer in conjunction with viewing a Web page through a browser. It does not address the trickier issue of whether whole or partial interim copies made in RAM of node computers during the course of transmission through the Internet also constitute "copies" within the purview of a copyright owner's copyright rights.

However, a 2004 decision from the Fourth Circuit, CoStar v. Loopnet,[25] held that transient copies made by an OSP acting merely as a conduit to transmit information at the instigation of others does not create fixed copies sufficient to make it a direct infringer of copyright. "While temporary electronic copies may be made in this transmission process, they would appear not to be 'fixed' in the sense that they are 'of more than transitory duration,' and the ISP therefore would not be a 'copier' to make it directly liable under the Copyright Act."[26] The court drew a distinction between the final copy of a work made in the RAM of the ultimate user's computer, and the transient copies made by an OSP in the course of transmitting such copies:

> In concluding that an ISP has not itself fixed a copy in its system of more than transitory duration when it provides an Internet hosting service to its subscribers, we do not hold that a computer owner who downloads copyrighted software onto a computer cannot infringe the software's copyright. See, e.g., MAI Systems

---

MAI Sys., 845 F. Supp. 356 (E.D. Va. 1994); see also 2 M. Nimmer & D. Nimmer, Nimmer on Copyright § 8.08[A][1], at 8-114 (1999) (suggesting that RAM copies are fixed).

[21] See Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 260 (5th Cir. 1988) ("the act of loading a program from a medium of storage into a computer's memory creates a copy of the program"); Apple Computer, Inc. v. Formula Int'l, 594 F. Supp. 617, 621 (C.D. Cal. 1984) (noting that copying a program into RAM creates a fixation, albeit a temporary one); Telerate Sys. v. Caro, 8 U.S.P.Q.2d 1740 (S.D.N.Y. 1988) (holding that the receipt of data in a local computer constituted an infringing copy).

[22] Advanced Computer Services v. MAI Systems, 845 F. Supp. 356, 363 (E.D. Va. 1994).

[23] 53 U.S.P.Q.2d 1425 (D. Utah 1999).

[24] Id. at 1428.

[25] 373 F.3d 544 (4th Cir. 2004).

[26] Id. at 551.

> Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993). When the computer owner downloads copyrighted software, it possesses the software, which then functions in the service of the computer or its owner, and the copying is no longer of a transitory nature. See, e.g., Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 260 (5th Cir. 1988). "Transitory duration" is thus both a qualitative and quantitative characterization. It is quantitative insofar as it describes the period during which the function occurs, and it is qualitative in the sense that it describes the status of transition. Thus, when the copyrighted software is downloaded onto the computer, because it may be used to serve the computer or the computer owner, it no longer remains transitory. This, however, is unlike an ISP, which provides a system that automatically receives a subscriber's infringing material and transmits it to the Internet at the instigation of the subscriber.[27]

A 2008 decision of the Second Circuit, The Cartoon Network LP v. CSC Holdings, Inc.,[28] addressed the issue of RAM copying in considerable detail, ruling that buffer copies in RAM made by Cablevision Systems Corp. in the course of converting channels of cable programming from the head end feed into a format suitable for storage of individual programs by a network digital video recording service upon customer demand were not fixed for sufficient duration to constitute "copies."[29] Cablevision made the buffer copies in conjunction with offering its "Remote Storage" Digital Video Recorder (RS-DVR) service that enabled Cablevision customers to record copies of particular programs, like a normal DVR, but to store the recorded programs on Cablevision's servers rather than on a DVR device at their homes. Cablevision created buffer copies, one small piece at a time, of the head end programming in two buffers – a primary ingest buffer and a Broadband Media Router (BMR) buffer – even if no customer requested that a copy of particular programming be stored on its behalf in the RS-DVR service. The primary ingest buffer held no more than 0.1 seconds of each incoming channel's programming at any moment. The data buffer in the BMR held no more than 1.2 seconds of programming at any time. The plaintiffs argued that these buffer copies made Cablevision a direct infringer of their copyrights.[30]

The lower court found Cablevision a direct infringer largely in reliance on MAI and cases following it.[31] The Second Circuit, however, reversed. The court noted that to satisfy the statutory definition of "copies," two requirements must be met – an "embodiment" requirement (embodiment in a tangible medium from which it can be perceived or reproduced) and a "duration" requirement (embodiment for a period of more than transitory duration). The Second

---

27 Id.

28 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 2009 U.S. LEXIS 4828 (2009).

29 Id. at 129-30.

30 Id. at 123-24, 127.

31 Twentieth Century Fox Film Corp. v. Cablevision Sys. Corp., 478 F. Supp. 2d 607, 621-22 (S.D.N.Y. 2007).

Circuit found that the district court had mistakenly limited its analysis to the embodiment requirement, and that its reliance on MAI and cases following it was misplaced.[32]

> In general, those cases conclude that an alleged copy is fixed without addressing the duration requirement; it does not follow, however, that those cases assume, much less establish, that such a requirement does not exist. Indeed, the duration requirement, by itself, was not at issue in *MAI Systems* and its progeny.… Accordingly, we construe *MAI Systems* and its progeny as holding that loading a program into a computer's RAM *can* result in copying that program. We do not read *MAI Systems* as holding that, as a matter of law, loading a program into a form of RAM *always* results in copying.[33]

Turning to the facts of the case at hand, the Second Circuit ruled that, although the embodiment requirement was satisfied by the buffers because the copyrighted works could be copied from them,[34] the duration requirement had not been satisfied. The court noted that no bit of data remained in any buffer for more than a fleeting 1.2 seconds, unlike the data in cases like MAI, which remained embodied in the computer's RAM until the user turned the computer off.[35] "While our inquiry is necessarily fact-specific, and other factors not present here may alter the duration analysis significantly, these facts strongly suggest that the works in this case are embodied in the buffer for only a 'transitory' period, thus failing the duration requirement."[36] Accordingly, the acts of buffering in the operation the RS-DVR did not create "copies" for which Cablevision could have direct liability.[37]

The court in Costar Realty Information, Inc. v. Field[38] ruled that an allegation that the defendant accessed a password-protected database without authorization, which contained the plaintiff's copyrighted photographic images, raised a genuine dispute of material fact as to whether the defendant engaged in direct copyright infringement when he viewed the copyrighted work on a website that he did not have proper authorization to enter.[39] Citing the Intellectual Reserve case, the court ruled that "simply browsing a website that contains copyrighted material

---

[32] Cartoon Network, 2008 U.S. App. LEXIS 16458 at *14-16.

[33] Id. at *16, 18.

[34] Id. at *22. "The result might be different if only a single second of a much longer work was placed in the buffer in isolation. In such a situation, it might be reasonable to conclude that only a minuscule portion of a work, rather than 'a work' was embodied in the buffer. Here, however, where every second of an entire work is placed, one second at a time, in the buffer, we conclude that the work is embodied in the buffer." Id. at *22-23.

[35] Id. at *23.

[36] Id.

[37] Id. at *24.

[38] 2010 U.S. Dist. LEXIS 86567 (D. Md. Aug. 23, 2010).

[39] Id. at *37-38.

is sufficient to constitute copyright infringement because a copy of the work is made in the computer's RAM to enable the images to display on the computer monitor."[40]

3. The WIPO Treaties & the European Copyright Directive Are Unclear With Respect to Interim "Copies"

The language of two copyright treaties adopted during 1996 by the World Intellectual Property Organization (WIPO)[41] leaves open the issue of whether transitory images of data stored in RAM constitute "copies."[42]

(a) Introduction to the WIPO Treaties & the European Copyright Directive

The WIPO treaties were adopted as a result of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions hosted by WIPO in Geneva on December 2-20, 1996. More than 700 delegates from approximately 160 countries attended this Conference, which was aimed at tightening international copyright law to respond to issues arising from worldwide use of the Internet. The Conference was also designed to bring existing legislation on copyrights more in line with the provisions of the Trade Related Intellectual Property (TRIPS) sections of the Uruguay Round trade agreement, which in 1994 set up the World Trade Organization (WTO).[43]

Three new treaties were considered, only two of which were adopted: the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty."[44] The WIPO Copyright Treaty strengthens the Berne Convention for the Protection of Literary and Artistic Works (the "Berne Convention"),[45] established in 1886, which was the first international copyright treaty. The WIPO Performances and Phonograms Treaty strengthens the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, completed in Rome in 1961 (the "Rome Convention").[46]

---

40 Id. at *38

41 WIPO is a United Nations organization which handles questions of copyrights and trademarks.

42 The treaties enter into force three months after 30 instruments of ratification or accession by member States have been deposited with the Director General of WIPO.

43 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments – Results of the Uruguay Round vol. 31; 33 I.L.M. 81 (1994).

44 The proposed WIPO Treaty on Intellectual Property in Respect of Databases generated huge controversy, and was not adopted at the Conference. "WIPO Delegates Agree on Two Treaties," 2 *BNA's Electronic Info. Pol'y & L. Rep*. 22, 22 (1997).

45 Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, 828 U.N.T.S. 221.

46 International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, Oct. 26, 1961, 496 U.N.T.X. 43.

Each of the treaties required 30 nations to accede to it before it would enter into force. On Dec. 5, 2001, Gabon became the 30th nation to accede to the WIPO Copyright Treaty, and on Feb. 20, 2002, Honduras became the 30th nation to accede to the WIPO Performances and Phonograms Treaty. Accordingly, each of those treaties entered into force ninety days thereafter, on March 6, 2002 and May 20, 2002, respectively.[47] The treaties are not self executing under United States law, and implementing legislation will have to be passed by Congress.

The two adopted treaties will effect important substantive changes in international copyright law that have potentially far reaching implications for the Internet, and the relevant provisions of these treaties will be discussed throughout this paper. The legislative history to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty took the form of several "Agreed Statements." Under the Vienna Convention, an Agreed Statement is evidence of the scope and meaning of the treaty language.[48] Relevant portions of the Agreed Statements will also be discussed in this paper.

Each of the signatories to the WIPO treaties was required to adopt implementing legislation to conform to the requirements of the treaties. The scope of legislation required in any particular country depends upon the substantive extent of that country's copyright law existing at the time of the treaty, as well the country's own views concerning whether its existing laws already conform to the requirements of the treaties. As discussed in detail below, WIPO implementation legislation in the United States took a largely minimalist view of the changes to United States copyright law required to conform to the WIPO treaties. It is curious that all the implementing legislation introduced in Congress implicitly took the position that U.S. law already contains most of the rights required under the WIPO treaties, in view of the fact that, as analyzed below, much of the language describing mandatory copyright rights in the WIPO treaties appears to go beyond the correlative rights in current United States law or to set up new rights entirely. The possibility that other countries would adopt legislation implementing the WIPO treaty rights in their seemingly broader form raises the prospect of varying scopes of rights in different countries, a situation that the WIPO treaties were intended to avoid in the first place.[49]

In contrast to the United States implementing legislation, the European Commission's "European Copyright Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society"[50] to update and harmonize member state copyright laws (which will be referred to herein as the "European Copyright Directive") seems to take a more expansive view, although individual member states are free to interpret the extent to which

---

47 "WIPO Copyright Treaty Enters Into Force As Gabon Becomes 30th Nation to Accede," *BNA's Electronic Commerce & Law Report* (Dec. 12, 2001) at 1224; "U.N. Announces Music Piracy Pact" (Feb. 21, 2002), available as of Feb. 21, 2002 at http://news.com.com/2100-1023-842169.html.

48 Vienna Convention on the Law of Treaties, May 23, 1969, art. 31(2), 1155 U.N.T.S. 331.

49 WIPO Copyright Treaty, Preamble, at 4; WIPO Performances and Phonograms Treaty, Preamble, at 22.

50 The text of the European Copyright Directive may be found at http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=2001&nu_doc=29&type_doc=Directive (available as of January 1, 2002).

their own copyright laws already conform to the dictates of the European Copyright Directive in adopting legislation in response to it.[51] The WIPO implementation legislation in the United States and the European Copyright Directive will be discussed at length throughout this paper as they relate to the various issues treated herein.

(b) The WIPO Copyright Treaty

Article 7 of an earlier draft of the WIPO Copyright Treaty would apparently have adopted the approach of MAI to the question of whether RAM copies fall within the reproduction right of the copyright holder.[52] The proposed Article 7(1) provided:

> (1) The exclusive right accorded to authors of literary and artistic works in Article 9(1) of the Berne Convention of authorizing the reproduction of their

---

[51] The European Copyright Directive was first circulated for comments among European legal experts. It was then officially published at the end of 1997 for a more public debate of its provisions. The European Parliament approved a final draft of the Directive on February 14, 2001. The European Commission, acting through the European Union ministers, accepted the final draft of the Directive on April 9, 2001.

[52] The WIPO Copyright Treaty contains a number of important provisions relevant to the Internet that are not discussed elsewhere in this paper. Article 2 codifies the idea/expression dichotomy of copyright law: "Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such." Article 4 expressly extends copyright protection to computer programs in all forms as literary works: "Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression."

Article 5 adopts the approach of the Supreme Court's decision in Feist Publications, Inc. v. Rural Telephone Serv., 499 U.S. 340 (1991), which held that only the selection or arrangement of a compilation of facts such as a database, and not the facts themselves, can be protected under copyright. Article 5 provides: "Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation." The proposed WIPO Treaty on Intellectual Property in Respect of Databases would have extended protection to the information itself in a database where such database was the fruit of substantial labor to compile. Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be Considered by the Diplomatic Conference, art. 1(1), WIPO Doc. CRNR/DC/6 (Aug. 30, 1996) <www.wipo.org/eng/diplconf/6dc_all.htm>. The controversy generated by this Treaty precluded its adoption by WIPO.

Article 7(1) provides that authors of computer programs, cinematographic works, and works embodied in phonograms shall enjoy the exclusive right of authorizing commercial rental to the public of the originals or copies of their works. Under Article 7(2), this rental right does not apply "in the case of computer programs where the program itself is not the essential object of the rental" or "in the case of cinematographic works, unless such commercial rental has led to widespread copying of such works materially impairing the exclusive right of reproduction." The Agreed Statement for Articles 6 and 7 notes that the expressions "copies" and "original and copies," being subject to the right of rental, "refer exclusively to fixed copies that can be put into circulation as tangible copies."

Article 6 of an earlier draft of the treaty would have required Contracting Parties to abolish non-voluntary broadcasting licenses within seven years of ratifying or acceding to the Treaty. This Article was deleted in the final adopted version.

works, in any manner or form, includes direct and indirect reproduction of their works, whether permanent or temporary.

The reference to "temporary" reproductions would have seemed to cover copies in RAM. The reference to "indirect" reproductions, particularly when coupled with the inclusion of "temporary" reproductions, might have been broad enough to cover interim, partial reproductions in RAM in the course of transmission of a work through the Internet, as well as complete copies of a work made in RAM and/or on a hard disk at the receiving computer.

In addition, proposed Article 7(2) of the treaty seemed to recognize the possibility that the language of Article 7(1) might be read to cover interim, partial reproductions during transmission, for it would have allowed signatory members (referred to as "Contracting Parties" in the treaty) to limit the right of reproduction in those instances:

> (2) Subject to the conditions under, and without prejudice to the scope of applicability of, Article 9(2) of the Berne Convention, it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the work perceptible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the work that is authorized by the author or permitted by law in accordance with the Berne Convention and this Treaty.[53]

---

[53] Although this provision apparently was designed to ameliorate the potential mischief that might result from deeming all interim copies of a work in the course of transmission to be within the copyright owner's rights, it suffered from a number of potential problems. First, it would have left the issue up to the individual Contracting Parties whether to legislate exemptions. Thus, some Contracting Parties could have legislated such exemptions, while others did not, and the scope of the exemptions could have varied from country to country. As a result, whether interim copies during the course of transmission constitute infringement could have turned on the countries through which the transmission path passes, which is arbitrary under the current transmission technology of the Internet.

Second, Article 7(2) stated that the exemptions would apply only to transient or incidental reproductions taking place in the course of an authorized use of a work. Thus, if the transmission *itself* is unauthorized, the exemptions would not have applied, and there could still have been potential liability for the interim reproductions. Yet the operators of the node computers in which the interim copies are made would have no way of knowing whether any particular packet passing through the node is part of an authorized transmission. Article 7(2) therefore was flawed.

Article 10(1) of the adopted version affords a more generic vehicle for the adoption of exemptions or exceptions to rights conferred in the Treaty: "Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty to an extent consistent with exceptions or limitations provided for in the Berne Convention in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author."

The requirement that exceptions "not unreasonably prejudice the legitimate interests of the author" provides little guidance as to where the boundaries should lie around exceptions that Contracting Parties may wish to adopt in implementing legislation. The Agreed Statement concerning Article 10 does nothing to clarify the uncertainty: "It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have

The proposed Article 7, and the subject of interim transmission copies in general, generated a lot of controversy at the Conference. Telecommunications companies and Internet providers particularly objected to Article 7 because they feared that protection for temporary copying would impose liability for the interim copying that inherently occurs in computer networks. On the other hand, content providers such as the software, publishing and sound recording industries, opposed any open-ended approach that would permit all temporary copying.[54]

To resolve the controversy, the proposed Article 7 was ultimately simply deleted entirely from the adopted version of the treaty.[55] The Agreed Statement pertaining to the right of reproduction (Previous Article 7) provides:

> The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder,[56] fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.

The Assistant Secretary of Commerce and Commissioner of Patents and Trademarks at the time, Bruce Lehman, who headed the U.S. delegation to the Conference, stated at the end of the Conference that the Agreed Statement was intended to make clear that the reproduction right includes the right to make digital copies, but also that certain copying, e.g., for temporary digital storage, will be permitted. Commissioner Lehman further expressed the view that the treaty language is broad enough to permit domestic legislation that would remove any liability on the part of network providers where the copying is simply the result of their functioning as a conduit for network services.[57] However, the Agreed Statement itself does nothing more than reference Article 9 of the Berne Convention, which of course was adopted long before digital copies were an issue under copyright law, and makes no explicit reference to "temporary digital storage." In addition, the phrase "storage of a protected work in digital form in an electronic medium" could potentially include temporary digital storage in a node computer during transmission. It is therefore difficult to agree with Commissioner Lehman that the Agreed Statement makes anything "clear."

---

been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital network environment."

[54] "WIPO Delegates Agree on Two Treaties," 2 *BNA's Electronic Info. Pol'y & L. Rep*. 22, 22 (1997).

[55] Id.

[56] Article 9(2) of the Berne Convention provides, "It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author."

[57] "WIPO Delegates Agree on Two Treaties," 2 *BNA's Electronic Info. Pol'y & L. Rep*. 22, 22-23 (1997).

Rather, the Agreed Statement seems to leave virtually open ended the question of whether temporary images in RAM will be treated as falling within the copyright owner's right of reproduction. The uncertainty surrounding the scope of the reproduction right in a digital environment that, at least early on, seemed to divide U.S. courts therefore appears destined to replicate itself in the international arena. The uncertainty is heightened by the fact that Article 9 of the Berne Convention allows signatories to adopt certain exceptions to the reproduction right, raising the prospect of inconsistent exceptions being adopted from country to country. As a result, whether interim copies made during the course of transmission constitute infringement may turn on the countries through which the transmission path passes, which is arbitrary under the current transmission technology of the Internet. The issue ignited debate in the United States in connection with the federal legislation to implement the treaty.

(c) The WIPO Performances and Phonograms Treaty

Curiously, despite the focus on and ultimate removal of the proposed Article 7 of the WIPO Copyright Treaty, Article 7 as adopted in the WIPO Performances and Phonograms Treaty appears to come closer to adopting the approach of MAI. Article 7 gives performers the exclusive right of "authorizing the direct or indirect reproduction of their performances fixed in phonograms" (emphasis added). As originally proposed, Article 7 contained language even closer to the MAI logic, for it expressed the reproduction right of performers as one of "authorizing the direct or indirect reproduction, whether permanent or temporary, of their performances fixed in phonograms" (emphasis added). The use of the phrase "permanent or temporary" would more strongly have suggested that temporary interim reproductions of performances would be within the performer's right of reproduction.

In addition, Article 7(2) in an earlier draft was also deleted, which made reference to transient copies as follows:

> Subject to the conditions under, and without prejudice to the scope of applicability of, Article 19(2), it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the fixed performance perceptible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the fixed performance that is authorized by the performer or permitted by law in accordance with this Treaty.

The Agreed Statement that was issued with respect to the right of reproduction in the WIPO Performances and Phonograms Treaty is very similar to the Agreed Statement on the same subject that was issued with the WIPO Copyright Treaty. The Agreed Statement issued with the WIPO Performances and Phonograms Treaty provides:

> The reproduction right, as set out in Articles 7 and 11, and the exceptions permitted thereunder through Article 16, fully apply in the digital environment, in particular to the use of performances and phonograms in digital form. It is understood that the storage of a protected performance or phonogram in digital

form in an electronic medium constitutes a reproduction within the meaning of these Articles.

Thus, the Agreed Statement for the WIPO Performances and Phonograms Treaty contains the same ambiguities noted above with respect to the Agreed Statement for the WIPO Copyright Treaty.

Similar to Article 7, Article 11 gives producers of phonograms the "exclusive right of authorizing the direct or indirect reproduction of their phonograms, in any manner or form." As in the case of Article 7, an earlier proposed version of Article 11 contained the phrase "whether permanent or temporary," but this phrase was deleted in the final adopted version.[58]

Both Articles 7 and 11 define the rights recited therein in terms of "phonograms." "Phonogram" is defined in Article 2(b) as any "fixation" of the sounds of a performance or of other sounds other than incorporated in a cinematographic or other audiovisual work.

"Fixation" is defined broadly in Article 2(c) as "the embodiment of sounds or the representations thereof, from which they can be perceived, reproduced or communicated through a device." Storage in RAM would seem to satisfy this definition of fixation. Thus, any unauthorized transmission of a performance, or of the sounds embodied in a phonogram fixing such performance, to RAM memory would potentially violate the rights of both the owner of the performance and of the phonogram.[59]

---

[58] Article 11(2) in an earlier draft, similar to the proposed and later deleted Article 7(2), was also deleted. Article 11(2) would have provided: "Subject to the conditions under, and without prejudice to the scope of applicability of, Article 19(2), it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the phonogram audible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the phonogram that is authorized by the producer of the phonogram or permitted by law in accordance with this Treaty."

[59] The WIPO Performances and Phonograms Treaty contains a number of important provisions relevant to the Internet that are not discussed elsewhere in this paper. Article 4 requires Contracting Parties to afford national treatment to nationals of other Contracting Parties. Article 5(1) affords moral rights to performers: "Independently of a performer's economic rights, and even after the transfer of those rights, the performer shall, as regards his live aural performances or performances fixed in phonograms, have the right to claim to be identified as the performer of his performances, except where omission is dictated by the manner of the use of the performance, and to object to any distortion, mutilation or other modification of his performances that would be prejudicial to his reputation." A proposed Article 5(4), which was deleted in the final version, would have allowed any Contracting Party to declare in a notification deposited with the Director General of WIPO that it will not apply the provisions of Article 5.

Article 6 grants performers the exclusive right of authorizing the broadcasting and communication to the public of their unfixed performances (except where the performance is already a broadcast performance) and the fixation of their unfixed performances. Articles 9 and 13 grant performers and producers of phonograms, respectively, the exclusive right of authorizing the commercial rental to the public of the original and copies of their performances fixed in phonograms and of their phonograms.

Article 15 provides that "[p]erformers and producers of phonograms shall enjoy the right to a single equitable remuneration for the direct or indirect use of phonograms published for commercial purposes for broadcasting or for any communication to the public." The Agreed Statement for Article 15 provides: "It is understood that

Thus, the WIPO Performances and Phonograms Treaty replicates the same uncertainty as the WIPO Copyright Treaty with respect to the issue of whether transient "copies" of performances and phonograms will fall within the copyright owner's right of reproduction.[60] Indeed, the definition of the right of reproduction in Article 7 and Article 11 to include "direct or indirect" reproductions, together with the broad definition of "fixation" in Article 2(c), arguably adopt an approach that is closer to the MAI decision than the WIPO Copyright Treaty.

4. The Requirement of Volition for Direct Liability

Even assuming the rationale of the MAI case and the provisions of the WIPO Treaties are applied to deem all reproductions during transmission of a work through the Internet to be "copies" within the copyright owner's rights, a difficult issue arises as to who should be responsible for the making of such copies. Multiple actors may be potentially connected with a particular copy or copies of a work on the Internet, such as a work posted to a bulletin board service (BBS) – the original poster of the work, the BBS operator, the Online Service Provider (OSP) through which the BBS is offered, a user downloading a copy of the work from the BBS, and perhaps the operators of node computers through which a copy of the work may pass during the course of such downloading. Which one or more of these actors should be deemed to have made the copy or copies?

The most difficult aspect of the issue of which actors should be liable for copies made in the course of the downloading, viewing or other transmission of a work through the Internet stems from the fact that many such copies will typically be made *automatically*. For example, "copies" of the work (in whole or in part) will automatically be made in the RAM (and possibly in temporary hard disk storage) of each interim node computer within the transmission path of the work through the Internet. And the modems on the initiating and receiving ends of the transmission will buffer the data to be transmitted. Internet search engine services may use

---

Article 15 does not represent a complete resolution of the level of rights of broadcasting and communication to the public that should be enjoyed by performers and phonogram producers in the digital age. Delegations were unable to achieve consensus on differing proposals for aspects of exclusivity to be provided in certain circumstances or for rights to be provided without the possibility of reservations, and have therefore left the issue to future resolution."

Under Article 17(1), the term of protection to be granted to performers under the Treaty is at least 50 years from the end of the year in which the performance was fixed in a phonogram. Under Article 17(2), the term of protection to be granted to producers of phonograms under the Treaty is at least 50 years from the end of the year in which the phonogram was published, or failing such publication within 50 years from fixation of the phonogram, 50 years from the end of the year in which the fixation was made.

[60] Article 16 affords a generic vehicle for the adoption of exemptions or exceptions to rights conferred in the Treaty. Article 16(1) provides that "Contracting Parties may, in their national legislation, provide for the same kinds of limitations or exceptions with regard to the protection of performers and producers of phonograms as they provide for in their national legislation, in connection with the protection of copyright in literary and artistic works." Article 16(2) provides, however, similar to the WIPO Copyright Treaty, that "Contracting Parties shall confine any limitations of or exceptions to rights provided for in this Treaty to certain special cases which do not conflict with a normal exploitation of the phonogram and do not unreasonably prejudice the legitimate interests of the performer or of the producer of phonograms."

"spiders" to "crawl" through the Internet and make copies in RAM of materials on websites in the course of creating an index of that material.

Should a volitional act be required on the part of a third party to be liable for a copy made during transmission? If so, is a *direct* volitional act to cause the copy to be made required (as in the case of the original poster or the ultimate recipient of the copy), or is it sufficient if there was a volitional act in setting up the automatic process that ultimately causes the copy to be made (as in the case of the BBS operator, the OSP or the search engine service)? In view of the fact that copyright law has traditionally imposed a standard of strict liability for infringement,[61] one could argue that a direct volitional act may not be required.[62]

In addition to copies made automatically on the Internet, many infringing copies may be made *innocently*. For example, one may innocently receive an e-mail message that infringes the copyright rights of another and print that message out. Or one may innocently encounter (and copy into the RAM of one's computer or print out) infringing material in the course of browsing.

Several cases have addressed the issue of direct liability on the part of OSPs, BBS operators, and others for infringement of the reproduction right by users of the service, and in particular how much of a volitional act is required for direct infringement liability:

(a) The Netcom Case

The well known case of Religious Technology Center v. Netcom On-Line Communication Services[63] refused to impose direct infringement liability on an OSP for copies made through its service, at least where the OSP had no knowledge of such infringements. In that case the plaintiffs sought to hold liable the OSP (Netcom) and the operator of a BBS which gained its Internet access through the OSP for postings of the plaintiffs' copyrighted works on the bulletin board. The works in question were posted by an individual named Erlich[64] to the BBS's computer for use through Usenet.[65] The BBS's computer automatically briefly stored them. The OSP then automatically copied the posted works onto its computer and onto other computers on the Usenet. In accordance with usual Usenet procedures, Usenet servers

---

61 Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361, 1367 & n.10 (N.D. Cal. 1995); R. Nimmer, Information Law ¶ 4.06, at 4-25 (2001). Intent can, however, affect statutory damages to be awarded to the plaintiff. Netcom, 907 F. Supp. at 1367.

62 But cf. R. Nimmer, Information Law ¶ 4.06, at S4-50 (2001 Cum. Supp. No. 2) ("Although copyright is a strict liability statute, there should be some [sort] of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.").

63 907 F. Supp. 1361 (N.D. Cal. 1995).

64 In an earlier order, the court had entered a preliminary injunction against Erlich himself.

65 The Usenet is "a worldwide community of electronic BBSs that is closely associated with the Internet and with the Internet community. The messages in Usenet are organized into thousands of topical groups, or 'Newsgroups' .... As a Usenet user, you read and contribute ('post') to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings from other sites." Daniel P. Dern, The Internet Guide for New Users 196-97 (1994).

maintained the posted works for a short period of time – eleven days on Netcom's computer and three days on the BBS's computer.[66] The OSP neither created nor controlled the content of the information available to its subscribers, nor did it take any action after being told by the plaintiffs that Erlich had posted infringing messages through its system.[67]

The court cast the issue of direct liability as "whether possessors of computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party."[68] The court distinguished MAI, noting that "unlike MAI, the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean that Netcom has caused the copying. The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it."[69] The court held that, absent any volitional act on the part of the OSP or the BBS operator other than the initial setting up of the system, the plaintiffs' theory of liability, carried to its natural extreme, would lead to unreasonable liability:

> Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.[70]

Accordingly, the court refused to hold the OSP liable for direct infringement. The court also refused to hold the BBS operator liable for direct infringement. "[T]his court holds that the storage on a defendant's system of infringing copies and retransmission to other servers is not a direct infringement by the BBS operator of the exclusive right to *reproduce* the work where such copies are uploaded by an infringing user."[71] The court further held that the warning of the presence of infringing material the plaintiffs had given did not alter the outcome with respect to direct infringement liability:

> Whether a defendant makes a direct copy that constitutes infringement cannot depend on whether it received a warning to delete the message. This distinction may be relevant to contributory infringement, however, where knowledge is an element.[72]

The result of the Netcom case with respect to liability for direct infringement for the transmission and intermediate storage of copyrighted materials by an OSP was codified in the

---

66 Netcom, 907 F. Supp. at 1367.

67 Id. at 1368.

68 Id.

69 Id. at 1369.

70 Id. at 1370.

71 Id. at 1370-71 (emphasis in original).

72 Id. at 1370.

first safe harbor for OSPs set forth in Section 512(a)(1) of the Digital Millennium Copyright Act,[73] discussed in detail in Section III.C below.

(b) The MAPHIA Case

Another well known case, Sega Enterprises Ltd. v. MAPHIA,[74] adopted the logic of the Netcom case and refused to hold a BBS and its system operator directly liable for the uploading and downloading of unauthorized copies of Sega's video games, even though the defendants participated in encouraging the unauthorized copying, which was not true in Netcom. (As discussed below, the court did, however, find contributory liability.) The evidence established that the system operator had knowledge that the infringing activity was going on through the bulletin board, and indeed that he had specifically solicited the uploading of the games for downloading by users of the bulletin board.[75] The system operator also sold video game "copiers," known as "Super Magic Drives," through the MAPHIA BBS, which enabled subscribers to the BBS to play games which had been downloaded from the BBS.[76]

In granting a motion by Sega seeking summary judgment and a permanent injunction, the court refused to impose direct liability for copyright infringement on the BBS and its system operator, Chad Sherman. The court cited the Netcom case for the proposition that, although copyright is a strict liability statute, there should be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.[77] The court further stated:

> While Sherman's actions in this case are more participatory than those of the defendants in Netcom, the Court finds Netcom persuasive. Sega has not shown that Sherman himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sherman operated his BBS, that he knew infringing activity was occurring, and that he solicited others to upload games. However, whether Sherman knew his BBS users were infringing on Sega's copyright, or encouraged them to do so, has no bearing on whether Sherman directly caused the copying to occur. Furthermore, Sherman's actions as a BBS operator and copier seller are more appropriately analyzed under contributory or vicarious liability theories. Therefore, because

---

73 H.R. Rep. No. 105-551 Part 1, at 11, 24 (1998).

74 948 F. Supp. 923 (N.D. Cal. 1996).

75 Id. at 928.

76 Id. at 929. The Super Magic Drive consisted of a connector which plugged into the video game console, a receptacle which accepted video game cartridges, a main unit having a RAM to store games, and a floppy disk drive. "A MAPHIA BBS user can download video programs through his or her computer onto a floppy disk and make copies with his or her computer or play those game programs through the adaptor drive. To play a downloaded game, the user places the floppy disk into the video game copier. The user can choose the 'run program' option and run the video game program from the floppy disk without a video game cartridge. The adaptor drive also allows the user to copy the contents of a game cartridge onto a floppy disk."Id.

77 Id. at 932.

Sega has not shown that Sherman directly caused the copying, Sherman cannot be liable for direct infringement.[78]

(c) The Sabella Case

Similarly, in Sega Enterprises Ltd. v. Sabella,[79] the court refused to hold a BBS operator liable for direct infringement of the reproduction right where there was no evidence that the operator did any unauthorized copying herself. The defendant, Sabella, was the system operator of a BBS called "The Sewer Line," which contained a directory called "Genesis," into which were uploaded and downloaded infringing copies of Sega's video games by subscribers to the BBS. The defendant also sold copiers that enabled users to play Sega games directly from floppy disks without the need for a Sega game cartridge, and allowed purchasers of her copiers to download files from her BBS without charge for a certain time period.

Although the court agreed that the defendant's activities were more participatory than those of the defendant in Netcom, the court nevertheless found the Netcom court's logic persuasive. "Sega has not shown that Sabella herself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sabella should have known such activity was occurring, that she sold copiers that played games such as those on her BBS, and that she gave her copier customers downloading privileges on her BBS."[80] Citing Netcom, the court concluded that "whether Sabella knew her BBS users were

---

[78] Id. (citations to Netcom omitted). An earlier opinion in the case, issued in conjunction with the granting of a preliminary injunction to Sega, although somewhat unclear in its holding, seemed to suggest that the defendants *could* be held liable for direct infringement, at least for the unauthorized copies being uploaded through the bulletin board, although not for the subsequent downloading of copies by user of the bulletin board. See Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679, 683 (N.D. Cal. 1994). The court in the later opinion, however, disavowed this interpretation of its earlier opinion. With respect to its earlier order granting a preliminary injunction, the court stated, "To the extent that order can be read to suggest that Sherman may be liable for direct copyright infringement, it is clarified and superseded by this order." Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 932 n.5 (N.D. Cal. 1996).

The court also rejected a fair use defense raised by Sherman. With respect to the first fair use factor, the purpose and character of the use, the court found that Sherman's activities in encouraging the uploading and downloading of Sega's games was clearly commercial. "Sherman intended to profit directly from the content of the information made available on his BBS because his copier customers could use the game files to play the games rather than purchase Sega game cartridges. This distinguishes Sherman from the Internet provider in Netcom who did not gain anything from the content of the information available to subscribers." Id. at 934.

With respect to the second fair use factor, the nature of the copyrighted work, the court noted that the Sega video games were for entertainment uses and involved fiction and fantasy, so that the second factor weighed against fair use. Id. The court found that the third factor, the extent of the work copied, weighed against fair use because BBS users copied virtually entire copyrighted works, and Sherman had not shown any public benefit or explanation for the complete copying. Id. at 935. Finally, the court found that the fourth factor, the effect of the use upon the market, also weighed against fair use. "Even if the users are only playing the games in their own homes and even if there are currently only a limited number of users that have copiers, unrestricted and widespread conduct of this sort would result in a substantial adverse impact on the market for the Sega games."Id.

[79] 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

[80] Id. at 29,847-48.

infringing on Sega's copyright or encouraged them to do so, has no bearing on whether Sabella directly caused the copying to occur."[81]

The court did rule, however, that Sabella was liable for contributory infringement. The court cited the Ninth Circuit's holding in Fonovisa, Inc. v. Cherry Auction, Inc. that "providing the site and facilities for known infringing activity is sufficient to establish contributory liability."[82] The court noted that Sabella provided the BBS as a central depository site for the unauthorized copies of games, and allowed subsequent distribution of the games by user downloads. "She provided the facilities for copying the games by providing, monitoring, and operating the BBS software, hardware, and phone lines necessary for the users to upload and download games."[83] Accordingly, she was liable for contributory infringement under the Fonovisa standard.[84]

The court went further, however, holding that even an alternative and higher standard of "substantial participation," Sabella was liable. "Sabella did more than provide the site and facilities for the known infringing conduct. She provided a road map on the BBS for easy identification of Sega games available for downloading."[85] The court also rejected Sabella's fair use defense, issued a permanent injunction against Sabella, and awarded Sega statutory damages of $5,000 per infringed work.

In contrast to the preceding cases, several cases have held that where a defendant BBS operator has a more direct participation in the acts of infringement of its subscribers or users, there can be direct infringement liability for those acts:

(d) The Frena Case

Playboy Enterprises, Inc. v. Frena,[86] decided before Netcom, MAPHIA and Sabella, goes further than those cases and established liability for the acts of subscribers without a direct volitional act on the part of the operator. In that case, the court held the operator of a BBS, Frena, responsible for infringement of the rights of *distribution* and *display* (although curiously not the right of *reproduction*) with respect to the plaintiff's copyrighted photographs, which were distributed and displayed through the bulletin board by subscribers, despite evidence that the operator never himself uploaded any of the photographs onto the bulletin board and removed the

---

81 Id. at 29,848.

82 76 F.3d 259, 264 (9th Cir. 1996).

83 Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 at 29,849.

84 Another recent case applied the Fonovisa standard to hold the defendant Cyrix Corporation liable for contributory infringement for posting on its website some copyrighted applet software of the plaintiff from which it could be downloaded for use with the defendant's sound boards. "Cyrix is probably also contributorily liable because it encouraged and provided the resources for known infringing activity, i.e. the copying by others of the applet software that Cyrix made available on its website." Creative Labs, Inc. v. Cyrix Corp., 42 U.S.P.Q.2d 1872, 1875-76 (N.D. Cal. 1997).

85 Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 at 29,849.

86 839 F. Supp. 1552 (M.D. Fla. 1993).

photographs as soon as he was made aware of them. [87] "There is no dispute that Defendant Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies [himself]." [88] Although the case did not generate a finding of liability with respect to the right of reproduction, the court's logic with respect to finding infringement of the rights of distribution and display would seem to apply to the reproduction right as well.

The reach of Frena may be limited, however, because the BBS was apparently one devoted to photographs, much of it of adult subject matter, and subscribers routinely uploaded and downloaded images therefrom. Thus, the court may have viewed Frena as a more direct participant in the infringement, having set up a bulletin board that was devoted to the kind of activity that would foreseeably lead to infringement. The undisputed evidence of the presence on the bulletin board of the plaintiff's photographs, some of which had been edited to remove the plaintiff's trademarks and to add Frena's advertisements, was apparently evidence of sufficient involvement for the court to find direct infringement of the public distribution right. Similarly, Frena's selection of the infringing content for inclusion in the bulletin board was apparently sufficient involvement to find direct infringement of the public display right.[89]

In addition, as discussed in detail below, the legislative history of the Digital Millennium Copyright Act, which contains a number of safe harbors that address the issue of OSP liability, states that it was intended to overrule the Frena case, at least to the extent Frena suggested that passive, automatic acts engaged in through a technological process initiated by another through the facilities of an OSP could constitute direct infringement on the part of the OSP.[90] In a case decided in 2001, the Fourth Circuit held that the Digital Millennium Copyright Act had indeed overruled Frena "insofar as that case suggests that [passive, automatic acts engaged in through a technological process initiated by another] could constitute direct infringement."[91]

(e) The Webbworld Case

In a case factually similar to Frena, a company operating a website was held directly liable for the posting of copyrighted material on its site which could be downloaded by subscribers. In Playboy Enterprises, Inc. v. Webbworld, Inc.,[92] the defendant Webbworld, Inc. operated a website called Neptics, which made adult images available to subscribers who paid $11.95 per month. Over a period of several months, images became available through the Neptics website which were originally created by or for the plaintiff Playboy Enterprises, Inc.

---

87 Id. at 1554.

88 Id. at 1556.

89 K. Stuckey, Internet and Online Law § 6.10[1][b], at 6-88 – 6-89 (2008).

90 H.R. Rep. No. 105-551 Part 1, at 11 (1998).

91 ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001). A subsequent district court cited with approval the Fourth Circuit's decision on this point. See Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 695-96 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

92 968 F. Supp. 1171 (N.D. Tex. 1997)

The court rejected the defendant's argument that it could not be held directly liable for infringement under the logic of the Netcom case. The court distinguished the Netcom case on the ground that Netcom did not create or control the content of the information available to its subscribers, but rather merely provided access to the Internet. In contrast, the court noted that Neptics was receiving payment selling the images it stored on its computers, and therefore was acting as more than merely an information conduit.[93]

The defendant also argued that it could not be held liable for direct infringement because it had no control over the persons who posted the infringing images to the adult newsgroups from which Neptics obtained its material. The court rejected this argument: "While this may be true, Neptics surely has control over the images it chooses to sell on the Neptics' website. Even the absence of the ability to exercise such control, however, is no defense to liability. If a business cannot be operated within the bounds of the Copyright Act, then perhaps the question of its legitimate existence needs to be addressed."[94]

(f) The Sanfilippo Case

In Playboy Enterprises, Inc. v. Sanfilippo,[95] the court found the defendant operator of a website through which 7475 of the plaintiff's copyrighted images were available directly liable for infringement. The defendant admitted copying 16 files containing a great many of the images from a third party source onto his hard drive and CD-ROM. He also admitted that 11 other files containing such images were uploaded to his hard drive by a third party. The court found that, because the defendant had authorized the third party to upload such files to his site, the defendant was directly liable for such upload as a violation of the exclusive right under Section 106 of the copyright statute to "authorize" others to reproduce a copyrighted work. The court also found that the defendant had willfully infringed 1699 of the copyrighted images.

One of the most interesting aspects of the Sanfilippo case is the amount of damages the court awarded. The plaintiff sought statutory damages, and argued that a statutory damages award should be made for each individual image that was infringed. The defendant argued that, in awarding damages, the court should consider the fact that the copied images were taken from compilations and, therefore, an award should be made only with respect to each particular

---

93 Id. at 1175.

94 Id. The court also held that the principals of Webbworld could be held vicariously liable for the infringements. Although the principals had no control over those responsible for originally uploading the infringing images onto the Internet sites from which Webbworld drew its images, the principals had the right and ability to control what occurred on the Neptics website. The court ruled that the $11.95 subscription fee gave the principals a sufficient direct financial benefit from the infringing activity to hold them vicariously liable. Id. at 1177.

The court made its rulings in the context of a motion for summary judgment by the plaintiff. The court granted summary judgment of infringement with respect to sixty-two copyrighted images, but denied summary judgment with respect to sixteen additional images because of the presence of material issues of fact. In a subsequent ruling, the court found the defendants directly and vicariously liable with respect to these sixteen additional images based on a similar legal analysis of liability. See Playboy Enterprises, Inc. v. Webbworld, Inc., 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

95 1998 U.S. Dist. LEXIS 5125 (S.D. Cal. 1998).

magazine's copyright from which the images were taken. The court rejected this argument and allowed a statutory damage award for each image on the grounds that each image had an independent economic value on its own, each image represented "a singular and copyrightable effort concerning a particular model, photographer, and location,"[96] and the defendant marketed each one of the images separately. The court awarded statutory damages of $500 per image, for a total damage award of $3,737,500.[97]

(g) The Free Republic Case

Even where there is a direct volitional act on the part of a website operator in copying copyrighted material onto its site, difficult questions relating to First Amendment and fair use rights may arise, particularly where the Web is used to facilitate free ranging discussion among participants. For example, in 1998, the Los Angeles Times and The Washington Post filed a copyright infringement lawsuit against the operator of a website called the Free Republic. The site contained news stories from dozens of sources (including the plaintiffs), posted both by the operator of the site and its users, and users were allowed to attach comments to the stories.[98] The plaintiffs argued that, because verbatim complete copies of their news stories were often posted on the website, it was reducing traffic to their own websites on which the articles were posted, and was harming their ability to license their articles and to sell online copies of archived articles.[99] The defendants raised defenses under the fair use doctrine and under the First Amendment.[100] The defendants moved for summary judgment on all claims and the plaintiffs cross moved for summary judgment on the defendants' defense of fair use.

The court rejected the defendants' fair use argument and ruled that the defendants might be liable for infringement.[101] The court ruled that the first fair use factor (purpose and character of the use) favored the plaintiffs, noting there was little transformative about copying the entirety or portions of the articles, since the articles on the defendants' site served the same purpose as that for which one would normally seek to obtain the original – for ready reference if and when websites visitors needed to look at it.[102] The court also rejected the addition of commentary to the articles as favoring the defendants under the first factor, noting that the first posting of an article to the site often contained little or no transforming commentary, and in most cases it was not necessary to copy verbatim the entire article in order for users to be able to comment on the

---

96 Id. at *18-19.

97 The plaintiff requested an astronomical $285,420,000 in statutory damages ($20,000/image for 5776 images that were not willfully infringed, and $100,000/image for 1699 images that were willfully infringed).

98 Los Angeles Times v. Free Republic, 54 U.S.P.Q.2d 1453, 1455-56 (C.D. Cal. 2000).

99 Id. at 1457.

100 Id. at 1454-55.

101 The court limited its opinion to the availability of the defenses on which the defendants had moved for summary judgment. The court stated it was expressing no opinion as to whether, "given that the 'copying' of news articles at issue in this case is to a large extent copying by third-party users," the plaintiffs could prove a claim against the defendants for copyright infringement. Id. at 1458.

102 Id. at 1460-61.

article.[103] Finally, the court noted that the Free Republic site was a for-profit site, for which the copying enhanced the defendants' ability to solicit donations and generate goodwill for their website operation and other businesses of the website operator.[104]

The second fair use factor (nature of the copyrighted work) favored the defendants, because the copied news articles were predominantly factual in nature.[105] The third fair use factor (amount and substantiality of the portion used in relation to the copyrighted work as a whole) favored the plaintiffs, because in many cases exact copies of the entire article were made and the court had previously found that copying of the entire article was not necessary to comment on it.[106] Finally, the fourth fair use factor (effect of the use on the potential market for or value of the copyrighted work) favored the plaintiffs, because the court found that the availability of complete copies of the articles on the Free Republic site fulfilled at least to some extent demand for the original works and diminished the plaintiffs' ability to sell and license their articles.[107] On balance, then, the court concluded that the defendants could not establish a fair use defense.[108]

The court also rejected the defendants' First Amendment defense on the ground that the defendants had failed to show that copying entire news articles was essential to convey the opinions and criticisms of visitors to the site. The court noted that visitors' critiques could be attached to a summary of the article, or Free Republic could have provided a link to the plaintiffs' websites where the articles could be found.[109]

The parties subsequently settled the case, pursuant to which the court entered a stipulated final judgment enjoining the defendants from copying, posting, uploading, downloading, distributing or archiving any of the plaintiffs' works, or encouraging others to do so, or operating any website or other online service that accomplished or permitted any of the foregoing, except as otherwise permitted by the plaintiffs in writing or by the fair use doctrine. The defendants agreed to pay $1,000,000 in statutory damages for past infringing acts.[110]

---

[103] Id. at 1461 & 1463-64. The most telling fact on the latter point was that the Free Republic provided a hypertext link to *Jewish World Review's* website at its request, and asked that Free Republic visitors no longer copy the publication's articles verbatim. Id. at 1463.

[104] Id. at 1464-66.

[105] Id. at 1467.

[106] Id. at 1468.

[107] Id. at 1470-71. The court rejected the defendants' argument that its site was increasing hits to the plaintiffs' sites through referrals off its own site, noting that the defendants had not addressed how many hits to the plaintiffs' sites were diverted away as a consequence of the posting of articles to the Free Republic. The court also cited several cases rejecting the argument that a use is fair because it increases demand for the plaintiff's copyrighted work. Id. at 1471.

[108] Id. at 1472.

[109] Id. at 1472-73.

[110] Los Angeles Times v. Free Republic, 56 U.S.P.Q. 2d 1862 (C.D. Cal. 2000).

(h) The MP3.com Cases

In 2000, the Recording Industry Association of America, Inc. (RIAA), on behalf of 10 of its members, filed a complaint in federal court in the Southern District of New York for willful copyright infringement against MP3.com, based on MP3.com's new "My.MP3" service.[111] According to the complaint, this service allowed users to gain access through the Internet, and download digital copies of, commercial CDs, using one of two component services:

"Instant Listening Service" – Under this service, a user could place an order for a commercial CD through one of several online CD retailers cooperating with MP3.com, and then immediately have access to the song tracks on that CD stored on an MP3.com server, before arrival of the shipment of the physical CD ordered by the user.[112]

"Beam-it" – Under this service, a user could insert a commercial CD or a copy thereof (authorized or unauthorized) into his or her computer CD-ROM drive. If the MP3.com server was able to recognize the CD, the user was then given access to the song tracks contained on the CD stored on an MP3.com server.[113]

In order to offer the My.MP3 service, MP3.com purchased and copied the tracks from several tens of thousands of commercial CDs onto its servers.[114] When users accessed sound recordings through My.MP3, it was these reproductions made by MP3.com that were accessed, and not any copies made from the users' own CD.[115] The plaintiffs sought a ruling that the copying of the commercial CDs onto the MP3.com servers constituted willful infringement of the copyright rights of the plaintiffs.

The case raised the very interesting issue of whether, assuming that users who are the owners of a lawful copy of a CD could lawfully upload a copy thereof to an MP3.com server for their own private use under Section 1008[116] of the Audio Home Recording Act of 1992[117] or under the fair use doctrine, it should be lawful for MP3.com to assist users in accomplishing that, and, if so, whether it should be permissible to do so by advance copying of tracks in anticipation of a user ordering or already owning a CD containing those tracks.

---

111 Complaint for Copyright Infringement, UMG Recordings, Inc. v. MP3.com, Inc., No. 00 Civ. 0472 (S.D.N.Y. Jan. 21, 2000).

112 Id. ¶ 4 & App. A.

113 Id.

114 UMG Recordings Inc. v. MP3.com Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

115 Id.

116 Section 1008 provides: "No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings." 17 U.S.C. § 1008.

117 Pub. L. No. 102-563, 106 Stat. 4244 (1992).

The court ruled that the copying by MP3.com of the commercial CDs made out a prima facie case of direct copyright infringement,[118] and rejected the defendant's assertion that such copying was a fair use. The court ruled that the first fair use factor (purpose and character of the use) weighed against the defendant because the defendant's purpose for the use was commercial – although defendant was not charging users a fee for the service, "defendant seeks to attract a sufficiently large subscription base to draw advertising and otherwise make a profit."[119] The court rejected the defendant's argument that the copying was transformative because it allowed users to "space shift" their CDs into another format in which they could enjoy their sound recordings without lugging around physical CDs, ruling that the argument was "simply another way of saying that the unauthorized copies are being retransmitted in another medium – an insufficient basis for any legitimate claim of transformation."[120]

With respect to the second factor (nature of the copyrighted work), the court held that, because the copyrighted works at issue were creative musical works, this factor weighed against defendant.[121] The third factor (amount and substantiality of the copyrighted work used) also weighed against the defendant because the defendant had copied, and the My.MP3 service replayed, the copyrighted works in their entirety.[122]

Finally, with respect to the fourth factor (effect of the use upon the potential market for or value of the copyrighted work), the court noted that the defendant's activities "on their face invade plaintiffs' statutory right to license their copyrighted sound recordings to others for reproduction."[123] The defendant argued that its activities enhanced the plaintiffs' sales, since subscribers could not gain access to recordings through MP3.com unless had already purchased, or agreed to purchase, their own CD copies of those recordings. The court rejected this argument on the following rationale:

> Any allegedly positive impact of defendant's activities on plaintiffs' prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs' copyrighted works. This would be so even if the copyrightholder had not yet entered the new market in issue, for a copyrightholder's "exclusive" rights, derived from the Constitution and the

---

[118] "Thus, although defendant seeks to portray its service as the 'functional equivalent' of storing its subscribers' CDs, in actuality defendant is re-playing for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs' copyrighted CDs. On its face, this makes out a presumptive case of infringement under the Copyright Act of 1976 …." 92 F. Supp. 2d at 350.

[119] Id. at 351.

[120] Id. Contrast this holding with the Ninth Circuit's statement in RIAA v. Diamond Multimedia Sys., 180 F.3d 1072, 1079 (9th Cir. 1999), in which the Ninth Circuit found space shifting of a recording from a CD onto the "Rio" portable MP3 player device (through a process known as "ripping," or re-encoding of music data encoded in CD format into the MP3 file format) to be "paradigmatic noncommercial personal use entirely consistent with the purposes of the [Audio Home Recording Act]."

[121] UMG, 92 F. Supp. 2d at 351-52.

[122] Id. at 352.

[123] Id.

> Copyright Act, include the right, within broad limits, to curb the development of such a derivative market by refusing to license a copyrighted work or by doing so only on terms the copyright owner finds acceptable.[124]

The court therefore ruled that the defendant was not entitled to a fair use defense as a matter of law, and entered partial summary judgment holding the defendant to have infringed the plaintiffs' copyrights.[125] Subsequent to the court's ruling of infringement, the defendant settled with all but one of the plaintiff record companies (Universal Music Group) by taking a license to reproduce the plaintiffs' recordings on its servers and to stream them over the Internet to its subscribers, for which MP3.com reportedly paid $20 million to each of the record companies and agreed to pay a few pennies each time a user placed a CD in his or her locker, plus a smaller amount each time a track was played.[126]

Universal Music Group pursued a claim of statutory damages against MP3.com. The court concluded that MP3.com's infringement was willful, and awarded statutory damages of $25,000 per CD illegally copied by MP3.com.[127] Even based on the defendant's assertion that there were no more than 4,700 CDs for which the plaintiffs qualified for statutory damages (an issue that was to have been the subject of a separate trial), the statutory damages award would have come to $118,000,000.[128] On the eve of trial, the defendant settled with Universal Music Group by agreeing to pay the plaintiff $53.4 million and to take a license to Universal's entire music catalog in exchange for unspecified royalty payments.[129]

MP3.com's legal troubles did not end with the settlements with the RIAA plaintiffs. On Aug. 8, 2001, a group of over 50 music publishers and songwriters filed suit against MP3.com on claims of copyright infringement very similar to those asserted by the RIAA plaintiffs. The plaintiffs sought to hold MP3.com liable for the copies of their works made in connection with the My.MP3.com service, as well as for the subsequent "viral distribution" of copies of their works allegedly done through services such as Napster, Gnutella, Aimster, and Music City by MP3.com users after they download digital copies through MP3.com.[130] Numerous other suits

---

124 Id. (citations omitted).

125 Id. at 353.

126 See Jon Healey, "MP3.com Settles with BMG, Warner," *San Jose Mercury News* (June 10, 2000), at 1A; Chris O'Brien, "MP3 Sets Final Pact: Universal Music Group Will Get $53.4 Million," *San Jose Mercury News* (Nov. 15, 2000) at 1C, 14C.

127 UMG Recordings Inc. v. MP3.com, Inc., 56 U.S.P.Q.2d 1376, 1379, 1381 (S.D.N.Y. 2000). The court rejected the plaintiffs' argument that a statutory damages award should be made for each song copied, rather than each CD. The court cited 17 U.S.C. § 504(c)(1), which provides that a statutory damages award may be recovered in a specified range "with respect to any one work," and further provides that "all parts of a compilation or derivative work constitute one work." UMG Recordings Inc. v. MP3.com Inc., 109 F. Supp. 2d 223, 224-25 (S.D.N.Y. 2000).

128 56 U.S.P.Q.2d at 1381.

129 O'Brien, supra note 126, at 1C.

130 "Music Publishers, Songwriters Sue MP3.com for 'Viral Distribution' of Copyrighted Works," *BNA's Electronic Commerce & Law Report* (Aug. 29, 2001) at 933. In late August of 2001, MP3.com was acquired by media company Vivendi Universal.

were brought against MP3.com as well. For example, in Sept. of 2001, Isaac, Taylor & Zachary Hanson also sued MP3.com for copying of their copyrighted songs on My.MP3.com.[131]

Numerous opinions have been issued as a result of these lawsuits, holding MP3.com liable for willful copyright infringement and ruling it collaterally estopped from denying that it willfully infringed the plaintiffs' various copyrighted works when it created the "server copies" of thousands of CDs in late 1999 and early 2000.[132]

(i) The CoStar Case

In CoStar Group Inc. v. LoopNet, Inc.,[133] the plaintiff CoStar maintained a copyrighted commercial real estate database that included photographs. The defendant LoopNet offered a service through which a user, usually a real estate broker, could post a listing of commercial real estate available for lease. The user would access, fill out, and submit a form for the property available. To include a photograph of the property, the user was required to fill out another form. The photograph would initially be uploaded into a separate folder on LoopNet's system, where it would first be reviewed by a LoopNet employee to determine that it was in fact a photograph of commercial property and that there was no obvious indication the photograph was submitted in violation of LoopNet's terms and conditions. If the photograph met LoopNet's criteria, the employee would accept it and post it along with the property listing. CoStar claimed that over 300 of its copyrighted photographs had been posted on LoopNet's site, and sued LoopNet for both direct and contributory copyright liability.[134]

CoStar argued that LoopNet should be directly liable for copyright infringement because, acting through its employees' review and subsequent posting of the photographs, LoopNet was directly copying and distributing the photographs, citing the Frena case discussed above in Section II.A.4(d). The district court rejected this argument, noting that the Fourth Circuit in the ALS Scan case had concluded that the legislative history of the DMCA indicated Congress' intent to overrule the Frena case and to follow the Netcom case, under which an OSP's liability for postings by its users must be judged under the contributory infringement doctrine.[135]

The Fourth Circuit affirmed this ruling on appeal.[136] Citing its own decision in the ALS Scan case, the Fourth Circuit noted that it had already held that the copyright statute implies a requirement of volition or causation, as evidenced by specific conduct by the purported infringer,

---

131 Steven Bonisteel, "Hanson Sues Music Locker Service Over Copyright" (Sept. 26, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/170530.html.

132 See, e.g., Country Road Music, Inc. v. MP3.com, Inc., 279 F.Supp.2d 325 (S.D.N.Y. 2003); Zomba Enters., Inc. MP3.com, Inc., No. 00 Civ. 6833 (S.D.N.Y. Jun. 8, 2001); Teevee Toons, Inc. v. MP3.com, Inc., 134 F. Supp. 2d 546 (S.D.N.Y. 2001); UMG Recordings, Inc. v. MP3.com, Inc., No. 00 Civ. 472, 200 WL 1262568 (S.D.N.Y. 2000).

133 164 F. Supp. 2d 688 (D. Md. 2001).

134 Id. at 691-92.

135 Id. at 695-96.

136 CoStar v. LoopNet, 373 F.3d 544 (4th Cir. 2004).

for direct liability.[137] Mere ownership of an electronic facility by an OSP that responds automatically to users' input is not sufficient volition for direct liability. "There are thousands of owners, contractors, servers, and users involved in the Internet whose role involves the storage and transmission of data in the establishment and maintenance of an Internet facility. Yet their conduct is not truly 'copying' as understood by the Act; rather, they are conduits from or to would-be copiers and have no interest in the copy itself."[138]

The court also inferred a requirement of volition from the statute's concept of "copying," which requires the making of "fixed" copies. For the reasons discussed in Section II.A.2 above, the court concluded that transient copies made by an OSP acting merely as a conduit to transmit information at the instigation of others does not create sufficiently fixed copies to make it a direct infringer of copyright.[139] Accordingly, the court concluded, "[a]greeing with the analysis in Netcom, we hold that the automatic copying, storage and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement under §§ 501 and 106 of the Copyright Act."[140] The court also affirmed the district court's ruling that the quick review of photographs performed by LoopNet's employees before allowing them to be posted on the site did not amount to "copying," nor did it add volition to LoopNet's involvement in storing the copy.[141]

(j) The Ellison Case

The case of Ellison v. Robertson,[142] discussed in detail in Section III.C.6(b)(1)(i) below, refused to hold an OSP liable for direct infringement based on infringing materials posted on its service by users without its knowledge on Usenet servers hosted by AOL (infringing copies of fictional works).

(k) Perfect 10 v. Cybernet Ventures

In Perfect 10, Inc. v. Cybernet Ventures, Inc.,[143] the court refused to hold the defendant Cybernet, an "age verification service" that enrolled subscribers, after verifying their age as an adult, to a service that would enable them to gain access for a monthly fee to a large number of member sites displaying pornographic pictures, liable as a direct copyright infringer based on the unauthorized presence of the plaintiffs' copyrighted photographs on several of the member sites. The court discussed the Netcom, MAPHIA, and Hardenburgh cases (the Hardenburgh case is discussed in Section II.C below), then concluded as follows:

---

137 Id. at 549.

138 Id. at 551.

139 Id..

140 Id. at 555.

141 Id. at 556.

142 189 F. Supp. 2d 1051 (C.D. Cal. 2002), aff'd in part and rev'd in part, 357 F.3d 1072 (9th Cir. 2004) (district court's ruling of no direct infringement not challenged on appeal).

143 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

> The principle distilled from these cases is a requirement that defendants must actively engage in one of the activities recognized in the Copyright Act. Based on the evidence before the Court it appears that Cybernet does not use its hardware to either store the infringing images or move them from one location to another for display. This technical separation between its facilities and those of its webmasters prevents Cybernet from engaging in reproduction or distribution, and makes it doubtful that Cybernet publicly displays the works. Further, there is currently no evidence that Cybernet has prepared works based upon Perfect 10's copyrighted material. The Court therefore concludes that there is little likelihood that Perfect 10 will succeed on its direct infringement theory.[144]

(l) Field v. Google

In Field v. Google,[145] discussed in greater detail in Section III.B.4(a) below, the court ruled that Google should not be liable as a direct infringer for serving up through its search engine, in response to user search queries, copies of the plaintiff's copyrighted materials that had been cached by Google's automated crawler, the Googlebot. Citing the Netcom and CoStar cases, the court noted that a plaintiff must "show volitional conduct on the part of the defendant in order to support a finding of direct copyright infringement."[146] For some unknown reason, the plaintiff did not allege that Google committed infringement when its Googlebot made the initial copies of the plaintiff's Web pages on which his copyrighted materials had been placed and stored those copies in the Google cache, nor did the plaintiff assert claims for contributory or vicarious liability. Instead, the plaintiff alleged that Google directly infringed his copyrights when a Google user clicked on a link on a Google search results page to the Web pages containing his copyrighted materials and downloaded a cached copy of those pages from Google's computers.[147]

The court rejected this argument:

> According to Field, Google itself is creating and distributing copies of his works. But when a user requests a Web page contained in the Google cache by clicking on a "Cached" link, it is the user, not Google, who creates and downloads a copy of the cached Web page. Google is passive in this process. Google's computers respond automatically to the user's request. Without the user's request, the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur. The automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement under the Copyright Act.[148]

---

[144] Id. at 1168-69.

[145] 412 F. Supp. 2d 1106 (D. Nev. 2006).

[146] Id. at 1115.

[147] Id.

[148] Id.

(m) Parker v. Google

In Parker v. Google,[149] pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled "29 Reasons Not To Be A Nice Guy." He posted Reason # 6 on USENET. Parker asserted that Google's automatic archiving of this USENET posting constituted a direct infringement of his copyright. He also claimed that when Google produced a list of hyperlinks in response to a user's query and excerpted his web site in that list, Google again directly infringed his copyrighted work.[150]

The district court rejected these claims. Citing the Costar and Netcom cases, the district court held that "when an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition is missing. The automatic activity of Google's search engine is analogous. It is clear that Google's automatic archiving of USENET postings and excerpting of websites in its results to users' search queries do not include the necessary volitional element to constitute direct copyright infringement."[151]

On appeal, the Third Circuit affirmed in an unpublished decision.[152] The court noted that, "to state a direct copyright infringement claim, a plaintiff must allege volitional conduct on the part of the defendant," and Parker's allegations failed to allege any volitional conduct on the part of Google.[153]

(n) The Cablevision Case

In Twentieth Century Fox Film Corp. v. Cablevision Sys.,[154] the district court ruled that Cablevision was liable for direct copyright infringement based on the offering of a network digital video recording system known as the "Remote-Storage DVR System" (RS-DVR), which permitted customers to record cable programs on central servers at Cablevision's facilities and play the programs back for viewing at home. The technology underlying the RS-DVR worked as follows. Cablevision took the linear programming signal feed received at its head end and reconfigured it by splitting the feed into a second stream, which was then reformatted through a process known as "clamping" to convert the bitrate of the stream into one that was more efficient. In the process of clamping, portions of programming were placed into buffer memory. The stream was then converted into a number of single program transport streams, one channel per stream. The converted streams were then fed into a special set of "Arroyo" servers, which at any given moment in time, stored in a buffer three frames of video from each of the linear channels carried by Cablevision, so that if a customer requested that a particular program be

---

149 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

150 Id. at 496.

151 Id. at 497.

152 Parker v. Google, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

153 Id. at *6, 8.

154 478 F. Supp. 2d 607 (S.D.N.Y. 2007).

recorded, the appropriate packets could be retrieved from the buffer memory and copied to the customer's designated hard drive storage space on the Arroyo server.[155]

The RS-DVR service allowed customers to request that a program be recorded in one of two ways. The customer could navigate an on-screen program guide and select a future program to record, or while watching a program, the customer could press a "record" button on a remote control. In response, the Arroyo server would receive a list of recording requests, find the packets for the particular programs requested for recording, then make a copy of the relevant program for each customer that requested it be recorded. A separate copy would be stored in each customer's designated hard drive storage space on the Arroyo server. If no customer requested that a particular program be recorded, no copy of that program was made on the hard drives of the Arroyo server. When the customer selected a recorded program for playback, the Arroyo server would locate the copy of the desired program stored on the customer's designated hard drive storage space, then cause the program to be streamed out. The stream containing the program would be transmitted to every home in the node where the requesting customer was located, but only the requesting set-top box would be provided the key for decrypting the stream for viewing.[156]

The plaintiffs alleged direct copyright infringement based on Cablevision's creation of the copies on the hard drives of the Arroyo servers and of the buffer copies. Although Cablevision did not deny that these copies were being made, it argued that it was entirely passive in the process and the copies were being made by its customers. It also argued, based on the Sony case, that it could not be liable for copyright infringement for merely providing customers with the machinery to make the copies.[157]

The court rejected these arguments, ruling that the RS-DVR was not merely a device, but rather a service, and that, by providing the service, it was Cablevision doing the copying. In particular, the court found the relationship between Cablevision and RS-DVR customers to be significantly different from the relationship between Sony and VCR users. Unlike a VCR, the RS-DVR did not have a stand-alone quality. Cablevision retained ownership of the RS-DVR set-top box, and the RS-DVR required a continuing relationship between Cablevision and its customers. Cablevision not only supplied the set-top box for the customer's home, but also decided which programming channels to make available for recording, and housed, operated, and maintained the rest of the equipment that made the RS-DVR's recording process possible. Cablevision also determined how much memory to allot to each customer and reserved storage capacity for each customer on a hard drive at its facility. Customers were offered the option of acquiring additional capacity for a fee.[158]

In sum, the court concluded that the RS-DVR was more akin to a video-on-demand (VOD) service than to a VCR or other time-shifting device. The court noted that the RS-DVR

---

[155] Id. at 613-14.

[156] Id. at 614-16.

[157] Id. at 617-18.

[158] Id. at 618-19.

service was in fact based on a modified VOD platform. With both systems, Cablevision decided what content to make available to customers for on-demand viewing. As in VOD, the number of available pathways for programming delivery was limited; if there were none available, the customer would get an error message or busy signal. Thus, in its architecture and delivery method, the court concluded that the RS-DVR bore a striking resemblance to a VOD service – a service that Cablevision provided pursuant to licenses negotiated with programming owners.[159] Accordingly, the court ruled that a reasonable fact finder could conclude only that the copying at issues was being done not by the customers, but by Cablevision itself.[160]

With respect to the buffer copies, Cablevision argued that the buffer copies were not sufficiently fixed to be cognizable as "copies" under copyright law. The court rejected this argument, noting that the buffer copies were sufficiently permanent to make the Arroyo hard disk copies from, and were therefore capable of being reproduced, as required by the definition of "fixation." The court also cited the numerous court decisions, and the Copyright Office's August 2001 report on the DMCA, concluding that RAM copies are "copies" for purposes of the copyright act. Accordingly, the court concluded that summary judgment of direct infringement was warranted with respect to both the Arroyo server copies and the buffer copies.[161]

Finally, the court ruled, based on similar logic, that Cablevision was engaged in infringing transmissions and public performances to its customers.[162] The court noted that, "where the relationship between the party sending a transmission and party receiving it is commercial, as would be the relationship between Cablevision and potential RS-DVR customers, courts have determined that the transmission is one made 'to the public.'"[163]

On appeal, the Second Circuit reversed in The Cartoon Network LP v. CSC Holdings, Inc.[164] The Second Circuit's rulings with respect to the issue of buffer copies are discussed in Section II.A.2 above. With respect to the copies created on the hard drives of the Arroyo servers, the court noted that Netcom and its progeny direct attention to the volitional conduct that causes the copy to be made. In the case of an ordinary VCR, the court noted that it seemed clear that the operator of the VCR – the person actually pressing the button to make the recording, supplies the necessary element of volition, not the manufacturer of the device. The court concluded that the RS-DVR customer was not sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party for copies that were made automatically upon that customer's command. The court distinguished cases holding liable a copy shop making course packs for college professors, finding a significant difference between making a request to a human employee, who then voluntarily operates the copying system to make the

---

159 Id. at 619.

160 Id. at 621.

161 Id. at 621-22.

162 Id. at 622-23.

163 Id. at 623.

164 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 2009 U.S. LEXIS 4828 (2009).

copy, and issuing a command directly to a system, which automatically obeys commands and engages in no volitional conduct.[165] "Here, by selling access to a system that automatically produces copies on command, Cablevision more closely resembles a store proprietor who charges customers to use a photocopier on his premises, and it seems incorrect to say, without more, that such a proprietary 'makes' any copies when his machines are actually operated by his customers."[166]

Nor was Cablevision's discretion in selecting the programming that it would make available for recording sufficiently proximate to the copying to displace the customer as the person who "made" the copies. Cablevision's control was limited to the channels of programming available to a customer and not to the programs themselves. Cablevision had no control over what programs were made available on individual channels or when those programs would air, if at all. In that respect, Cablevision possessed far less control over recordable content that it did in the VOD context, where it actively selected and made available beforehand the individual programs available for viewing. Thus, Cablevision could not have direct liability for the acts of its customers, and any liability on its part would have to be based on contributory liability. The district court's noted "continuing relationship" with its RS-DVR customers, its control over recordable content, and the instrumentality of copying would be relevant to contributory liability, but not direct liability.[167]

With respect to the issue of direct liability, the Second Circuit concluded: "We need not decide today whether one's contribution to the creation of an infringing copy may be so great that it warrants holding that party directly liable for the infringement, even though another party has actually made the copy. We conclude only that on the facts of this case, copies produced by the RS-DVR system are 'made' by the RS-DVR customer, and Cablevision's contribution to this reproduction by providing the system does not warrant the imposition of direct liability."[168]

The Second Circuit's rulings with respect whether Cablevision was engaged in unauthorized public performances through the playback of the RS-DVR copies are discussed in Section II.B.5 below.

(o) Arista Records v. Usenet.com

In Arista Records LLC. V. Usenet.com, Inc.,[169] the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on "spool" news servers operated by

---

[165] Id. at 131.

[166] Id. at 132.

[167] Id. at 132-33.

[168] Id. at 133.

[169] 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.[170]

The plaintiffs contended that the defendants directly infringed their copyrights by engaging in unauthorized distribution of copies of their musical works to subscribers who requested them for download. The court, relying on the Netcom and Cablevision cases, ruled that a finding of direct infringement of the distribution right required a showing that the defendants engaged in some volitional conduct sufficient to show that they actively participated in distribution of copies of the plaintiffs' copyrighted sound recordings. The court found sufficient volitional conduct from the following facts. The defendants were well aware that digital music files were among the most popular files on their service, and took active measures to create spool servers dedicated to MP3 files and to increase the retention times of newsgroups containing digital music files. They took additional active steps, including both automated filtering and human review, to remove access to certain categories of content (such as pornography), while at the same time actively targeting young people familiar with other file-sharing programs to try their services as a supposedly safe alternative to peer-to-peer music file sharing programs that were getting shut down for infringement. From these facts, the court ruled that the defendants' service was not merely a passive conduit that facilitated the exchange of content between users who uploaded infringing content and users who downloaded such content, but rather the defendants had so actively engaged in the distribution process so as to satisfy the volitional conduct requirement. Accordingly, the court granted the plaintiffs' motion for summary judgment on their claim for direct infringement of the distribution right.[171]

(p) Quantum Systems v. Sprint Nextel

In Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp.,[172] Quantum sued Sprint for copyright infringement based on the automated loading of Quantum's software into the RAM of 13 Sprint computers from unauthorized copies on the hard disk when those computers were turned on or rebooted. The jury found liability and Sprint argued on appeal that the district court erred in denying its JMOL motion and sustaining the jury's finding of infringement because there was no evidence that Sprint engaged in volitional copying, since the RAM copies were automatically generated when the computers containing unauthorized, but unutilized, copies of the software on the hard disk were turned on. The court rejected this argument, distinguishing its Costar decision, which involved an ISP that merely provided electronic infrastructure for copying, storage, and transmission of material at the behest of its users. By contrast, in the instant case the copying was instigated by the volitional acts of Sprint's own employees who

---

[170] Id. at 130-31.

[171] Id. at 132, 146-49. As a sanction for litigation misconduct, including spoliation of evidence and sending key employees out of the country on paid vacations so they could not be deposed, the court precluded the defendants from asserting an affirmative defense of protection under the DMCA's safe harbor provisions. Id. at 137-42.

[172] 2009 U.S. App. LEXIS 14766 (4th Cir. July 7, 2009).

loaded the original copies of the software onto Sprint computers and then rebooted the computers, thereby causing the RAM copies.[173]

(q) Disney Enterprises v. Hotfile

In Disney Enterprises, Inc. v. Hotfile Corp.,[174] the defendant operated the web site www.hotfile.com, at which users could upload electronic files to Hotfile's servers. Upon upload, the user received a unique link to the file. The Hotfile servers would then automatically make five additional copies of the uploaded files and assign each copy a unique link. Each link acted as a locator, allowing anyone with the link to click it or plug it into a web browser in order to download the file. Third party sites, not Hotfile, spread the links that allowed persons to download the files.[175]

Hotfile made a profit in two ways. First, although anyone could use a link to download a file, Hotfile charged members a fee that enabled them to download files much faster than non-members. Second, Hotfile sold "hotlinks" that allowed third party sites to post a link that, when clicked, automatically began to download the file, without ever directing the person clicking the link to hotfile.com. To increase its number of members, Hotfile paid users to upload the most popular content to its servers and asked that the users promote their links. Hotfile's affiliate program, for example, paid those uploading files cash when the file was downloaded 1000 times. The complaint alleged that, as a result of their popularity, copyright-infringing files constituted the bulk of files downloaded through Hotfile, Hotfile's business encouraged persons to upload material with copyright protection, and Hotfile understood the consequences of its business model.[176]

The defendants filed a motion to dismiss the plaintiff's claims for direct and secondary liability for copyright infringement. The court granted the motion as to direct infringement, invoking the requirement of Netcom that there must be some volitional act on the part of the defendant in making the copies in order to establish direct liability. Here the hotfile.com web site merely allowed users to upload and download copyrighted material without volitional conduct on the part of the defendants.[177] The court found unpersuasive two cases relied on by the plaintiffs, the Mp3tunes[178] and Usenet.com[179] cases, to support their argument that the

---

[173] Id. at *1-3 & 15-18.

[174] 798 F. Supp. 2d 1303 (S.D. Fla. 2011).

[175] Id. at 1306.

[176] Id. at 1306-07.

[177] Id. at 1307-08.

[178] Capitol Records, Inc. v. Mp3Tunes, LLC, 2009 U.S. Dist. LEXIS 96521 (S.D.N.Y. Oct. 16, 2009), which held, without much analysis, that a company's knowledge of massive infringement plausibly alleged volitional conduct.

[179] Arista Records LLC v. Usenet.com, Inc. 633 F. Supp. 2d 124 (S.D.N.Y. 2009), which held that a company, having a policy encouraging infringement plus the ability to stop that infringement, was liable for direct copyright infringement.

defendants, by creating a plan that induced infringement, were liable for direct infringement. Although the court noted that the two cases supported the plaintiffs' argument, the court stated that it believed the cases were not correctly decided. The court also rejected the plaintiffs' attempt to distinguish Netcom on the ground that it applied only where a defendant violated a copyright holder's right to reproduce – but not to distribute. The court noted that the Netcom court stated it considered the copyright holder's right to distribution in its analysis. The court also rejected the plaintiffs' argument that they had alleged a volitional act in the form of Hotfile's making of additional copies once the copyrighted material was uploaded to its server, because courts had repeatedly held that the automatic conduct of software, unaided by human intervention, is not volitional.[180]

The court found, however, that the plaintiffs had adequately pled claims for inducement, contributory, and vicarious liability. Inducement and contributory infringement were adequately pled by allegations that hotfile.com was a web site that Hotfile used to promote copyright infringement and that Hotfile took affirmative steps to foster the infringement by creating a structured business model that encouraged users to commit copyright infringement. Vicarious liability was adequately pled by allegations that Hotfile had complete control over the servers that users employed to infringe, had the technology necessary to stop the infringement, refused to stop the massive infringement, and actually encouraged the infringement because the infringement increased its profits.[181]

(r) Perfect 10 v. Megaupload

In Perfect 10, Inc. v. Megaupload Limited,[182] the defendant operated a file storage service through the "Megaupload" web site (among others), which allowed users to upload files. After upload, the web site created a unique URL to the file, and anyone with the URL could then download the file from Megaupload's servers. Both Megaupload and its users disseminated URLs for various files throughout the Internet. In order to view, copy, or download files from the web sites without a waiting period, users were required to pay a membership fee. The plaintiff sued the defendants for direct and secondary copyright infringement because thousands of its copyrighted photographs were uploaded to Megaupload and available for downloading. Those photos contained copyright notices and were labeled "Perfect 10" or "Perfect-10." The complaint alleged that Megaupload depended on, and provided substantial payouts to, affiliate web sites who catalogued the URLs providing access to a mass of pirated content on Megaupload's servers, and that Megaupload encouraged its users to upload materials through a rewards program. The defendant moved to dismiss the direct and secondary liability claims.[183]

With respect to the direct infringement claim, the court noted that under Netcom, an important element of direct infringement is volitional conduct, and the element of volitional

---

[180] Hotfile, 798 F. Supp. 2d at 1307-09.

[181] Id. at 1301.

[182] 2011 U.S. Dist. LEXIS 81931 (July 27, 2011).

[183] Id. at *3-5.

conduct applies to all exclusive rights under the copyright act.[184] Drawing all reasonable inferences in the plaintiff's favor, the court found that the plaintiff had adequately pled a claim for direct infringement:

> Megaupload serves as more than a passive conduit, and more than a mere "file storage" company: it has created distinct websites, presumably in an effort to streamline users' access to different types of media (e.g., megaporn.com, megavideo.com); it encourages and, in some cases pays, its users to upload vast amounts of popular media through its Rewards Programs; it disseminates URLs for various files throughout the internet; it provides payouts to affiliate websites who maintain a catalogue of all available files; and, last, at a minimum, it is plausibly aware of the ongoing, rampant infringement taking place on its websites. Taken together, Perfect 10 has adequately alleged Megaupload has engaged in volitional conduct sufficient to hold it liable for direct infringement.[185]

The court also concluded that claims of contributory infringement were adequately pled. Knowledge of infringement had been adequately pled because, in addition to takedown notices (which the court noted doubt as to whether takedown notices automatically imply knowledge), many of the allegations giving rise to direct infringement also gave rise to knowledge. The plaintiff had also adequately pled a material contribution to infringement in that Megaupload encouraged, and in some cases, paid its users to upload vast amounts of popular media through its rewards programs, disseminated URLs that provided access to such media, and provided payouts to affiliates who catalogued the URLs for all available media.[186]

The court concluded, however, that the plaintiff had not adequately pled claims of vicarious liability, because it did not allege facts suggesting that Megaupload had the right and ability to supervise infringing conduct of its third party users. Accordingly, the court dismissed the claim for vicarious liability without prejudice.[187]

(s) Wolk v. Kodak Imaging Network

This case, which refused to find direct liability on the part of Kodak Imaging Network for lack of volitional conduct, is discussed in Section III.C.6(b)(1)(iii).q below.

(t) Fox Broadcasting v. Dish Network

Fox sought a preliminary injunction against Dish Network, which had a contract with Fox granting it the right to retransmit Fox broadcast material to its subscribers, for offering a high definition digital video recorder called the "Hopper" and two associated services called "PrimeTime Anywhere" (PTAT) and "AutoHop." Because the Hopper was designed to service

---

184 Id. at *10.

185 Id. at *11-12 (citations to the complaint omitted).

186 Id. at *16-17.

187 Id. at *19.

multiple televisions, it had three tuners and a two-terabyte hard drive, which allowed Hopper users to watch or record on three different television stations at once. The Hopper had the additional unique capability of streaming all four of the major television networks on a single satellite transponder, which allowed a user to watch or record all four network broadcasts while leaving the other two tuners available for recording non-network programs or watching them on other television sets equipped with additional set top boxes. The PTAT feature allowed subscribers to set a single timer on the Hopper to record all primetime programming on any of the four major broadcast networks each night of the week. Dish determined the start and end time of the primetime block each night. In order to use PTAT, the user had to specifically enable it from the main menu. Once enabled, a screen appeared allowing the user to choose to disable recordings of certain networks on certain days of the week. If the user did not select otherwise, the default settings caused the Hopper to record the entire primetime window on all four of the major networks every day of the week. A user could begin watching the recorded programs immediately after PTAT started recording, and could cancel a particular PTAT recording on a given day up until 20 minutes before primetime programming began. All PTAT recordings were stored locally on the Hopper in users' homes. Unless the user selected otherwise, PTAT recordings were automatically deleted after eight days. The Hopper also worked with the "Sling Adapter," which allowed subscribers to view Hopper content on their computers and mobile devices via the Internet.[188]

AutoHop was a feature that allowed users to skip commercials in PTAT recordings with the click of their remote control. If AutoHop was available for a particular PTAT program, the user was given the option to enable it for that show. If the user enabled AutoHop, the Hopper would automatically skip commercial breaks during that program. Markers inserted into the PTAT recordings to mark the beginning and end of the commercials were checked manually by technicians who viewed a separate quality assurance ("QA") copy of the recording made by Dish and stored on its servers. The technician would view the QA recording, fast-forwarding through the program itself to the commercial breaks, to ensure that the markings were accurate and no portion of the program was cut off. If the QA copies revealed an error in the marking process, technicians could correct the error on a later broadcast to ensure that AutoHop functioned properly for users who enabled it. If there was not enough time to correct a marking error before the last broadcast ended, then AutoHop would not be available for that particular show.[189]

Fox sought a preliminary injunction against the PTAT and AutoHop functions on grounds of copyright infringement. The court turned first to whether Fox could have secondary liability for any infringing acts of its subscribers. Applying the Supreme Court's Sony case, the court noted that nothing suggested Hopper users were using the PTAT copies for anything other than time-shifting in their homes or on mobile devices, an activity determined to be a fair use in

---

[188] Fox Broadcasting Co. v. Dish Network, L.C.C., 2012 U.S. Dist. LEXIS 169112 at *6, 8-13 (C.D. Cal. Nov. 7, 2012).

[189] Id. at *15-16.

Sony. Because there was therefore no direct infringement on the part of PTAT users, Dish could not have secondary copyright liability.[190]

The court then turned to whether Dish could have liability for direct copyright infringement for the making of the PTAT copies or the QA copies of Fox's programming. Citing the Netcom and Cablevision cases, the court concluded that it was Dish's subscribers, and not Dish itself, who were making the copies. The court considered the various ways in which Fox attempted to distinguish the facts at hand from the Cablevision case:

– Dish decided which networks were available on PTAT and defaulted the PTAT settings to record all four networks. Those decisions, while undoubtedly discretionary authority that Dish maintained, were similar to Cablevision's unfettered discretion in selecting the programming available for recording. But Dish had no control over what programs Fox and the other networks chose to make available during primetime, and Dish recorded the programs only if the user made the initial decision to enable PTAT. The court concluded that the default settings did not support Fox's contention that Dish, rather than its users, made the copies.

– Dish decided the length of time each copy was available for viewing before automatic deletion after a certain number of days and a user could neither delete nor preserve the original PTAT copy before that time. The court was not convinced, however, that this control, being exercised *after* the creation of the copies, was relevant to whether Dish caused the copies to be made in the first place, which were created only upon the users choosing to enable PTAT.

– Dish decided when primetime recordings started and ended each night and the user could not stop a copy from being made during the copying process, but had to wait until the recording ended before disabling the link to it on the hard drive. The court acknowledged that these limitations on user choice evinced Dish's greater participation in the copying process, but nevertheless found that such involvement was not materially different from an Internet service provider that copied a file in automatic response to a user's request, as in the Loopnet case. Although Dish defined some of the parameters of copyright for time-shifting purposes, it was ultimately the user who caused the copy to be made by enabling PTAT.

Accordingly, the court ruled that it was the user, not Dish, who was the most significant and important cause of the copy, and Fox had therefore not established a likelihood of success on the merits of its claim that by Dish directly infringed on its exclusive right to reproduction through PTAT.[191]

The court next ruled that Dish's making of the QA copies did not constitute a fair use under the application of the four statutory fair use factors. Under the first factor, while the QA copies themselves were not sold or otherwise monetized, they were made for the commercial purpose of providing a high quality commercial skipping product that more users would want to activate. The copies were not transformative because they did not alter their originals with new

---

[190] Id. at *19-22.

[191] Id. at *24-35.

expression, meaning or message. The first factor therefore weighed against fair use. The creative nature of the copyrighted works copied entitled them to heightened protection and cut against fair use under the second factor. The third factor also weighed against Dish because the entire works were copied, although the court noted that the third factor was of considerably less weight than the other factors due to the limited nature of the ultimate use.[192]

Turning to the fourth factor, the court noted that the QA copies were used to perfect the functioning of AutoHop, a service that, standing alone, did not infringe. However, the record showed that a market existed for the right to copy and use Fox programs, given that Fox licensed copies of its programs to companies including Hulu, Netflix, iTunes, and Amazon to offer viewers the Fox programs in various formats. In fact, the record suggested that Dish chose to offer AutoHop to its subscribers in order to compete with other providers who paid for the rights to use copies of the Fox programs through licensing agreements. By making an unauthorized copy for which it had not paid and using it for AutoHop, Dish harmed Fox's opportunity to negotiate a value for those copies and also inhibited Fox's ability to enter into similar licensing agreements with others in the future by making the copies less valuable. Therefore, the fourth factor also cut against Dish, and the court ruled that the QA copies did not constitute a fair use. The fact that consumers ultimately used AutoHop in conjunction with PTAT for private home use, a fair use under Sony, did not render the intermediate copies themselves a fair use as well.[193]

The court then considered whether Dish was liable for violation of Fox's distribution right and found that it was not. Citing the Perfect 10 v. Amazon case,[194] the court noted that infringement of the distribution right requires actual dissemination of a copy by sale or other transfer of ownership, or by rental, lease, or lending. Here, a PTAT-enabled Hopper recorded primetime programming locally and, at most that local copy was disseminated within a single household. PTAT and AutoHop therefore did not involve any actual distribution of unauthorized copies, so the court concluded that Fox had not established a likelihood of success on the merits of its distribution claim.[195]

Lastly, the court turned to a consideration of whether a preliminary injunction should issue based on the court's finding that the QA copies were infringing.[196] The court concluded that no preliminary injunction should issue because Fox had not established a likelihood of irreparable harm if Dish were not enjoined from making and using the QA copies. The record suggested that the extent of harmed caused by the QA copies was calculable in money damages. The fact that Fox had licensing agreements with other companies showed that *copies* of the Fox programs had a market value that other companies already paid in exchange for the right to use the copies. Although Fox had submitted evidence that some irreparable harms, such as loss of

---

192 Id. at *39-41.

193 Id. at *41-44.

194 Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

195 Fox Broadcasting, 2012 U.S. Dist. LEXIS 169112 at *45-47.

196 The court observed that "neither the marking announcements nor the ad-skipping effect of AutoHop implicates any copyright interest …." Id. at 57.

control over its copyrighted works and loss of advertising revenue, might stem from the ad-skipping use to which the QA copies were put, the record did not show that those harms flowed from the QA copies themselves. Rather, if those harms were to materialize, they would be a result of the ad-skipping itself, which did not constitute copyright infringement. The court therefore concluded that any injury was compensable with money damages and did not support a finding of irreparable harm.[197]

(u) Summary of Case Law

To sum up, under a majority of the cases decided to date, a direct volitional act of some kind is required for liability for direct copyright infringement. The MAPHIA and Sabella, Cablevision, and Hotfile cases suggest that it is insufficient for direct liability for an actor such as a BBS or web site operator to have provided only encouragement of the acts (such as initial uploading of unauthorized copies) that lead to infringement. Similarly, the CoStar, Ellison and Perfect 10 v. Cybernet Ventures cases suggest that an OSP will not have direct liability for infringing material posted on its service by users or available through its service on third party sites where the OSP has not encouraged such posting or had advance knowledge of it. And the Field v. Google and Parker v. Google cases hold that a search engine operator will not have direct liability for serving up cached copies of copyrighted materials in an automated response to user requests based on search results. Rather, for direct liability the defendant must have engaged in the very acts of infringement themselves in a volitional way.

However, the Frena, Webbworld, Sanfilippo, Quantum Systems and Megaupload cases (as well as the Hardenburgh and Webbworld cases discussed in Section II.C below with respect to the public display and distribution rights) suggest that where an actor such as a BBS operator or web site operator has some form of substantial direct involvement in the anticipated acts that lead to infringement or in the infringing acts themselves (such as resale of the infringing material), there may be a finding of sufficient volitional activity to impose direct liability. And the Arista Records v. Usenet.com case suggests that direct liability for violation of the distribution right can be premised on active promotion of sharing of illicit files coupled with close control over what types of material are featured for distribution in the first instance. Thus, to establish direct liability for infringement one must look at whether the defendant participated in the very acts of infringement themselves.

As discussed in Section III.C below, the Digital Millennium Copyright Act[198](referred to herein as the "DMCA") defines certain safe harbors against liability for OSPs who act as merely passive conduits for infringing information and without knowledge of the infringement. An OSP must meet quite specific detailed requirements to qualify for the safe harbors relating to acting as a passive conduit and innocent storage of infringing information. Where an OSP does not qualify for these safe harbors, the standards under the case law discussed above will apply to determine liability.

---

[197] Id. at *56-60.

[198] Pub. L. No. 105-304, 112 Stat. 2860 (1998).

5. The Reproduction Right Under WIPO Implementing Legislation

(a) United States Legislation

Four bills were introduced in Congress to implement the WIPO treaties. Two of them, neither of which were ultimately enacted, would have attempted to clarify the issue of whether interim copies made during the course of transmission infringe the reproduction right. The bill that was adopted – The Digital Millennium Copyright Act – contains nothing explicitly addressing the scope of the reproduction right in a digital environment.

(1) The Digital Millennium Copyright Act

The DMCA was signed into law by President Clinton on Oct. 28, 1998. It is essentially an enactment of H.R. 2281, introduced in the House in July of 1997 by Rep. Howard Coble, and its nearly identical counterpart in the Senate, S. 1121, introduced by Sen. Orrin Hatch also in July of 1997, which was later combined with another bill and, as combined, denominated S. 2037. Both H.R. 2281 and S. 1121 were introduced with the support of the Clinton administration.

Title I of the DMCA, entitled the "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998" and comprised of Sections 101 through 105, implements the WIPO treaties. Title I takes a minimalist approach to implementing the requirements of the WIPO treaties. The Clinton administration took the view that most of the enhanced copyright protections set forth in the treaties were already available under United States law, so that no major changes to U.S. law were believed necessary to implement the treaties.

Specifically, the DMCA addresses only the requirements of Arts. 11 and 12 of the WIPO Copyright Treaty, and of Arts. 18 and 19 of the WIPO Performances and Phonograms Treaty, to provide adequate legal protection and effective legal remedies against (i) the circumvention of effective technological measures that are used by rights holders to restrict unauthorized acts with respect to their protected works, and (ii) the removal or alteration of any electronic rights management information (information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work), or the distribution or communication to the public of copies of works knowing that the electronic rights management information has been removed or altered. The specific provisions of these bills are discussed in further detail below. These bills contain nothing addressing the reproduction right or how that right relates to the digital environment.

(2) Legislation Not Adopted

An alternative bill to implement the WIPO treaties, S. 1146, entitled the "Digital Copyright Clarification and Technology Education Act of 1997," was introduced on Sept. 3, 1997 by Sen. John Ashcroft. Like the DMCA, S. 1146 contained language to implement prohibitions against the circumvention of technologies to prevent unauthorized access to copyrighted works and to provide electronic rights management information about a work, although it adopted a different approach to doing so than the DMCA, as discussed further below.

S. 1146 also contained, however, a much broader package of copyright-related measures. With respect to the reproduction right, S. 1146 would have clarified that ephemeral copies of a work in digital form that are incidental to the operation of a device in the ordinary course of lawful use of the work do not infringe the reproduction right. Specifically, S. 1146 would have added a new subsection (b) to Section 117 of the copyright statute to read as follows:

> (b) Notwithstanding the provisions of section 106, it is not an infringement to make a copy of a work in a digital format if such copying –
>
> (1) is incidental to the operation of a device in the course of the use of a work otherwise lawful under this title; and
>
> (2) does not conflict with the normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

The proposed new clause (b)(1) was similar to the right granted in the existing Section 117 of the copyright statute with respect to computer programs, which permits the making of copies of the program "as an essential step in the utilization of the computer program in conjunction with a machine."[199] Clause (b)(1) would have extended this right to the otherwise lawful use of other types of works in a digital format, to the extent that copying is necessary for such use. It would seem to have covered activities such as the loading of a musical work into memory in conjunction with playing the work, the incidental copies of a movie or other work ordered on demand that are made in memory in the course of the downloading and viewing of the movie, and the various interim copies of a work that are made in node computers in the routine course of an authorized transmission of the work through the Internet.

The limiting language contained in new clause (b)(2) was drawn directly from the WIPO treaties themselves. Specifically, Article 10 of the WIPO Copyright Treaty permits treaty signatories to provide for limitations of or exceptions to the rights granted under the treaty "in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author." The scope of reach of this language is obviously not self evident, and the boundaries of this exception to the reproduction right are therefore not entirely clear. However, the exception should apply to at least the most common instances in which incidental copies must be made in the course of an authorized use of a digital work, including in the course of an authorized transmission of that work through a network.

Another bill introduced into Congress to implement the WIPO copyright treaties was H.R. 3048, entitled the "Digital Era Copyright Enhancement Act," which was introduced on Nov. 14, 1997 by Rep. Rick Boucher. With respect to the reproduction right, H.R. 3048 contained an identical amendment to Section 117 as S. 1146 that would have permitted the making of incidental copies of a work in digital form in conjunction with the operation of a device in the ordinary course of lawful use of the work.

---

[199] 17 U.S.C. § 117.

The clarifying amendment to Section 117 concerning the reproduction right that these alternative bills would have set up was not ultimately adopted by Congress in the DMCA.

(b) The European Copyright Directive

The European Copyright Directive contains strong statements of copyright owners' rights to control the reproduction, distribution and presentation of their works online. The European Copyright Directive requires legislative action by EC member states with respect to four rights: the reproduction right,[200] the communication to the public right,[201] the distribution right,[202] and protection against the circumvention or abuse of electronic management and protection systems.[203]

With respect to the reproduction right, the European Copyright Directive adopts essentially the same broad language of proposed Article 7(1) of the WIPO Copyright Treaty that provoked so much controversy and was ultimately deleted from the WIPO Copyright Treaty. Specifically, Article 2 of the European Copyright Directive provides that member states must "provide the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form" of copyrighted works. The extension of the reproduction right to "direct or indirect" and "temporary or permanent" reproductions would seem to cover even ephemeral copies of a work made during the course of transmission or use of a copyrighted work in an online context. Indeed, the official commentary to Article 2 notes that the definition of the reproduction right covers "all relevant acts of reproduction, whether on-line or off-line, in material or immaterial form."[204] The commentary also appears to adopt the approach of the MAI case in recognizing copies of a work in RAM as falling within the reproduction right: "The result of a reproduction may be a tangible permanent copy, like a book, but it may just as well be a non-visible temporary copy of the work in the working memory of a computer."[205]

To provide counterbalance, however, Article 5(1) of the European Copyright Directive provides an automatic exemption from the reproduction right for "[t]emporary acts of reproduction … which are transient or incidental, which are an integral and essential part of a technological process whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance." This provision is very similar to the new clause (b) that would have been added to Section 117 of the U.S. copyright statute under S. 1146 and H.R. 3048 (discussed in Section II.A.5(a)(2) above). The Article 5(1) exception would appear to cover the store and forward procedure adopted by routers and the RAM copy produced

---

200 European Copyright Directive, art. 2.

201 Id. art. 3.

202 Id. art. 4.

203 Id. arts. 6-7.

204 Commentary to Art. 2, ¶ 2.

205 Id. ¶ 3.

as a result of browsing at least by a private user (whether browsing for a commercial purpose would have "independent economic significance" is unclear).[206] The exception does not apply to computer programs or databases because they are separately regulated in other Directives.[207]

Thus, the European Copyright Directive adopts an approach that affords the reproduction right a very broad inherent scope, but provides an explicit and automatic exemption for copies that are made incidental to the use[208] of a work through a technological process, such as transmission through a network or loading into memory for viewing or playing of the work. Indeed, Recital (33) of the European Copyright Directive notes that the exception of Article 5(1) "should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information."

According to Recital (32) of the European Copyright Directive, the final Directive, unlike its predecessor drafts, opted for an approach of listing "an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public." These exceptions and limitations are enumerated in Articles 5(2) and 5(3). The exceptions and limitations in Article 5(2) apply only to the reproduction right, whereas the exceptions and limitations in Article 5(3) apply to both the reproduction right and the right of communication to the public.

Under Article 5(2), member states may provide for exceptions or limitations to the reproduction right in the following cases:

> (a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic techniques or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;
>
> (b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly or indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;

---

[206] Justin Harrington & Tina Berking, "Some Controversial Aspects of the EU Copyright Directive (Directive 2001/29/EC)," *Cyberspace Lawyer*, Jan. 2003, at 2, 3-4. The Electronic Commerce Directive contains exemptions in respect of hosting, caching and acting as a mere conduit. Id. at 4.

[207] David Schollenberger, "Entertainment Without Borders" (Mar. 2003), at 9 (seminar paper on file with the author).

[208] An earlier version of Art. 5(1) provided that the use of the work must be "authorized or otherwise permitted by law." A copy of an earlier version of the European Copyright Directive and comments may be found at www.bna.com/e-law/docs/ecdraft.html (last modified Dec. 2, 1997).

(c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;

(d) in respect of ephemeral recordings of works made by broadcasting organizations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the ground of their exceptional documentary character, be permitted;

(e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

It is interesting to note that the majority of these exceptions are conditioned upon the rightholders receiving fair compensation, and they cover only copying that is for non-commercial purposes. Exception (b) is of particular interest, for it provides a right for natural persons to make copies for private use and for purposes that are neither directly or indirectly commercial, provided the rightholders receive fair compensation. Presumably the exception would apply where a natural person has purchased a copy of a copyrighted work, thereby providing fair compensation to the rightholders, and thereafter makes additional copies for personal, noncommercial uses – e.g., by making a copy of one's purchased music CD onto a cassette for use in one's car. The drafters of the European Copyright Directive deemed this right of private use to be of such significance that under Article 6(4), member states are permitted to take measures to ensure that beneficiaries of this right are able to take advantage of it, "unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions."[209]

The right of private use contained in Article 5(2)(b) is similar to a right afforded in the United States under the Audio Home Recording Act (AHRA), 17 U.S.C. § 1008, which provides, "No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings." This statute is discussed in detail in Section II.A.7 below, and in Section III.C.2.(c)(1) below in connection with the Napster litigations. Napster, Inc., the operator of a service that enabled subscribers to share music files in MP3 audio format with one another, asserted the AHRA as a defense to an allegation by copyright owners that it was contributorily and vicariously liable for the unauthorized sharing of copyrighted sound recordings through its service. Napster argued that the AHRA permitted its subscribers to share

[209] Under the last paragraph of Article 6(4), this right of member states to take measures to ensure that beneficiaries of the right of private use are able to take advantage of it does not apply "to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them."

such sound recordings because they were shared for personal use by its subscribers. As discussed in detail below, the courts rejected this argument.

Perhaps in response to online systems like Napster, the drafters of the European Copyright Directive seem to have been concerned that the exception for personal use in Article 5(2)(b) not be construed to permit the unauthorized sharing of copyrighted works in digital form through online systems, at least without compensation to the rightholders affected. Specifically, Recital (38) of the European Copyright Directive states:

> Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audio-visual material for private use, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. … Digital private copying is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be make in certain respects between them.

In addition, the drafters of the European Copyright Directive seemed to contemplate that "intermediaries" providing services through which infringing activities take place online should be subject to injunctive relief to stop unauthorized transmissions of copyrighted works through its service. Recital (58) of the European Copyright Directive provides:

> In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

Under Article 5(3), member states may provide for further exceptions or limitations to the reproduction right and the right of communication to the public in the following cases:

> (a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this proves impossible, and to the extent justified by the non-commercial purpose to be achieved;
>
> (b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;

(c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author's name, is indicated, unless this proves impossible;

(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, and that, unless this proves impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;

(e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

(f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this proves impossible;

(g) use during religious celebrations or official celebrations organized by a public authority;

(h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;

(i) incidental inclusion of a work or other subject-matter in other material;

(j) use for the purpose of advertising public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;

(k) use for the purpose of caricature, parody or pastiche;

(l) use in connection with the demonstration or repair of equipment;

(m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;

(n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of [Article 5(2)] of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;

(o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

Note that, unlike many of the exceptions of Article 5(2), the exceptions of Article 5(3) are not conditioned upon fair compensation to the rightholders.

6. Peer-to-Peer File Sharing

(a) BMG Music v. Gonzalez

In BMG Music v. Gonzalez,[210] defendant Cecilia Gonzalez sought to defend her downloading of more than 1370 copyrighted songs through the Kazaa file-sharing network by arguing that her actions should fall under the fair use doctrine on the theory that she was just sampling the music to determine what she liked sufficiently to buy at retail.[211] The Seventh Circuit rejected this argument out of hand. Focusing principally on the fourth fair use factor – the effect of the use upon the potential market for or value of the copyrighted work – Judge Easterbrook noted that as file sharing had increased over the last four years, sales of recorded music had dropped by approximately 30%. Although other economic factors may have contributed, he noted that the events were likely related.[212]

He further noted that rights holders had economic interests beyond selling compact discs containing collections of works – specifically, there was also a market in ways to introduce potential consumers to music. Noting that many radio stations stream their content over the Internet, paying a fee for the right to do so, he noted that Gonzalez could have listened to streaming music to sample songs for purchase, and had she done so, the rights holders would have received royalties from the broadcasters.[213] Rejecting the proffered fair use defense, Judge Easterbrook stated, "Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying 'fair use' if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute."[214]

The plaintiffs sought statutory damages for Gonzalez' unauthorized copying, seeking the minimum amount of $750 per work infringed. Gonzalez sought to reduce the award below the $750 minimum by arguing under Section 504(c)(2) that she was not aware and had no reason to believe that her acts constituted infringement of copyright. The district court rejected the request under the provisions of Section 402(d), which provides that if a valid notice of copyright appears

---

[210] 430 F.3d 999 (7th Cir. 2005).

[211] Id. at 889-90.

[212] Id. at 890.

[213] Id. at 891.

[214] Id.

on the phonorecords to which a defendant had access, then no weight shall be given to the defendant's interposition of a defense based on innocent infringement in mitigation of actual or statutory damages.[215] Gonzalez sought to avoid Section 402(d) by arguing that there were no copyright notices on the data she downloaded. The court rejected this argument: "She downloaded data rather than discs, and the data lacked copyright notices, but the statutory question is whether 'access' to legitimate works was available rather than whether infringers earlier in the chain attached copyright notices to the pirated works. Gonzalez readily could have learned, had she inquired, that the music was under copyright."[216]

(b) Columbia Pictures v. Bunnell

In Columbia Pictures Industries, Inc. v. Bunnell,[217] the court entered judgment against defendant Valence Media LLC, operator of the web site at www.torrentspy.com, for willful inducement of copyright infringement, contributory copyright infringement, and vicarious copyright infringement. The court awarded the plaintiffs statutory damages of $30,000 per infringement for each of 3,699 infringements shown, for a total judgment of $110,970,000. The court also issued a permanent injunction enjoining the defendants from encouraging, inducing, or knowingly contributing to the reproduction, download, distribution, upload, or public performance or display of any copyrighted work at issue, and from making available for reproduction, download, distribution, upload, or public performance or display any such work.[218]

(c) Sony BMG Music Entertainment v. Tenenbaum

In Sony BMG Music Entertainment v. Tenenbaum,[219] the court rejected a broadside fair use defense for the file-sharing by a college sophomore, Joel Tenenbaum, of 30 copyrighted songs belonging to the plaintiffs. Describing the defense raised by the defendant's counsel as "truly chaotic,"[220] the court noted that it represented a version of fair use so broad that it would excuse all file sharing for private enjoyment. As the court described counsel's defense, "a defendant just needs to show that he did not make money from the files he downloaded or distributed – i.e., that his use was 'non-commercial' – in order to put his fair use defense before a

---

215 Id. at 891-92.

216 Id. at 892. Gonzalez also challenged the district court's award of the $750 amount on summary judgment, arguing that the choice of amount is a question for the jury. The Seventh Circuit noted that, although a suit for statutory damages under Section 504(c) is a suit at law to which the seventh amendment applies, this does not mean that a jury must resolve every dispute. When there are no disputes of material fact, a court may enter summary judgment without transgressing the Constitution. The court noted that Gonzalez had argued for the minimum amount of $750 per song and the plaintiffs had been content with that amount, which the district court then awarded on summary judgment. Id.

217 2008 U.S. Dist. LEXIS 63227 (C.D. Cal. July 10, 2008).

218 Id. at *1-3.

219 672 F. Supp. 2d 217 (D. Mass. 2009), rev'd, 660 F.3d 487 (1st Cir. 2011), cert. denied, 132 S. Ct. 2431 (2012).

220 Id. at 220.

jury. Beyond that threshold, the matter belongs entirely to the jury, which is entitled to consider any and all factors touching on its innate sense of fairness – nothing more and nothing less."[221]

The court first turned to the threshold issue of whether fair use is an equitable defense. Noting that a number of courts had suggested that it is, the court nevertheless opined that even if fair use is an entirely equitable defense, it is not clear that its determination requires a jury trial, because judges, not juries, traditionally resolve equitable defenses. However, given that two leading copyright historians had suggested that the equitable label may be a misnomer, and because neither party pressed the point, the court assumed that fair use is a jury question, without resolving the question of the equitable origins of the defense. But because fair use is ultimately a legal question, the court noted that, in the face of the plaintiff's motion for summary judgment on the fair use issue, the defendant could put the defense to a jury only if he showed through specific, credible evidence that the facts relevant to that legal analysis were in dispute. The defendant had failed to do so.[222]

Turning to an application of the four fair use factors, the court found that the first factor – purpose and character of the use – favored the plaintiffs. The court rejected the defendant's binary distinction between "commercial" and "non-commercial" uses under the first factor, noting that the purpose and character of a use must be classified along a spectrum that ranges from pure, large-scale profit-seeking to uses that advance important public goals, like those recognized in the statute. The defendant's file sharing fell somewhere in between. Although the court was not willing to label it "commercial," as the plaintiffs urged, the court ruled that because the use was not accompanied by any public benefit or transformative purpose, the first factor cut against fair use.[223] The second factor – nature of the copyrighted work – also cut against fair use because musical works command robust copyright protection.[224]

The defendant argued that the third factor – portion of the work used – cut against the plaintiffs because he was alleged to have downloaded only individual songs, but not full albums, and it was the albums in which the plaintiffs registered their copyrights, while the individual songs were works made for hire. The court rejected this argument, noting that under existing file sharing case law, individual songs were regularly treated as the relevant unit for evaluating infringement and fair use of musical works.[225]

With respect to the fourth factor – effect on the potential market for the work – the defendant argued that his file sharing made little economic difference to the plaintiffs because the songs at issue were immensely popular and therefore widely available on file sharing networks. The court rejected this as an improper framework for the analysis. Rather, one must consider the effect on the market of the sum of activity if thousands of others were engaged in

---

[221] Id. at 221.

[222] Id. at 223-24.

[223] Id. at 227-29.

[224] Id. at 229.

[225] Id. at 229-30.

the same conduct. The plaintiffs had provided evidence that the widespread availability of free copies of copyrighted works on the Internet had decreased their sales revenue, and the defendant had offered no affidavits or expert report to disprove or dispute that evidence.[226]

The court's opinion contains a few other interesting observations with respect to the doctrine of fair use as applied to file sharing. First, citing the case of American Geophysical Union v. Texaco Inc.,[227] the court noted that a fair use determination may be affected by the availability or absence of authorized ways to obtain the work in question. The defendant asserted that the emergence of easy-to-use, paid outlets for digital music, such as the iTunes music store, had lagged well behind the advent of file sharing, and this fact should affect the fair use analysis. The court responded that, whatever the availability of authorized digital alternatives was when peer-to-peer networks first because widespread in 1999, it was clear that by August 2004 – when the defendant's file sharing was detected – a commercial market for digital music had fully materialized. In light of that chronology, the unavailability of paid digital music was simply not relevant to the court's application of the fair use doctrine.[228]

Although granting the plaintiffs' motion for summary judgment on the defendant's fair use defense, the court concluded with the following two interesting dicta:

– "[T]he Court does not believe the law is so monolithic, or the principles of fair use so narrow that they could not encompass some instances of file sharing copyrighted works. This Court, unlike others that have spoken on the subject, can envision a scenario in which a defendant sued for file sharing could assert a plausible fair use defense – for example, the defendant who 'deleted the mp3 files after sampling them, or created mp3 files exclusively for space-shifting purposes from audio CDs they had previously purchased.' (Berkman Center Br. at 36-37, document # 177-3.) The Court can also envision a fair use defense for a defendant who shared files during a period before the law concerning file sharing was clear and paid outlets were readily available. … A defendant who shared files online during this interregnum, sampling the new technology and its possibilities, but later shifted to paid outlets once the law because clear and authorized sources available, would present a strong case for fair use."[229]

– "As this Court has previously noted, it is very, very concerned that there is a deep potential for injustice in the Copyright Act as it is currently written. It urges – no implores – Congress to amend the statute to reflect the realities of file sharing. There is something wrong with a law that routinely threatens teenagers and students with astronomical penalties for an activity whose implications they may not have fully understood. The injury to the copyright holder may be real, and even substantial, but, under the statute, the record companies do not even have to prove actual damage."[230]

---

[226] Id. at 230-31.

[227] 60 F.3d 913, 931 (2d Cir. 1994).

[228] Tenenbaum, 672 F. Supp. 2d at 235-36.

[229] Id. at 237-38.

[230] Id. at 237.

Following a trial, the jury found that Tenenbaum had willfully infringed the plaintiffs' copyrights and imposed statutory damages of $22,500 per song, yielding a total award of $675,000.[231] In response to the defendant's motion for a new trial or remitter, the trial court held that an award of that size, given that Tenenbaum reaped no pecuniary reward from the infringement and the infringing acts caused the plaintiffs minimal harm, violated the due process clause of the Constitution as excessive. The court found the award to be far greater than necessary to serve the government's legitimate interests in compensating copyright owners and deterring infringement and that, in fact, it bore no meaningful relationship to those objectives. Accordingly, the court reduced the jury's award to one-tenth the amount, or $2,250 per infringed work (three times the statutory minimum), for a total award of $67,500. The court noted that such amount was still more than the court itself might have awarded in its independent judgment, but the amount was the greatest amount that the Constitution would permit given the facts of the case.[232] The court also reaffirmed its previous ruling rejecting Tenenbaum's fair use defense.[233]

On appeal, the First Circuit reversed, finding that the district court erred when it bypassed Tenenbaum's remittitur arguments based on the excessiveness of statutory damages and reached the constitutional due process issue. The court noted that, under established precedent, a trial court's reduction of compensatory damages must, to avoid *Seventh Amendment* error, allow the plaintiff a new trial. Punitive damage awards, by contrast, may be reduced on due process grounds without offering the plaintiff a new trial without running afoul of the *Seventh Amendment*. In bypassing remittitur and the offer of a new trial, the district court had assumed that statutory damage awards should be treated largely as punitive, not compensatory, awards for *Seventh Amendment* purposes.[234] But the First Circuit found that statutory damages have both a compensatory and punitive element, and further noted that the Supreme Court had ruled in the Feltner case[235] that the *Seventh Amendment* provides a right to a jury trial on all issues pertinent to an award of copyright statutory damages. Given these important *Seventh Amendment* issues, the First Circuit held that the district court had erred in not ordering remittitur, which would have afforded a number of possible outcomes that could have eliminated the constitutional due process issue altogether, or at the very least materially reshaped it – e.g., by altering the amount of the award at issue or even the evidence on which to evaluate whether a particular award was excessive.[236]

The court also rejected the defendant's argument that no statutory damages can be awarded where harm caused by the defendant has not been proved, and that statutory damages

---

231 Sony BMG Music Entertainment v. Tenenbaum, 721 F. Supp. 2d 85, 87 (D. Mass. 2010), rev'd, 2011 U.S. App. LEXIS 19086 at *74-75 (1st Cir. Sept. 16, 2011), cert. denied, 2012 U.S. LEXIS 3908 (U.S. May 21, 2012).

232 Id. at 89-90.

233 Id. at 98-99.

234 Sony BMG Music Entertainment v. Tenenbaum, 660 F.3d 487, 514 (1st Cir. 2011), cert. denied, 132 S. Ct. 2431 (2012).

235 Feltner v. Columbia Pictures Television, Inc., 523 U.S. 340 (1998).

236 Tenenbaum, 660 F.3d at 511, 514-15.

cannot be awarded unless reasonably related to actual damages.[237] The court further rejected a number of challenges to the district court's jury instructions, including a challenge to the instruction that willful infringement means that a defendant had knowledge that his actions constituted copyright infringement or acted with reckless disregard for the copyright holder's rights. The First Circuit joined precedent from sister circuits that had unanimously and routinely found that an infringement is willful under Section 504 if it is knowing or in reckless disregard of the copyright holder's rights.[238]

Accordingly, the court affirmed the finding of liability against Tenenbaum and the injunctive relief, but vacated the district court's due process damages ruling and reversed the reduction of the jury's statutory damages award. The court reinstated the jury's award of damages and remanded for consideration of the defendant's motion for common law remittitur based on excessiveness. If on remand, the district court allowed any reduction through remittitur, the First Circuit ruled that the plaintiffs must be given the choice of a new trial or acceptance of remittitur.[239]

On remand, the district court ruled there was no basis for common law remittitur of the award because it was not grossly excessive, inordinate, shocking to the conscience of the court, or so high that it would be a denial of justice to permit it to stand. Tenenbaum had personally received multiple warnings from various sources across several years about downloading and distributing copyrighted materials, including the fact that his activities could subject him to liability of up to $150,000 per infringement. There was thus ample evidence of willfulness on his part and the need for deterrence based on his blatant contempt of warnings and apparent disregard for the consequences of his actions.[240] Turning next to the legal principles set forth by the First Circuit for evaluating a due process challenge to the award, the court ruled that under the applicable standard – a statutory damages award comports with due process as long as it cannot be said to be so severe and oppressive as to be wholly disproportioned to the offense of obviously unreasonable – the award must withstand a due process challenge. The court concluded that, given the deference afforded Congress' statutory award determination and the public harms it was designed to address, the particular behavior of Tenenbaum in the case, and the fact that the award was not only within the range for willful infringement but also below the limit for non-willful infringement, it could not be said that its amount was either wholly disproportioned to the offense or obviously unreasonable.[241]

---

[237] Id. at 502, 506.

[238] Id. at 507.

[239] Id. at 515.

[240] Sony BMG Music Entertainment v. Tenenbaum, 2012 U.S. Dist. LEXIS 119243 at *6-10 (D. Mass. Aug. 23, 2012).

[241] Id. at *14-18.

(d) Capitol Records v. Thomas-Rasset

The case of Capitol Records, Inc. v. Thomas-Rasset[242] presented a factual situation very similar to that of the Tenenbaum case. Jammie Thomas-Rasset, an individual, was accused by several record companies of copyright infringement for downloading and distributing their copyrighted sound recordings through the Kazaa peer-to-peer filing sharing application. Three jury trials were conducted, each of which resulted in a finding of willful infringement. The first jury returned a statutory damages award of $9,250 per song for a total award of $222,000 based on the defendant's distribution of 24 songs. The court vacated the verdict, however, and granted a new trial based on its conclusion that it had erred in giving a jury instruction which addressed the existence of a "making available" right. The second jury returned a statutory damages award of $80,000 per song for a total award of $1,920,000. Upon motion to set aside the award, the court ruled the award was shocking and unjust and remitted the award to $2,250 per song, or three times the statutory minimum – the same amount as the district judge used in the Tenenbaum case. The plaintiffs then exercised their right to reject remittitur and requested a new trial. The third jury returned a verdict awarding statutory damages in the amount of $62,500 for each song, for a total award of $1,500,000.[243]

The defendant filed a motion to reduce the damages award on the ground that it violated the due process clause of the Constitution because it bore no reasonable relationship to the actual damages caused by the defendant. The court noted that, although in the past it had endeavored to avoid unnecessary adjudication of a constitution issue by relying upon remittitur, based on the plaintiffs' demonstrated refusal to accept a remittitur and the fact that the defendant had not requested remittitur, the court felt it was required to address the constitutionality of the award. Reviewing the relevant legal authority governing the constitutionality of damage awards, the court concluded that, although the due process clause does not require that a statutory damages award be confined or proportioned to the plaintiff's actual loss or damages, the award should bear *some* relation to the actual damages suffered. That was not the case here.[244] "In the case of an individual, like Thomas-Rasset, who infringes by using peer-to-peer networks, the potential gain from infringement is access to free music to build a personal library, which could be purchased, at most, for thousands of dollars, not the possibility of hundreds of thousands – or even millions – of dollars in profits."[245]

Finding a broad legal practice of establishing a treble award as the upper limit permitted in both statutory and common law contexts to address willful or particularly damaging behavior, the court concluded, with citation to the Tenenbaum case, that "in this particular case, involving a first-time willful, consumer infringer who committed illegal song file-sharing for her own

---

242 799 F. Supp. 2d 999 (D. Minn. 2011).

243 Id. at 1002-03.

244 Id. at 1003, *1007-08.

245 Id. at 1010.

personal use, $2,250 per song [three times the minimum statutory amount], for a total award of $54,000, is the maximum award consistent with due process."[246]

After the court issued this ruling in the Thomas-Rasset case, the First Circuit reversed the Tenenbaum case, finding that the district court should not have reached the constitutional issues, but instead should have relied upon the mechanism of remittitur/new trial to address the size of the award. However, it should be noted that the procedural posture in which the district court issued its constitutional ruling in the Thomas-Rasset case, in which a previous rejection of remittitur and election of a new trial had taken place and the defendant had not requested remittitur again, was very different from the procedural posture in which the Tenenbaum court issued its ruling, where the court simply went directly to the constitutional issues in response to the defendant's motion for remittitur or a new trial.

The court in the Thomas-Rasset case issued a permanent injunction prohibiting the defendant from infringing the plaintiffs' copyrights, present or future, in any sound recording. The court rejected, however, the plaintiffs request that the court include language in the injunction barring the defendant from "making available" any of the plaintiffs' sound recordings for distribution:[247]

> Plaintiffs argue that, if Thomas-Rasset makes Plaintiffs' copyrighted works available on a peer-to-peer network, she will have completed all of the steps necessary for her to engage in the same illegal distribution of Plaintiffs' works for which she has already been found liable. Because the Court has held that the Copyright Act does not provide a making-available right, it will not enjoin Thomas-Rasset from making the copyrighted sound recordings available to the public.[248]

On appeal, the plaintiffs argued that the Eighth Circuit should reverse the district court's order granting a new trial and reinstate the first jury's award of $222,000. The plaintiffs also sought a broadened injunction that would forbid Thomas-Rasset from making their copyrighted sound recordings available for distribution. In summary, the Eighth Circuit held that the plaintiffs were entitled to the remedies they sought: damages of $222,000 and a broadened injunction that prohibited Thomas-Rasset to make available the plaintiffs' sound recordings for distribution. However, because the verdicts returned by the second and third juries were sufficient to justify those remedies, the court found it unnecessary to consider the merits of the district court's order granting a new trial after the first verdict. And although the court acknowledged the importance of the "making available" legal issue to the plaintiff recording companies, the court ruled that they were not entitled to an opinion on an issue of law that was

---

[246] Id. at 1013.

[247] Id. at 1016.

[248] Id.

unnecessary for the remedies sought or to a freestanding decision on whether Thomas-Rasset violated the law by making recordings available.[249]

On appeal, Thomas-Rasset lodged no objection to reinstatement of the first verdict, subject to arguments about the constitutionality of the size of the damages. She also offered to acquiesce in the entry of an injunction that would forbid her from making available copyrighted works for distribution, which would render moot the issue whether making works available is part of the distribution right of the copyright holder. In response, the Eighth Circuit observed that it reviews judgments, not decisions on issues. The entitlement of the plaintiffs to the remedies sought – damages of $222,000 and an injunction against making copyrighted works available to the public – were the matters in controversy. That the plaintiffs sought these remedies with the objective of securing a ruling on a particular legal issue did not make that legal issue itself the matter in controversy.[250] "Once the requested remedies are ordered, the desire of the companies for an opinion on the meaning of the Copyright Act, or for a statement that Thomas-Rasset violated the law by making works available, is not sufficient to maintain an Article III case or controversy."[251]

With respect to the scope of the injunction that should have been issued, the Eighth Circuit noted that the district court's refusal to enjoin the making available of the recordings was an error of law, even assuming that the district court was correct in concluding that the distribution right does not include a right of making available, because a district court has authority to issue a broad injunction in cases where a proclivity for unlawful conduct has been shown. Here, Thomas-Rasset's willful infringement and subsequent efforts to conceal her actions showed such a proclivity. Accordingly, the district court erred after the third trial by concluding that the broader injunction requested by the plaintiffs was impermissible as a matter of law. An injunction against making recordings available was lawful and appropriate under the circumstances, even accepting the district court's interpretation of the Copyright Act. Because Thomas-Rasset was not resisting expanding the injunction to include that relief, the Eighth Circuit directed the district court to modify the judgment to include the requested injunction.[252]

With respect to the question of damages, the Eighth Circuit ruled that the district court erred in reducing the third jury's verdict to $2,250 per work, for a total of $54,000, on the ground that this amount was the maximum permitted by the Constitution. Under relevant Supreme Court authority, damages awarded pursuant to a statute violate due process only if they are so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable, and that was not the case here. The court noted that Congress set a statutory damages range for willful copyright infringement of $750 to $150,000 per infringed work, and the $222,000 sought was toward the lower end of that broad range. And it noted that the Supreme Court has rejected the notion that the constitutional inquiry calls for a comparison of an

---

[249] Capitol Records, Inc. v. Thomas-Rasset, 2012 U.S. App. LEXIS 19040 at *3-4 (8th Cir. Sept. 11, 2012).

[250] Id. at *14-15.

[251] Id. at *15.

[252] Id. at *16-19.

award of statutory damages to actual damages caused by the violation – because statutory damages are imposed as a punishment for the violation of a public law, Congress may adjust their amount to the public wrong rather than the private injury, just as if the award were going to the state. Accordingly, the Eighth Circuit concluded that the plaintiffs were entitled to the $222,000 award they sought, and the question whether the district court correctly granted a new trial after the first verdict was moot.[253]

7. The Immunity of the Audio Home Recording Act (AHRA)

The Audio Home Recording Act of 1992 (AHRA)[254] made two major substantive changes to copyright law. First, Subchapter D of the AHRA (Section 1008) immunizes certain noncommercial recording and use of musical recordings in digital or analog form.[255] Section 1008 provides:

> No action may be brought under this title alleging infringement of copyright[256] based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.

Second, Subchapters B and C (Sections 1002-1007) of the AHRA require (i) that any "digital audio recording device" (DARD) conform to the "Serial Copyright Management System" (SCMS), which allows unlimited first generation copies of an original source, but prohibits second generation copies (i.e., copies of a copy), and (ii) that manufacturers and distributors of digital audio recording devices and digital audio recording media (such as DAT tape and recordable CDs) pay royalties and file various notices and statements to indicate payment of those royalties.[257]

(a) The Napster Cases

For a discussion of the rulings with respect to the AHRA in the Napster cases, see Section III.C.2(c)(1) below.

---

253 Id. at *16, 19-29.

254 Pub. L. No. 102-563, 106 Stat. 4244 (1992), codified at 17 U.S.C. §§ 1001-1010.

255 *Nimmer* § 8B.01 (2000).

256 The immunity applies with respect to copyrights in both the sound recordings and any musical compositions embodied therein. Id. § 8B.07[C][2], at 8B-90.

257 Id. §§ 8B.02 & 8B.03 (2000).

(b) The Aimster Case

In In re Aimster Copyright Litigation,[258] the plaintiffs brought copyright infringement claims against the Aimster peer-to-peer file sharing site and its operators for secondary liability for the infringing distribution of the plaintiffs' copyrighted sound recordings. On a motion for a preliminary injunction, the defendants asserted that the plaintiffs had failed to establish that Aimster's users were engaged in direct copyright infringement because the AHRA provided an affirmative defense. The defendants argued that the AHRA shielded them from liability because it was intended to immunize from liability personal use of copyrighted material by protecting all noncommercial copying by consumers of digital and analog musical recordings, relying on the Ninth Circuit's Diamond Multimedia case, discussed in Section III.C.2(c)(1) above.[259]

The court rejected the defendants' reliance on the AHRA, distinguishing the Diamond Multimedia case as follows:

> The facts of the instant case and Diamond Multimedia are markedly different. The activity at issue in the present case is the copying of MP3 files from one user's hard drive onto the hard drive of another user. The Rio in Diamond Multimedia, by contrast, "merely [made] copies in order to render portable, or 'space shift,' those files that already reside on a user's hard drive." 180 F.3d at 1079. The difference is akin to a[n] owner of a compact disc making a copy of the music onto a tape for that owner's sole use while away from home versus the owner making thousands of copies of the compact disk onto a tape for distribution to all of his friends. Furthermore, Diamond Multimedia had nothing whatsoever to do with whether the MP3 files on the owner's computers themselves infringed copyrights. Rather, the decision was limited solely to the infringement issue regarding the act of shifting files from a computer to a personal device and whether that copying was subject to the particular requirements of the AHRA. In short, Defendant's reliance on Diamond Multimedia is entirely misplaced.[260]

(c) Atlantic Recording Corp. v. XM Satellite Radio

In Atlantic Recording Corp. v. XM Satellite Radio, Inc.,[261] numerous record companies sued XM Satellite Radio for contributory, vicarious and inducement copyright liability based on XM's offering of digital radio broadcast services together with special receivers marketed as "XM + MP3" players that allowed subscribers to record, retain and library individually

---

[258] 252 F. Supp. 2d 634 (N.D. Ill. 2002), aff'd on other grounds, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[259] Id. at 648-49.

[260] Id. at 649.

[261] 2007 U.S. Dist. LEXIS 4290 (S.D.N.Y. Jan. 19, 2007).

disaggregated and indexed audio files from XM broadcast performances. The record companies challenged these capabilities as an infringing "digital download delivery service."[262]

XM offered several services specifically to XM + MP3 player users that were the subject of the plaintiff's challenge. First, while listening to XM programming, an XM + MP3 user could instantly record any song at the touch of a button. To facilitate such recording, the XM + MP3 player maintained a short-term buffered copy of every broadcast song a user listened to. As a result, a user could record and store in its entirety any broadcast song he or she heard, even if the user started listening to the song after it began to play.[263]

Second, XM provided XM + MP3 users with playlists from blocks of broadcast programming which had been disaggregated into individual tracks. XM sent users such digital playlists with title and artist information included. The playlists identified all songs broadcast over a particular channel and during a particular period of time. Users could then scroll through a playlist and select which songs to store for future replay, and which to delete. Using this utility, users could hear and store individual songs without actually listening to XM broadcast programming.[264]

Third, XM provided to users a search function together with "ArtistSelect" and "TuneSelect" utilities that made it easy for a user to find out when a requested song was being broadcast. XM would send the listener immediate notice when his or her chosen artists or songs were played on any XM channel. The user could then immediately switch channels and store the requested track onto his or her XM + MP3 player.[265]

Fourth, the XM + MP3 players enabled users to store the approximate equivalent of 1,000 songs recorded from XM broadcasts for as long as the user maintained an XM subscription. Accordingly, the court found that these songs were effectively leased to the XM subscriber for as long as he or she maintained status as a subscriber.[266]

XM brought a motion to dismiss the copyright claims on the ground that it was shielded from infringement actions by Section 1008 of the AHRA because it was acting as a distributor of a digital audio recording device (DARD) immunized by the AHRA. The court first turned to whether the XM + MP3 players constituted a DARD. The plaintiffs argued that they did not, citing the Ninth Circuit's decision in Recording Industry Ass'n of Am. v. Diamond Multimedia Sys.,[267] which held that the Diamond Rio device at issue was not a DARD because it could not make copies from a transmission but instead could make copies only from a computer hard drive, which is exempted under Section 1001(5)(B) of the AHRA. The court distinguished the facts of

---

[262] Id. at *6.

[263] Id. at *9.

[264] Id.

[265] Id. at *9-10.

[266] Id. at *10-11.

[267] 180 F.3d 1072 (9th Cir. 1999).

the Diamond case, noting that the XM + MP3 players could receive from transmissions and were capable of copying without an external computer or computer hard drive.[268] "Accordingly, at this stage of the proceeding, relying on plain meaning statutory interpretation and the definition of a DARD contained in Diamond, until proven otherwise by means of discovery, the Court treats the [XM + MP3 players] as DARDs."[269]

The court next turned to whether the AHRA offered XM complete immunity from the plaintiffs' copyright claims. XM argued that, because it was a distributor of DARDs, it did have such immunity. The court rejected this argument, noting that, while Section 1008 would protect XM from suit for actions based on the distribution of DARDs, such protection would not act as a wholesale, blanket protection for other conduct that XM might be engaged in beyond such distribution. In particular, XM's acts as a satellite radio broadcaster could form a separate basis for copyright liability. Indeed, the plaintiffs' complaint made clear that their claims of copyright infringement were based on XM's acting without authorization as a commercial content delivery provider that delivered permanent digital copies of sound recordings to those devices without permission from the copyright owner.[270]

More specifically, the plaintiffs alleged that, in providing services specific to users of XM + MP3 players, XM was acting outside the scope of its statutory license for broadcast service under Section 114 of the copyright statute – XM's only source of permission to use the plaintiffs' recordings. Such unauthorized acts, according to the plaintiffs, were encroaching directly on their digital download business.[271] The court agreed, finding that by broadcasting and storing copyrighted music on DARDs for later recording by the consumer, XM was acting as a both a broadcaster and a distributor, but was paying license fees only to be a broadcaster.[272]

XM argued that its XM + MP3 player was much like a traditional radio/cassette player and should therefore not be viewed as an improper adjunct to broadcasts. The court rejected this analogy, noting that, in the case of traditional radio/cassette players, the only contact between manufacturers of the devices and users occurred at the point of sale. The court found it quite apparent that the use of a radio/cassette player to record songs played over free radio did not threaten the market for copyrighted works as would the use of a recorder which stores songs from private radio broadcasts on a subscription fee basis. The court further noted that, although XM subscribers might put XM + MP3 players to private use, several court decisions had rejected attempts by for profit users to stand in the shoes of their customers making non-profit or noncommercial uses.[273]

---

[268] XM Satellite, 200 U.S. Dist. LEXIS 4290 at *14 n.4.

[269] Id.

[270] Id. at *16-18.

[271] Id. at *19.

[272] Id. at *20.

[273] Id. at *21-22.

The court therefore denied XM's motion to dismiss: "The Court finds that because of the unique circumstances of XM being both a broadcaster and a DARD distributor and its access to the copyrighted music results from its license to broadcast only, that the alleged conduct of XM in making that music available for consumers to record well beyond the time when broadcast, in violation of its broadcast license, is the basis of the Complaint, and being a distributor of a DARD is not. Thus the AHRA, on these facts, provides no protection to XM merely because they are distributors of a DARD."[274]

B. The Right of Public Performance

Section 106(4) of the copyright statute grants the owner of copyright in a work the exclusive right to perform the work publicly. The right applies to literary, musical, dramatic, and choreographic works, pantomimes, motion pictures and other audiovisual works. It does not apply to pictorial, graphic, sculptural, and architectural works. It also does not apply to sound recordings, other than with respect to public performances by digital transmission,[275] although a public performance of a sound recording may infringe the right of public performance of the underlying musical work that is recorded in the sound recording.

Section 101 provides that to perform a work "publicly" means:

> (1) to perform ... it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or
>
> (2) to transmit or otherwise communicate a performance ... of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.

Because this definition encompasses transmissions of works, it clearly implicates online activity. However, to fall within the public performance right, there must be a transmission of a *performance* of the work, not merely of the work itself. Thus, for example, transmission of the digitally encoded sounds of a musical work to the hard disk of a recipient computer may infringe

---

[274] Id. at *23-24.

[275] The Digital Performance Right in Sound Recordings Act of 1995 created a limited public digital performance right in sound recordings as of February 1, 1996. Pub. L. No. 104-39, 109 Stat. 336 (codified at 17 U.S.C. §§ 106, 114, 115). Certain transmissions of performances are exempt. The exemptions do not apply, however, to an "interactive" service, which the copyright statute defines as a service "one that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient." 17 U.S.C. §§ 114(d)(1), 114(j)(7).

the right of distribution of the work (as well as the reproduction right), but not the public performance right, because the work is not being *performed*[276] at the recipient's end.

1. Isochronous Versus Asynchronous Transmissions

One of the most hotly debated issues concerning the scope of the public performance right in online contexts is whether, to fall within the copyright owner's right of public performance, the "performance" must be accomplished by a transmitted signal that is capable of immediate conversion to a performance moment-by-moment in time (referred to as an "isochronous transmission"), or whether it is sufficient that the transmitted signal is sent either faster or slower (overall or moment-by-moment) than the embodied performance (referred to as an "asynchronous transmission").[277]

The definition of performing a work publicly in Section 101 of the copyright statute was drafted at a time when "transmissions" were generally isochronous transmissions, as in broadcasting. If this definition is read to require an isochronous transmission – and to date all of the types of transmissions that courts have held to be public performances have been isochronous transmissions[278] – then many acts of downloading of works on the Internet (being asynchronous transmissions), even if followed by in-home playback, may not fall within the public performance right. The issue is far from settled, however, and performing rights societies have argued to the contrary.[279] The issue is particularly significant for musical works because different organizations are often responsible for licensing and collecting royalties for public distribution and public performance of musical works.

Even if an isochronous transmission is required for a public performance, the distinction between isochronous and asynchronous transmissions becomes highly blurred on the Internet. Because the Internet is based on packet switching technology, all transmissions through the Internet are in some sense "asynchronous." Moreover, through use of buffering in memory or storage of information on magnetic or optical storage, either at the transmitting or the receiving end or both, of all or parts of transmitted data, even an asynchronous transmission can effect a smooth, moment-by-moment performance at the receiving end.

One can argue that the determinative factor of whether a public performance has been accomplished should be judged from the perspective of what the recipient perceives, not the transmission technology used (whether isochronous or asynchronous), especially if the transmitting party controls when and what the recipient sees. For example, the Senate Report accompanying the Digital Performance Right in Sound Recordings Act of 1995 suggests that burst transmissions for prompt playback may constitute public performances:

---

[276] The copyright statute provides that "[t]o 'perform' a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible." 17 U.S.C. § 101.

[277] K. Stuckey, Internet and Online Law § 6.08[4][b], at 6-63 – 6-64 (2008).

[278] Id. at 6-64.

[279] Id.

> [I]f a transmission system was designed to allow transmission recipients to hear sound recordings substantially at the time of transmission, but the sound recording was transmitted in a high-speed burst of data and stored in a computer memory for prompt playback (such storage being technically the making of a phonorecord), and the transmission recipient could not retain the phonorecord for playback on subsequent occasions (or for any other purpose), delivering the phonorecord to the transmission recipient would be incidental to the transmission.[280]

2. The Meaning of "Publicly"

Section 106(4) grants the exclusive right to perform a work "publicly." Section 101 defines performing a work "publicly" to include performance by transmission to an audience that may receive the transmission at different times, at different places, or both. Thus, the mere fact that recipients may download performances of a work at dispersed times on demand through the Internet does not diminish the "public" nature of such performances. For example, in On Command Video Corp. v. Columbia Pictures Industries, Inc., [281] the court held that the public performance right was implicated by a system of video cassette players wired to hotel rooms which was capable of transmitting guest-selected movies to the occupants of one room at a time.

In sum, the breadth of definition of "public" performances makes a variety of online transmissions of "on demand" information potentially within the public performance right. How contemporaneously the playback of that information must be with the transmission in order for there to be deemed a "performance" under current United States law remains to be seen. The WIPO treaties could render many of these issues largely academic in view of the fact that the current public performance right could become subsumed in the potentially broader right of "communication to the public" or "making available to the public" contained in the WIPO treaties discussed below. However, as discussed further below, the implementation of the WIPO treaties in the DMCA takes a minimalist approach and does not adopt separate rights of "communication to the public" or "making available to the public." Accordingly, the noted uncertainties with respect to the right of public performance are likely to await further clarification through judicial development.

3. Live Nation Motor Sports v. Davis

In Live Nation Motor Sports, Inc. v. Davis,[282] the plaintiff promoted and produced motorcycle racing events and streamed webcasts of the events on its web site. Although the facts are unclear from the court's opinion, the defendant provided links to the plaintiff's web site that enabled users of the defendant's web site to view the webcasts from the defendant's web site. The plaintiff sought a preliminary injunction against the defendant, arguing that the defendant's

---

[280] S. Rep. No. 104-128, at 39 (1995), reprinted in 1995 U.S.C.C.A.N. 356, 386.

[281] 777 F. Supp. 787 (N.D. Cal. 1991).

[282] 2006 U.S. Dist. LEXIS 89552 (N.D. Tex. Dec. 11, 2006).

links to the plaintiff's web site constituted an unauthorized display and performance of the plaintiff's copyrighted broadcasts.[283]

The court granted a preliminary injunction enjoining the defendant from providing Internet links to the plaintiff's webcasts of its racing events or otherwise displaying or performing the plaintiff's webcasts.[284] With almost no analysis, the court ruled that the plaintiff had a likelihood of success on its copyright claim because "the unauthorized 'link' to the live webcasts that [the defendant] provides on his website would likely qualify as a copied display or performance of [the plaintiff's] copyrightable material."[285] The court found a threat of irreparable harm to the plaintiff because the defendant's links would cause the plaintiff to lose its ability to sell sponsorships or advertisements on the basis that its website was the exclusive source of the webcasts.[286]

Although the unclear facts of this case make its reach uncertain, it could potentially imply that any unauthorized link that causes material available on another site to be streamed through an unauthorized site could constitute an infringing public display or performance.

4. United States v. ASCAP

In United States v. ASCAP,[287] the district court ruled that the downloading of a digital music file embodying a particular song does not constitute a public performance of that song. The case arose out of an application that Yahoo, RealNetworks and AOL made to ASCAP for a license to publicly perform the musical works of the ASCAP repertoire by means of their respective Internet services. After the parties were unable to agree on a licensing fee, ASCAP applied to the court for a determination of a reasonable fee. The parties cross-moved for partial summary judgment on the issue of whether downloading a digital music file embodying a song constitutes a public performance of the song.[288]

The court noted that the copyright statute provides that, to "perform" a work means to "recite," "render," or "play" it, and the plain meanings of each of those terms require contemporaneous perceptibility. Accordingly, the court concluded that for a song to be "performed," it must be transmitted in a manner designed for contemporaneous perception. The downloading of a music file is more accurately characterized as a method of reproducing that file, rather than performing it.[289] The court also noted that its interpretation was consistent with

---

283 Id. at *3-4.

284 Id. at *18.

285 Id. at *12.

286 Id. at *15.

287 485 F. Supp. 2d 438 (S.D.N.Y. 2007), aff'd, 627 F.3d 64 (2d Cir. 2010), cert. denied, 181 L.Ed.2d 232 (Oct. 3, 2011).

288 Id. at 440-41. The applicants conceded that the streaming of a musical work does constitute a public performance. Id. at 442.

289 Id. at 443-44. The court also found this interpretation consistent with the holdings of those courts that have addressed downloading of music over the Internet using peer-to-peer file transfer programs. For example, the

the Copyright Office's position in its 2001 DMCA Section 104 Report to Congress, in which the Copyright Office stated that "we do not endorse the proposition that a digital download constitutes a public performance even when no contemporaneous performance takes place."[290]

On appeal, the Second Circuit affirmed this ruling.[291] The Second Circuit agreed with the district court that the ordinary sense of the words "recite," "render," and "play" refer to actions that can be perceived contemporaneously. Downloaded songs are not performed in any perceptible manner during the transfers – the user must take some further action to play the songs after download. Because the electronic download itself involves no recitation, rendering, or playing of the musical work encoded in the digital transmission, the court held that such a download is not a performance of that work.[292]

The Second Circuit rejected ASCAP's argument that all downloads fall under clause (2) of the definition of "perform or display a work 'publicly'" in Section 101[293] because downloads "transmit or otherwise communicate a performance," namely the initial or underlying performance of the copyrighted work, to the public. The Second Circuit cited its 2008 ruling in Cartoon Network (discussed in the next subsection) that, when the statute speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission, not simply to transmitting a recording of a performance. ASCAP's alternative interpretation was flawed because, in disaggregating the "transmission" from the simultaneous "performance" and treating the transmission itself as a performance, ASCAP rendered superfluous the subsequent "a performance … of the work" as the object of the transmittal. Cartoon Network recognized that a "transmittal of a work" is distinct from a transmittal of "a performance" – the former being a transmittal of the underlying work and the latter being a transmittal that is itself a performance of the underlying work. Accordingly, the court ruled that transmittal without a performance does not constitute a "public performance."[294]

---

court cited the holding in Maverick Recording Co. v. Goldshteyn, 2006 U.S. Dist. LEXIS 52422, at *8 (E.D.N.Y. July 31, 2006) ("Downloading and uploading copyrighted files from a peer-to-peer network constitutes, respectively, *reproducing and distributing* copyrighted material in violation of 17 U.S.C. § 106.") (emphasis added). ASCAP, 2007 U.S. Dist. LEXIS 31910 at *14.

290 Id. at 444 (quoting U.S. Copyright Office, Digital Millennium Copyright Act Section 104 Report to the United States Congress at xxvii-xxviii (Aug. 29, 2001)).

291 United States v. ASCAP, 627 F.3d 64 (2d Cir. 2010), cert. denied, 181 L.Ed.2d 232 (Oct. 3, 2011).

292 Id. at 73.

293 That clause provides that to "perform or display a work "publicly" means "(2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times." 17 U.S.C. § 101.

294 ASCAP, 627 F.3d at 73-74.

5. The Cablevision Case

In The Cartoon Network LP v. CSC Holdings, Inc.[295] the Second Circuit ruled on whether the playback through Cablevision's network of copies of cable programs stored on its servers at the instance of its customers as part of its "Remote Storage" Digital Video Recorder (RS-DVR) system constituted unauthorized public performances of the stored works. The detailed facts of how the RS-DVR system worked are set forth in Section II.A.4(n) above. Cablevision argued that the transmissions generated in response to customer requests for playback of programs stored on its network servers by customers did not constitute public performances because the RS-DVR customer, not Cablevision, invoked the transmitting and thus the performing, and the transmissions were not "to the public."[296]

The court ruled that it need not address Cablevision's first argument because, even if the court were to assume that Cablevision made the transmissions when RS-DVR playbacks occurred, the RS-DVR playbacks did not involve the transmission of a performance "to the public." The court began its analysis by noting that the second, or "transmit," clause of the definition of public performance applies "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."[297] The court observed, "The fact that the statute says 'capable of receiving the performance,' instead of 'capable of receiving the transmission,' underscores the fact that a transmission of a performance is itself a performance."[298]

The Second Circuit therefore focused on who was "capable of receiving" performances through playbacks via the RS-DVR system. Cablevision argued that, because each RS-DVR transmission was made using a single unique copy of a work, made by an individual subscriber, one that could be decoded exclusively by that subscriber's cable box, only one subscriber was capable of receiving any given RS-DVR transmission. By contrast, the district court had suggested that, in considering whether a transmission was "to the public," one should consider not the potential audience of a particular transmission, but the potential audience of the underlying *work* whose content was being transmitted. The Second Circuit ruled that the district court's approach was inconsistent with the language of the transmit clause, which speaks of persons capable of receiving a particular "transmission" or "performance," and not of the potential audience of a particular "work."[299]

On appeal, the plaintiffs presented a slightly different argument, insisting that the same original performance of a work was being transmitted to Cablevision's various subscribers at different times upon request. The court noted that the implication of the plaintiffs' argument was that, to determine whether a given transmission of a performance was to the public, one should

---

[295] 536 F.3d 121(2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 2009 U.S. LEXIS 4828 (2009).

[296] Id. at 134.

[297] Id.

[298] Id.

[299] Id. at 135.

consider not only the potential audience of that transmission, but also the potential audience of any transmission of the same underlying "original" performance. The court rejected this argument, noting that it would obviate any possibility of a purely private transmission.[300]

> We do not believe Congress intended such odd results. Although the transmit clause is not a model of clarity, we believe that when Congress speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission. Thus, HBO transmits its own performance of a work when it transmits to Cablevision, and Cablevision transmits its own performance of the same work when it retransmits the feed from HBO.[301]

Accordingly, the Second Circuit concluded that a court must look downstream, rather than upstream or laterally, to determine whether any link in a chain of transmissions made by a party constitutes a public performance, and should not examine the potential recipients of the content provider's initial transmission to determine who was capable of receiving the RS-DVR playback transmission. Because the RS-DVR system, as designed, made transmissions only to one subscriber using a copy made by that particular subscriber, the court concluded that the universe of people capable of receiving an RS-DVR transmission was the single subscriber whose self-made copy was used to the create the transmission, and the transmissions through the RS-DVR system were therefore not public performances.[302] The court cautioned, however, that its holding "does not generally permit content delivery networks to avoid all copyright liability by making copies of each item of content and associating one unique copy with each subscriber to the network, or by giving their subscribers the capacity to make their own individual copies. We do not address whether such a network operator would be able to escape any other form of copyright liability, such as liability for unauthorized reproductions or liability for contributory infringement."[303]

6. Ringtones – In re Application of Cellco Partnership

In In re Application of Celleco Partnership d/b/a Verizon Wireless,[304] the court ruled that the sale of ringtones by Verizon to its cell phone customers did not require payment to ASCAP for a public performance license for the musical works embodied in the ringtones. ASCAP argued that Verizon engaged in public performances of the musical works when it downloaded ringtones to its customers. It also argued that Verizon was both directly and

---

300 Id. at 135-36.

301 Id. at 136.

302 Id. at 137, 139. "If the owner of a copyright believes he is injured by a particular transmission of a performance of his work, he may be able to seek redress not only for the infringing transmission, but also for the underlying copying that facilitated the transmission. Given this interplay between the various rights in this context, it seems quite consistent with the Act to treat a transmission made using Copy A as distinct from one made using Copy B, just as we would treat a transmission made by Cablevision as distinct from an otherwise identical transmission made by Comcast." Id. at 138.

303 Id. at 139.

304 663 F. Supp. 2d 363 (S.D.N.Y. 2009).

secondarily liable for public performances of musical works when its customers played ringtones on their telephones upon incoming calls.[305]

The court rejected both these arguments. As to the first, citing the Cablevision case discussed in the previous subsection, the court ruled that, because only one subscriber was capable of receiving a particular transmission of a ringtone during download, such transmission was not itself made to the "public," regardless of whether a download could be considered a transmission of a "performance" of the musical works in the ringtone.[306] The court did note that, "[w]here a transmission is of a digital file rather than a performance that can be contemporaneously observed or heard, and where that transmission is but a link in a chain to a downstream public performance, it may be that the transmission is not an act of infringement for which the transmitter is directly liable under § 106(4), but rather an act that may subject the transmitter to contributory liability under § 106(4) for the infringement created by any ultimate public performance."[307] That could not be the case here, however, because the court concluded that there was no qualifying public performance under § 106(4) when the customer used the ringtone upon an incoming call.

Specifically, the court ruled that, when a ringtone plays on a cellular telephone, even when that occurs in public, the user is exempt from copyright liability under Section 110(4) of the copyright statute, which exempts any "performance of a nondramatic literary or musical work otherwise than in a transmission to the public, without any purpose of direct or indirect commercial advantage and without payment of any fee or other compensation for the performance to any of its performers, promoters, or organizers, if [] there is no direct or indirect admission charge."[308] The court held that on occasions when Verizon customers had activated their ringtones and the telephones rang in the presence of members of the public at a level where it could be heard by others, such playing of the musical works embodied in the ringtones satisfied all of the requirements of the §110(4) exemption: Verizon customers were not playing the ringtones for any commercial advantage, they did not get paid any fee or compensation for those performances, and they did not charge admission. Accordingly, there was no non-exempt public performance by the users of the ringtones to which Verizon could be secondarily liable.[309]

The court also rejected ASCAP's argument that Verizon was directly liable for itself engaging in a public performance of copyrighted musical works when ringtones played in public on customers' cell phones because it controlled the entire series of steps that allowed and triggered the cellular telephone to perform the musical works in public. The court noted that

---

[305] Id. at 368.

[306] Id. at 371.

[307] Id. at 374 n.14.

[308] Id. at 374 (quoting 17 U.S.C. § 110(4)).

[309] Id. at 375. Nor, in order to avoid secondary liability, was Verizon obligated to show that each and every customer would be able to meet its burden of proof that its performance of ringtones in public satisfied the § 110(4) exemption. "The law does not impose an insurmountable burden on Verizon to show precisely how each of its customers has actually used her telephone, but only requires it to demonstrate that customers as a group do not exhibit any expectation of profit when they permit the telephones to ring in public." Id. at 376.

Verizon's only role in the playing of a ringtone was the sending of a signal to alert a customer's telephone to an incoming call, and that signal was the same whether the customer had downloaded a ringtone or not, whether she had set the phone to play a ringtone upon receiving a call or not, whether she was in a public setting or not, and whether she had the ringtone volume turned high or low. And it was the caller, not Verizon, who initiated the entire process that led to the playing of the ringtone. Accordingly, Verizon did not engage in activity constituting direct liability, even if the ringing of its customers' phones in public constituted public performances.[310]

7. Warner Bros. v. WTV Systems

In Warner Bros. Entertainment Inc. v. WTV Systems,[311] the defendants offered a DVD "rental" service called "Zediva" that allowed customers to view streams from DVDs in DVD players hosted on the defendants' premises. To operate the service, the defendants purchased hundreds of DVD players and installed them in cabinets at a data center they leased in Santa Clara, California. The defendants also purchased copies of the plaintiffs' copyrighted works on DVD and placed those DVDs in their DVD players for selection by their customers. Each DVD remained in its respective DVD player while it was transmitted to the defendants' customers on multiple occasions.[312]

When a customer requested a particular work, the defendants, through their Zediva service, started the play process on a particular DVD player holding the requested work, converted the analog video signal from the DVD player into a digital signal using a video adapter, fed the digital signal into a DVD control server that converted the digital signal to a form suitable for streaming across the Internet, converted the digital signal to a format that could be viewed in the player created by the defendants and used on their web site, transmitted the performance via the Internet to the customer, and provided the customer with a custom viewer necessary to view the video stream. To begin the process, the customer clicked on a virtual button on the defendants' web site. Customers were unable to access all the other features available on a particular DVD, such as deleted and extra scenes, or other special DVD features. The defendants maintained exclusive control of their servers, and the customers had no control whatsoever over the various servers that the defendants used to direct traffic among their stacks of DVD players.[313]

The defendants described the Zediva service as allowing customers to "rent" a particular DVD and DVD player for 14 days. However, customers did not have access to or control over a specific DVD or DVD player. Instead, the defendants streamed the content of the DVD to a customer for a maximum period of four hours, provided that the customer did not pause it for more than one hour during that time. After four hours of total "rental" time or an hour-long pause, whichever occurred first, the defendants used the DVD player containing the same DVD

---

310 Id. at 376-79.

311 824 F. Supp. 2d 1003 (C.D. Cal. 2011).

312 Id. at 1006-07.

313 Id. at 1007 & n.2.

to transmit the work to a different customer. When the first customer made a request to resume viewing, the transmission might be sent from a different DVD or a different DVD player than the one originally used to transmit in the earlier "rental" period. According to the defendants' web site, if all of the copies of a particular work were "rented out" when a customer wanted to view the work, the customer could request to be notified, via email, when it became available.[314]

The plaintiffs claimed that the Zediva service infringed their rights of public performance and sought a preliminary injunction, which the court determined the plaintiffs were entitled to. Turning to whether the streams constituted public performances, the court noted that the definition of "public performance" in Section 106(4) is comprised of two clauses: (1) the "public place" clause, which states that a performance is public if it occurs at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; and (2) the "transmit" clause, which states that a performance is public if someone transmits or otherwise communicates the performance to a place specified by the public place clause, or to "the public," whether the members of the public capable of receiving the performance receive it in the same place or in separate places and at the same time or at different times.[315]

The defendants argued that their service offered "DVD rentals" rather than transmissions of performances. The court rejected this argument, analogizing to On Command Video Corp. v. Columbia Pictures Industries,[316] which held that transmissions of movies from a central console of VCRs (each VCR containing a copy of a particular movie) in a hotel to private guest rooms did not constitute "electronic rentals" similar to guests' physical borrowing of videotapes, but rather constituted transmissions of performances under the transmit clause of Section 106(4). In On Command, the fact that hotel guests initiated the transmission by turning on the television and choosing a video was immaterial. The court ruled that, as in On Command, the Zediva service fell under the transmit clause because it transmitted performances by communicating the images and sounds of the movies through the use of a device or process (the defendants' equipment, servers and the Internet) from its central bank of DVD players to individual customer's computers, where the images and sounds were received beyond the place from which they were sent. And as in On Command, the fact that Zediva's customers initiated the transmission by turning on their computers and choosing which of the works they wished to view was immaterial to the legal analysis.[317]

The court further ruled that the transmissions of the Zediva service were "to the public" for purposes of the transmit clause "because the relationship between Defendants, as the transmitter of the performance, and the audience, which in this case consists of their customers, is a commercial, 'public' relationship regardless of where the viewing takes place. The non-

---

[314] Id. at 1007.

[315] Id. at 1008-09.

[316] 777 F. Supp. 787, 789-90 (N.D. Cal. 1991).

[317] WTV Systems, 824 F. Supp. 2d at 1009-10.

public nature of the place of the performance has no bearing on whether or not those who enjoy the performance constitute 'the public' under the transmit clause."[318]

The court rejected the defendants' argument that their performances were not "to the public" in view of the Cartoon Network (Cablevision) case discussed in Section II.B.5 above. Under Cartoon Network, the Second Circuit found that the transmissions were not "to the public" because each RS-DVR playback transmission was made to a single subscriber using a single unique copy produced by that subscriber. By contrast, in this case, the defendants' customers did not produce their own unique copy of the plaintiffs' copyrighted works. Instead, like On Command, the same DVD was used over and over again to transmit performance of the works, which destroyed the one-to-one relationship on which the Cartoon Network decision depended for its finding that the transmissions were not to the public.[319]

The court also rejected the defendants' argument that it should adopt the Second Circuit's volitional requirement for direct copyright infringement liability. The court found that no Ninth Circuit case had adopted the volitional conduct requirement and that, in view of the fact that copyright infringement is a strict liability offense, the court was not inclined to adopt the volitional conduct requirement without clear instruction from the Ninth Circuit.[320] Finally, the court rejected the defendants' reliance on Professional Real Estate Investors, Inc.,[321] which involved a service provided by a hotel that rented videodiscs to its guests, who carried the discs to their rooms to watch them on in-room videodisc players. The Ninth Circuit found that because the performances at issue took place in a guest's private hotel room, the performances were not "in public," and the performances were not transmissions under the transmit clause because the guests carried the discs to their rooms, rather than the hotel transmitting a performance to the room from a central bank of players. The Ninth Circuit stated, however, that a closed circuit system similar to the one described in On Command would fall squarely within the transmit clause. Accordingly, the district court found that the Professional Real Estate case supported the court's finding of infringement.[322]

In concluding that the plaintiffs were entitled to a preliminary injunction, the court noted the following forms of irreparable harm: because the defendants were exploiting the plaintiffs copyrighted works without paying the normal licensing fees, they were depriving the plaintiffs of revenue and jeopardizing the continued existence of the plaintiffs' licensees' businesses; the Zediva service threatened the development of a successful and lawful video-on-demand market and, in particular, the growing Internet-based video-on-demand market; the presence of the Zediva service in the market threatened to confuse consumers about video-on-demand products, and to create incorrect but lasting impressions with consumers about what constitutes lawful video-on-demand exploitation of copyrighted works; and the Zediva service threatened the

---

318 Id. at 1010.

319 Id. at 1011 n.7.

320 Id.

321 866 F.2d 278 (9th Cir. 1989).

322 WTV Systems, 824 F. Supp. 2d at 1011.

development of a successful and lawful video-on-demand market by offering a sub-optimal customer experience (the defendants admitted they had received complaints about the quality of their service and that a lot of times customers would receive a notice that a particular copyrighted work was temporarily "out of stock" because all DVD players containing that particular work were in use).[323]

The case settled in October 2011, with Zediva agreeing to pay $1.8 million to six major movie studios and to cease showing their movies without permission.[324]

8. Capitol Records v. MP3tunes

For analysis of this case's rulings with respect to infringement of public performance rights against the operator of a music "locker" service, see Section III.C.6(b)(1)(iii).s below.

9. The Aereo Case

The widely followed case of American Broadcasting Cos. v. Aereo, Inc.[325] applied the logic of the Cablevision case, discussed in detail in Section II.B.5 above, to adjudicate important issues of the scope of the public performance right. The plaintiffs sought a preliminary injunction to stop Aereo from offering a private streaming service that allowed its users to access live copyrighted content over the Internet through various mobile devices such as PCs, laptops, smartphones, and tablet computers. The plaintiffs' motion for a preliminary injunction was limited in scope, challenging only the aspects of Aereo's service that allowed subscribers to view the plaintiffs' copyrighted television programs contemporaneously with the over-the-air broadcast of those programs.[326]

Aereo's service worked as follows. A user of Aereo's system, after logging into his account on Aereo's web site, could navigate through a programming guide to select television programs currently being aired or that would be aired at a later time. If the user selected a program that was currently being aired, the user was given two options, "Watch" and "Record." Selecting "Watch" caused Aereo's system to transmit a web page to the user in which the program started after a short delay, allowing the user to view the program "live," i.e., roughly contemporaneous with its over-the-air broadcast. If the user pressed the "Record" button after having begun watching a program using the "Watch" feature, the Aereo system retained the copy that the user had been watching. If "Record" was not selected, the copy was not retained and could not be viewed again later.[327]

---

[323] Id. at 1013-14. The court required the defendants to post a bond of $50,000 as a condition to issuance of the preliminary injunction. Id. at 1015.

[324] Melissa Lipman, "DVD Streaming Co. Settles Movie Studios' IP Suit For $2M," Oct. 28, 2011, available as of Aug. 3, 2012 at http://www.law360.com/articles/281603.

[325] 2012 U.S. Dist. LEXIS 96309 (S.D.N.Y. July 11, 2012).

[326] Id. at *2-4.

[327] Id. at *6-7.

Instead of selecting the "Watch" function at the outset, the user could press the "Record" button to schedule a recording of a program that would be broadcast at a later time or that was currently being aired. However, the "Record" feature could also be used, like the "Watch" feature, to view programs live – users could direct Aereo's system to begin a recording and then immediately begin playback of the recording as it was being made.[328]

The technology that implemented the service, which was designed specifically to take advantage of the reasoning of the Cablevision case, consisted of a large bank of individual antennas that could be "assigned" individually to specific users who wanted to watch or record a program. Specifically, when a user clicked on the "Watch" button, the user's web browser sent a request to Aereo's Application Server, which in turn sent a request and certain information about the user and the requested television program to Aereo's Antenna Server. The Antenna Server allocated resources to the user, including an antenna and transcoder, depending on whether the user was a "static" or "dynamic" user, a distinction based on the user's subscription plan with Aereo. Static users had a set of previously selected antennas that had been assigned to them, whereas dynamic users, who were the vast majority of Aereo's subscribers, were randomly assigned an antenna each time they used Aereo's system. No two users were assigned a single antenna at the same time. The data obtained by a particular antenna while allocated to a particular user was not shared with or accessible by any other Aereo use. [329]

Once these resources were allocated, the Antenna Server sent a "tune" request that directed the user's antenna to tune into a particular broadcast frequency band to obtain the desired program. The Antenna Server also sent a request to the Streaming Server that created a unique directory, assigned to the user, for storing the output data received by the antennas and processed by the transcoder. Once that directory was created, an electrical signal was sent from the antenna, processed and converted into data packets, and then sent to the transcoder, which encoded it in a form to be transmitted over the Internet. The encoded data was sent to the Streaming Server, where it was saved on a hard disk to a file in the previously created directory and, once saved, was read from that file into a RAM memory buffer that sent the data to the user over the Internet once a sufficient amount of data (at least six or seven seconds of programming) had accumulated. Essentially the same process occurred when the user engaged the "Record" function, the only substantial difference between the "Watch" and "Record" functions being that when a user engaged the "Record" function, the file saved to the hard disk was tagged as permanent and automatically retained, whereas the file saved using the "Watch" function was not automatically retained unless the user clicked "Record" while the show was still open on the user's web browser.[330]

The plaintiffs moved for a preliminary injunction. The court noted that the only significant factual dispute for purposes of that motion concerned the operation of Aereo's antennas. Aereo contended that each of its antennas functioned separately to receive the incoming broadcast signals. The plaintiffs asserted that Aereo's antennas functioned collectively

---

328 Id. at *7-8.

329 Id. at *9-10.

330 Id. at *11-13.

as a single antenna, because the individual antennas were packed so closely together on a board that they in effect had a shared metallic substructure which appeared to the incoming signals as one continuous piece of metal. After extensive review of the conflicting testimony of the parties' experts, the court determined that, based on the evidence at that stage of the proceedings, Aereo's antennas did indeed function independently – a crucial fact for applicability of the Cablevision case to the facts at hand.[331]

The court then turned to the first element of establishing entitlement to a preliminary injunction – likelihood of success on the merits. Aereo argued that Cablevision applied to its system because, like the RS-DVR system in Cablevision, its system created unique, user-requested copies that were transmitted only to the particular user that created them, and the performances were thus not public. The plaintiffs distinguished Cablevision on its facts, arguing that because Aereo's subscribers were watching the programs as they were still being broadcast, they were not using the copies Aereo created for time shifting purposes, and those copies therefore did not "break the chain" of the over-the air transmission received by Aereo. Thus, the plaintiffs contended, Aereo was engaged in a public performance that emanated from the original broadcast signal itself, much like a community antenna which simply passes along a broadcast signal the public. Stated differently, the plaintiffs argued that the stored copies of the signals made by Aereo should be viewed as merely facilitating the transmission of a single master copy – in this case, the broadcast signal – rather than as copies from which a distinct transmission was made.[332]

The court agreed with Aereo's characterization of its system and rejected the plaintiffs' attempts to distinguish Cablevision. With respect to the copies created by Aereo's system, the court found that they were not mere facilitating copies, but rather were no less materially significant to how the system functioned than the copies created in Cablevision's system. First, Aereo's system created a unique copy of each television program for each subscriber who requested to watch that program, saved to a unique directory on Aereo's hard disks assigned to that user. Second, each transmission that Aereo's system ultimately made to a subscriber was from that unique copy. Third, the transmission of the unique copy was made solely to the subscriber who requested it and no other subscriber was capable of accessing that copy. The court held that these factual similarities of Aereo's service to the Cablevision system suggested that Aereo's service fell within the core of what Cablevision held lawful. The court also ruled the fact that Aereo's users could "share" resource like antennas by using them at different times did not affect the analysis, as it remained clear that the copies Aereo's system made were unique for each user and not shared.[333]

The court found other similarities to Cablevision as well. An undercurrent in the Second Circuit's reasoning in Cablevision was that the Cablevision system merely allowed subscribers to enjoy a service that could also be accomplished using any standard DVR or VCR. Similarly, Aereo's functionality substantially mirrored that available using devices such as a DVR or a

---

[331] Id. at *13-22.

[332] Id. at *31-33.

[333] Id. at *34-36 & n.7.

Slingbox,[334] which allow users to access free, over-the-air broadcast television on mobile Internet devices of their choosing.[335] Moreover, the court found that the analysis the Second Circuit undertook in finding that the performance to the user was made from the copies stored in the Cablevision system rather than from, for example, the incoming stream of data, was equally applicable here. Specifically, Cablevision held that a public performance does not occur merely because a number of people are transmitted the same television program. Nor was the Second Circuit willing to accept the argument that, notwithstanding its creation of unique copies, Cablevision was actually transmitting to its users the performance of that work that occurred when the programming service supplying Cablevision's content transmitted that content to Cablevision. In fact, the Second Circuit expressly refused to look back to the received signal to judge whether Cablevision was engaged in a public performance. The district court therefore observed that, given that each antenna in Aereo's system functioned independently, in at least one respect the Aereo system presented a stronger case than Cablevision for attaching significance to the copies made because, unlike Cablevision in which multiple copies were all created from a single stream of data, each copy made by Aereo's system was created from a separate stream of data.[336]

The district court also rejected the plaintiffs' attempt to distinguish Cablevision on the ground that Cablevision addressed only copies used for time shifting. The court noted that nowhere in Cablevision did the Second Circuit articulate a requirement that the copies be used for time shifting in order to "break the chain" of transmission from the original broadcaster to the end user. Rather, the Second Circuit's analysis of the public performance claim was entirely directed toward explaining why the copies created by the system in Cablevision were significant and resulted in performances to a limited, non-public audience. Nor did anything in Cablevision turn on the times at which individuals received their transmissions.[337]

Finally, the court rejected the plaintiffs' suggestion that Cablevision addressed only transmissions using the same medium as the initial broadcast that were made to the same device and to the same place as the initial transmission. Although points of distinction from Cablevision, the court found no reason to believe that they had any material bearing on who was

---

[334] A Slingbox, when connected to a user's television in the home, digitized the received signals, including live broadcast television, and allowed them to be streamed over the Internet to the user's personal mobile devices. Id. at *8.

[335] Id. at *36-37.

[336] Id. at *36-39.

[337] Id. at *40-47. The court found the plaintiffs' argument that "complete" time shifting should be required to fit within the contours of Cablevision even less persuasive, as the argument was no longer tied to the rationale that time shifting is required to "break the chain" of the original transmission. For example, an Aereo user who began watching a recording of the Academy Awards, initially broadcast at 6:00 p.m., one minute before the program ended at 11:00 p.m. would not have engaged in complete time shifting, although the chain of transmission would certainly have been "broken" across the nearly five hours of recording before viewing commenced. The court found that the plaintiffs had not provided an argument as to why a user who began watching a recording of a program one minute (or five minutes, or ten minutes) before the broadcast ended was part of a public performance but a user who began watching a minute after the program ended was not. Id. at *59-60.

"capable of receiving" a particular transmission or whether Aereo "breaks the chain" of transmission.[338]

Accordingly, the court concluded that the plaintiffs were unlikely to succeed on the merits of their public performance claim.[339] The court, however, issued some words of caution about the scope of its decision. First, the court made clear that it did not accept Aereo's position that the creation of any fixed copy from which a transmission is made always defeats a claim for a violation of the public performance right, because such position would eviscerate the transmit clause given the ease of making reproductions before transmitting digital data. Nor did the court need to resolve Aereo's argument that its antennas, standing alone, defeated the plaintiffs' claims that it was engaged in a public performance. Instead, the court merely pointed out that it had found Aereo's use of single antennas to reinforce its conclusion that the copies created by Aereo's system were unique and accessible only to a particular user, as they indicated that the copies were created using wholly distinct signal paths. Because the copies were created from a signal received independently by each antenna, in order to find a "master" copy that was arguably being transmitted, the court would have been required, contrary to Cablevision, to look back to the incoming over-the-air signal rather than simply an earlier step in Aereo's process. Aereo's antennas thus reinforced the significance of the copies its system created and aided the court in finding that Aereo did not create mere facilitating copies.[340]

> As such, the Court's holding that Plaintiffs have not demonstrated a likelihood of success is limited. There may be cases in which copies are purely facilitory, such as true buffer copies or copies that serve no function whatsoever other than to pass along a clearly identifiable "master" copy from which the transmission is made. These facts, however, are not before the Court today.[341]

Turning to the other elements for a preliminary injunction, the court found that the plaintiffs had demonstrated they would suffer irreparable harm because Aereo would damage their ability to negotiate with advertisers by siphoning viewers from traditional distribution channels, in which viewership is measured by Nielsen ratings, into Aereo's service which is not measured by Nielsen, artificially lowering those ratings. Similarly, by poaching viewers from cable or other companies that license the plaintiffs' content, Aereo's activities would damage the plaintiffs' ability to negotiate retransmission agreements, as those companies would demand concessions from the plaintiffs to make up for the decrease in viewership. Aereo's service would also harm the plaintiffs' streaming of their content on their own web sites.[342]

---

338 Id. at *61-62.

339 In view of its conclusion that the plaintiffs had failed to demonstrate they were likely to succeed in establishing that Aereo's system resulted in a public performance, the court found it need not reach the issue of whether Aereo also could escape liability because it was the consumer, not Aereo, who made the transmissions that the plaintiffs complained of. Id. at *68.

340 Id. at *66-67.

341 Id. at *67.

342 Id. at 71-76.

With respect to the balance of hardships, the court found that the balance did not tip decidedly in favor of the plaintiffs. The harm to Aereo of a preliminary injunction would be substantial, as it had sufficient capital to continue operations for just six to seven months, after which it would likely shut down absent investment of further capital. An injunction was also likely to cause Aereo to lose employees and damage its ability to attract investors to obtain new capital, and to diminish its competitive advantage in launching a unique and innovative product. Having concluded that Aereo's service was likely lawful, the court ruled that it could not disregard the harms to Aereo that an injunction would cause by assuming its business was founded on infringement.[343]

In sum, the court concluded that because it could not accept the plaintiffs' attempts to distinguish Cablevision, the plaintiffs had not shown a likelihood of success on the merits. And although they had demonstrated they faced irreparable harm, they had not demonstrated that the balance of hardships decidedly tipped in their favor. Accordingly, the court denied the motion for a preliminary injunction.[344]

C. The Right of Public Display

Section 106(5) of the copyright statute grants the owner of copyright in a literary, musical, dramatic, and choreographic work, a pantomime, and a pictorial, graphic or sculptural work, including the individual images of a motion picture or other audiovisual work,[345] the exclusive right to display the work publicly.[346] Section 101 defines the meaning of "to display a work publicly" in virtually identical terms as the definition of "to perform a work publicly." Thus, a public display can be accomplished by a transmission of a display of the work to members of the public capable of receiving the display in the same place or separate places and at the same time or at different times.

The WIPO Copyright Treaty does not contain a right of public display per se. However, the right of public display is arguably subsumed under the right of communication to the public in the WIPO Copyright Treaty.

1. The Frena, Marobie-FL, Hardenburgh and Webbworld Cases

In Playboy Enterprises, Inc. v. Frena,[347] the court held that the making of photographs available on a BBS was a "public" display, even though the display was limited to subscribers, and subscribers viewed the photographs only upon downloading the photographs from the BBS on demand. Thus, making material available through the Internet even to only a small and select

---

343 Id. at *85-89.

344 Id. at *93-94.

345 To display a motion picture, one must display individual images "nonsequentially." K. Stuckey, Internet and Online Law § 6.03[5], at 6-17 (2008).

346 The right of public display does not apply to sound recordings, architectural works, and audiovisual works (except for display of individual images of an audiovisual work).

347 839 F. Supp. 1552 (M.D. Fla. 1993).

audience may still constitute a "public" display. The point at which a selected audience becomes so small that a display to such audience can no longer be considered a "public" display is unclear. The Playboy court seemed to define an audience as "public" if it contains "a substantial number of persons outside of a normal circle of family and its social acquaintances."[348]

Similarly, in Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,[349] the administrator of the Web page of the defendant, National Association of Fire Equipment Distributors (NAFED), placed certain files on NAFED's Web page containing three volumes of copyrighted clip art of the plaintiff. The court ruled that the placement of the files containing the clip art on the Web page constituted a direct violation of both the plaintiff's distribution right and public display right. The court concluded that the mere making available of the files for downloading was sufficient for liability, because "once the files were uploaded [onto the Web server], they were available for downloading by Internet users and … the [OSP] server transmitted the files to some Internet users when requested."[350] The court, citing the Netcom case, refused to hold the OSP supplying Internet service to NAFED directly or vicariously liable, although the court noted that the OSP might be liable for contributory infringement, depending upon whether the OSP knew that any material on NAFED's Web page was copyrighted, when it learned of that fact, and the degree to which the OSP monitored, controlled, or had the ability to monitor or control the contents of NAFED's Web page.[351]

And in Playboy Enterprises, Inc. v. Hardenburgh,[352] the defendants operated a BBS which made available graphic image files to subscribers for a fee, many of which contained adult material. To increase its stockpile of available information, and thereby its attractiveness to new customers, defendants provided an incentive to encourage subscribers to upload information onto the BBS. Subscribers were given "credit" for each megabyte of electronic data that they uploaded onto the system, which entitled them to download defined amounts of data from the system in return. Information uploaded onto the BBS went directly to an "upload file" where an employee of the BBS briefly checked the new files to ascertain whether they were "acceptable," meaning not pornographic and not blatantly protected by copyright.[353] Many of the plaintiff's copyrighted photographs appeared on the BBS and the plaintiff brought suit for infringement.

With respect to the issue of direct liability for the infringing postings of its subscribers, the court agreed with the Netcom decision's requirement of some direct volitional act or participation in the infringement. However, the court found that the facts of the case, unlike those of Frena, MAPHIA, and Netcom, were sufficient to establish direct liability for infringement of both the public display and distribution rights. The court based its conclusion on "two crucial facts: (1) Defendants' policy of encouraging subscribers to upload files, including

---

348 Id. at 1557.

349 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

350 Id. at 1241.

351 Id. at 1245.

352 982 F. Supp. 503 (N.D. Ohio 1997).

353 Id. at 506.

adult photographs, onto the system, and (2) Defendants' policy of using a screening procedure in which [its] employees viewed all files in the upload file and moved them into the generally available files for subscribers. These two facts transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement."[354]

Finally, in Playboy Enterprises, Inc. v. Webbworld, Inc.,[355] the court held the defendants directly liable for infringing public displays of copyrighted images for making such images available through a website for downloading by subscribers.

2. Kelly v. Arriba Soft

An important case construing the scope of the public display right on the Internet is that of Kelly v. Arriba Soft Corp.[356] In that case, the defendant Arriba was the operator of a "visual search engine" on the Internet that allowed users to search for and retrieve images. In response to a search query, the search engine produced a list of reduced, "thumbnail" images. To provide this functionality, Arriba developed a program called a "crawler" that would search the Web looking for images to index, download full-sized copies of the images onto Arriba's server, then use those images to generate lower resolution thumbnails. Once the thumbnails were created, the program deleted the full-sized originals from the server.[357]

When the user double-clicked on the thumbnail, a full-sized version of the image was displayed. During one period of time, the full-sized images were produced by "inline linking" – i.e., by retrieving the image from the original web site and displaying it on the Arriba web page with text describing the size of the image and a link to the originating site – such that the user would typically not realize the image actually resided on another web site. During a subsequent period of time, the thumbnails were accompanied by two links, a "source" and a "details" link. The "details" link produced a separate screen containing the thumbnail image with text describing the size of the image and a link to the originating site. Alternatively, by clicking on the "source" link or the thumbnail itself, the Arriba site produced two framed windows on top of the Arriba page: the window in the forefront contained the full-sized image, imported directly from the originating site; underneath that was a second window displaying the home page containing the image from the original site.[358]

Arriba's crawler copied 35 photographs on which the plaintiff, Kelly, held the copyrights into the Arriba database. When he complained, Arriba deleted the thumbnails of images that came from Kelly's own web sites and placed those sites on a list of sites that it would not crawl in the future. Several months later, Kelly sued Arriba, identifying in the complaint other images

---

354 Id. at 513.

355 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

356 336 F.3d 811 (9th Cir. 2003).

357 Id. at 815.

358 Id. at 815-16.

of his that came from third party web sites.[359] The district court ruled that Arriba's use of both the thumbnails and the full sized images was a fair use, and Kelly appealed.[360]

The Ninth Circuit, in an opinion issued in July of 2003,[361] affirmed the ruling that the use of the thumbnails was a fair use. Applying the first of the four statutory fair use factors, the court held that the thumbnails were a transformative use of Kelly's works because they were much smaller, lower resolution images that served an entirely different function than Kelly's original images. Users would be unlikely to enlarge the thumbnails and use them for artistic purposes because the thumbnails were of much lower resolution than the originals. Thus, the first fair use factor weighted in favor of Arriba.[362]

The court held that the second factor, the nature of the copyrighted work, weighed slightly in favor of Kelly because the photographs were creative in nature. The third factor, the amount and substantiality of the portion used, was deemed not to weigh in either party's favor. Although the entire images had been copied, it was necessary for Arriba to copy the entire images to allow users to recognize the image and decide whether to pursue more information about it or the originating web site.[363]

Finally, the court held that the fourth factor, the effect of the use upon the potential market for or value of the copyrighted work, weighed in favor of Arriba. The court found that Arriba's use of the thumbnail images would not harm the market for Kelly's use of his images or the value of his images. By displaying the thumbnails, the search engine would guide users to Kelly's web site rather than away from it. Nor would Arriba's use of the images harm Kelly's ability to sell or license the full-sized images. Anyone downloading the thumbnails would not be successful selling full sized-images from them because of the low resolution of the thumbnails, and there would be no way to view, create, or sell clear, full-sized images without going to Kelly's web sites. Accordingly, on balance, the court found fair use.[364]

The court reversed, however, the district court's ruling that Arriba's use of the full-sized images through inline linking or framing was a fair use and remanded for further proceedings. The Ninth Circuit's ruling on this issue was contrary to a result the Ninth Circuit had reached in an earlier opinion in the case issued in 2002,[365] which it withdrew when issuing its 2003 opinion. In the 2002 ruling, the Ninth Circuit had held, in a highly controversial ruling, that Arriba's inline linking to and framing of the full-sized images violated the plaintiff's public display

---

[359] Id. at 816.

[360] Id. at 816-17.

[361] The 2003 opinion withdrew an earlier and highly controversial opinion issued by the court in 2002, discussed further below.

[362] Id. at 818-19.

[363] Id. at 820-21.

[364] Id. at 821-22.

[365] Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002).

rights.[366] Interestingly, the court ruled that Kelly's reproduction rights had not been infringed: "This use of Kelly's images does not entail copying them but, rather, importing them directly from Kelly's web site. Therefore, it cannot be copyright infringement based on the reproduction of copyrighted works …. Instead, this use of Kelly's images infringes upon Kelly's exclusive right to 'display the copyrighted work publicly.'"[367] Apparently the court's observation that the offering of the full-sized images through linking "does not entail copying" was meant to refer to direct copying *by Arriba*, because a copy of the images is certainly made in the user's computer RAM, as well as on the screen, when the user clicks on the thumbnail to display the full sized image.

With respect to infringement of the display right, the court ruled in its 2002 opinion that the *mere act of linking* to the images constituted infringement. First, the court ruled that there was an unauthorized "display": "By inline linking and framing Kelly's images, Arriba is showing Kelly's original works without his permission."[368] Second, the court held that such "showing" was a "public" one: "A display is public even if there is no proof that any of the potential recipients was operating his receiving apparatus at the time of the transmission. By making Kelly's images available on its web site, Arriba is allowing public access to those images. The ability to view those images is unrestricted to anyone with a computer and internet access."[369] The court thus concluded that Arriba had directly infringed Kelly's public display rights: "By allowing the public to view Kelly's copyrighted works while visiting Arriba's web site, Arriba created a public display of Kelly's works. … Allowing this capability is enough to establish an infringement; the fact that no one saw the images goes to the issue of damages, not liability."[370]

The court went on in its 2002 opinion to hold that Arriba's display of Kelly's full-sized images was not a fair use. Unlike the case of the thumbnails, the court held that the use of the full-sized images was not transformative. "Because the full-sized images on Arriba's site act primarily as illustrations or artistic expression and the search engine would function the same without them, they do not have a purpose different from Kelly's use of them."[371] Accordingly, the first factor weighed against fair use. For the same reasons as before, the second factor weighed slightly in favor of Kelly.[372] The third factor weighed in favor of Kelly because, although it was necessary to provide whole images "to suit Arriba's purpose of giving users access to the full-sized images without having to go to another site, such a purpose is not

---

366 Kelly had never argued, either in the proceedings below or on appeal, that his public display rights had been infringed. The Ninth Circuit raised this issue on its own.

367 Id. at 944.

368 Id. at 945.

369 Id.

370 Id. at 946.

371 Id. at 947.

372 Id. at 947-48.

legitimate."[373] Finally, the fourth factor weighed in Kelly's favor, because "[b]y giving users access to Kelly's full-sized images on its own web site, Arriba harms all of Kelly's markets."[374]

The Ninth Circuit's ruling in its 2002 decision on the public display issue generated a lot of controversy, since the reach of that ruling was potentially so broad. In particular, the logic the Ninth Circuit adopted in its 2002 decision – that the mere act of inline linking to or framing of a work, whether or not users actually view the linked work – constitutes a public display of the linked work, could call into question the legality of many types of linking or framing that has not been expressly authorized by the owner of the linked material. Apparently in response to the controversy, on Oct. 10, 2002, the Ninth Circuit ordered additional briefing on issues of public display and derivative use rights raised by the case.[375]

In its 2003 decision, the Ninth Circuit omitted entirely the discussion of the public display right that had appeared in its 2002 decision. Instead, the court held that the district court should not have decided whether the display of the full-sized images violated Kelly's public display rights because the parties never moved for summary judgment on that issue.[376] In the proceedings below, Kelly had moved only for summary judgment that Arriba's use of the thumbnail images violated his display, reproduction and distribution rights. Arriba cross-moved for summary judgment and, for purposes of the motion, conceded that Kelly had established a prima facie case of infringement as to the thumbnail images, but argued that its use of the thumbnail images was a fair use. The Ninth Circuit concluded that, by ruling that use of both the thumbnail images and the full-sized images was fair, the district court had improperly broadened the scope of both Kelly's original motion to include a claim for infringement of the full-sized images and the scope of Arriba's concession to cover the prima facie case for both the thumbnail images and the full-sized images.[377] Accordingly, the court remanded for further proceedings with respect to the full-sized images to give the parties an opportunity to fully litigate those issues.[378]

3. Ticketmaster v. Tickets.com

See Section III.D.7 below for a discussion of this case, which distinguished the Kelly v. Arriba Soft case and held that Tickets.com's deep linking to pages on Ticketmaster's web site where tickets could be purchased for events listed on Tickets.com's site did not constitute an infringing public display.

---

373 Id. at 948.

374 Id.

375 "Ninth Circuit Orders Added Briefs on Hyperlinking Issues in Arriba Soft Appeal," *BNA's Electronic Commerce & Law Report* (Oct. 30, 2002) at 1082.

376 Kelly v. Arriba Soft Corp., 336 F.3d 811, 822 (9th Cir. 2003).

377 Id. at 817.

378 Id. at 822.

4. Perfect 10 v. Google (aka Perfect 10 v. Amazon)

Perfect 10 v. Google set forth a detailed adjudication of the boundaries of the display right on the Internet, and in particular, which entity should be deemed to perform the display for purposes of copyright liability when the display results through links from a web site to another web site storing copies of the copyrighted material at issue. Because both the district court and the Ninth Circuit issued very thorough, thoughtful opinions, the holdings of both courts will be explained in detail.

The plaintiff Perfect 10 sought to preliminarily enjoin Google from displaying thumbnails and full size versions of its copyrighted photographs through the "Google Image Search" function in response to user search queries. Google Image Search allowed a user to input a text search string and returned thumbnail images organized into a grid potentially responsive to the search query.[379]

To operate Google Image Search, Google created and stored in its cache thumbnail versions of images appearing on web sites crawled by Google's web crawler. The thumbnails chosen for display in response to search queries depended solely upon the text surrounding the image at the original site from which the image was drawn. When a user clicked on a thumbnail image, Google displayed a page comprised of two distinct frames divided by a gray horizontal line, one frame hosted by Google and the second one hosted by the underlying web site that originally hosted the full size image.[380] In the upper frame, Google displayed the thumbnail, retrieved from its cache, and information about the full size image, including the original resolution of the image and the specific URL associated with that image. The upper frame made clear that the image might be subject to copyright and that the upper frame was not the original context in which the full size image was found. The lower frame contained the original web page on which the original image was found. Google neither stored nor served any of the content displayed in the lower frame, which was stored and served by the underlying third party web site containing the original image.[381] Perfect 10 brought claims against Google for direct, vicarious and contributory copyright infringement.

Direct Infringement Claims. Perfect 10 alleged that Google directly infringed its copyrights by displaying and distributing the full size images hosted by third party web sites, and by creating, displaying and distributing thumbnails of its copyrighted full size images. Google conceded that it created and displayed thumbnails, but denied that it displayed, created, or distributed what was depicted in the lower frame of search results displays, which were generated via in-line links to third party sites storing the original images of interest.[382]

---

379 Perfect 10 v. Google, 416 F. Supp. 2d 828, 832-33 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

380 Id. at 833.

381 Id. at 833-34.

382 Id. at 838.

The district court began with a consideration of how "display" should be defined in the context of in-line linking, noting that two approaches were possible: (1) a "sever" test, in which display is defined as the act of *serving* content over the web, i.e., physically sending bits over the Internet to the user's browser, and (2) an "incorporation" test, in which display is defined as the mere act of *incorporating* content into a web page that is then pulled up by the browser through an in-line link. Under the server test, advocated in the case by Google, the entity that should be deemed liable for the display of infringing content is the entity whose server served up the infringing material. Under the incorporation test, advocated by Perfect 10, the entity that should be deemed liable for the display of infringing content is the entity that uses an in-line link in its web page to direct the user's browser to retrieve the infringing content.[383]

The district court reviewed the existing decisions dealing with the question of whether linking constitutes infringing "displaying" of copyrighted material. The court noted that in the Webbworld and Hardenburg cases,[384] the material was stored on the defendant's servers, and in the Perfect 10 v. Cybernet Ventures case,[385] it was unclear whether the defendant stored or served any of the infringing content. The court further noted that the Ninth Circuit had withdrawn its opinion in Kelly v. Arriba Soft[386] adopting the incorporation test in the face of widespread criticism of that decision. The court therefore found that none of these cases, or any other existing precedent, resolved the question before it.[387]

The district court concluded that the server test was the most appropriate one for determining whether Google's lower frames were a "display" of infringing material. The court articulated several reasons for adopting the server test. First, it is based on what happens at the technological level as users browse the web, and thus reflects the reality of how content actually travels over the Internet before it is shown on users' computers. Second, it precludes search engines from being held directly liable for in-line linking and/or framing infringing content stored on third party web sites, but allows copyright owners still to seek to impose contributory or vicarious liability on web sites for including such content. Third, web site operators can readily understand the server test and courts can apply it relatively easily. Fourth, in the instant case, it imposes direct liability on the web sites that took Perfect 10's full size images and posted them on the Internet for all to see. Finally, the server test promotes the balance of copyright law to encourage the creation of works by protecting them while at the same time encouraging the dissemination of information. The server test would avoid imposing direct liability for merely indexing the web so that users can more readily find the information they seek, while imposing direct liability for the hosting and serving of infringing content.[388]

---

383 Id. at 838-40.

384 These cases are discussed in Section II.C.1 above.

385 This case is discussed in Section II.A.4(k) above.

386 This case is discussed in Section II.C.2 above.

387 416 F. Supp. 2d at 840-43.

388 Id. at 843-44.

Applying the server test, the district court ruled that for purposes of direct infringement, Google's use of frames and in-line links did not constitute a "display" of the full size images stored on and served by infringing third party web sites, but Google did "display" the thumbnails of Perfect 10's copyrighted images because it created, stored, and served those thumbnails on its own servers.[389]

On appeal, the Ninth Circuit agreed with the district court that the "server" test should be used to determine which entity displays an image on the web, concluding that the test was consistent with the statutory language of the copyright statute. Under that test, Perfect 10 had made a prima facie case that Google's communication of its stored thumbnail images directly infringed Perfect 10's display rights. However, Google had not publicly displayed a copy of the full size infringing images when it framed in-line linked images that appeared on a user's computer screen.[390] The Ninth Circuit found that Google's activities with respect to the full size images did not meet the statutory definition of public display "because Google transmits or communicates only an address which directs a user's browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself."[391] The court also ruled that, because Google's cache merely stored the text of web pages, and not the images themselves, Google was not infringing the display right by virtue of its cache.[392]

Fair Use. The district court evaluated Google's assertion of the fair use defense to the display of the thumbnails. With respect to the first fair use factor, the purpose and character of the use, the court found that Google's display of the thumbnails was a commercial use, since Google derived significant commercial benefit from Google Image Search in the form of increased user traffic and, in turn, increased advertising revenue. The court distinguished the Ninth Circuit's decision in the Kelly v. Arriba Soft case by noting that, unlike Arriba Soft, Google derived direct commercial benefit from the display of thumbnails through its "AdSense" program, under which third party web sites could place code on their sites to request Google's server to algorithmically select relevant advertisements for display based on the content of the site, and then share revenue flowing from the advertising displays and click-throughs. If third party web sites participating in the AdSense program contained infringing copies of Perfect 10 photographs, Google would serve ads on those sites and split the revenue generated from users who clicked on the Google-served ads.[393] Accordingly, the court concluded that "AdSense unquestionably makes Google's use of thumbnails on its image search far more commercial than Arriba's use in *Kelly II*. Google' thumbnails lead users to sites that directly benefit Google's bottom line."[394]

---

389 Id. at 844.

390 Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1159-60 (9th Cir. 2007).

391 Id. at 1161 n.7.

392 Id. at 1162.

393 Perfect 10 v. Google, 416 F. Supp. 2d 828, 834, 846-47 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

394 Id. at 846. Google counterargued that its AdSense program policies prohibited a web site from registering as an AdSense partner if the site's web pages contained images that appeared in Google Image Search results. The

Relying on the Kelly v. Ariba Soft decision, the court concluded that the use of the thumbnails was transformative because their creation and display enabled the display of visual search results quickly and efficiently, and did not supersede Perfect 10's us of the full size images. But the court noted that the transformative nature of the thumbnail use did not end the analysis, because the use was also "consumptive." In particular, the court noted that after it filed suit against Google, Perfect 10 entered into a licensing agreement with a third party for the sale and distribution of Perfect 10 reduced-size images for download to and use on cell phones.[395] "Google's use of thumbnails does supersede this use of P10's images, because mobile users can download and save the thumbnails displayed by Google Image Search onto their phones."[396] On balance, then, the court concluded that, because Google's use of thumbnails was more commercial than Arriba Soft's and because it was consumptive with respect to Perfect 10's reduced-size images, the first factor weighed "slightly in favor" of Perfect 10.[397]

The district court ruled that the second fair use factor, the nature of the copyrighted work, weighed "only slightly in favor" of Perfect 10 because, although its photographs were creative, as in the case of the Kelly v. Arriba Soft case, they had appeared on the Internet before use in Google's search engine.[398] The court found that the third factor, the amount and substantiality of the portion used, favored neither party because Google's use of the copies of Perfect 10's images was no greater than necessary to achieve the objective of providing effective image search capabilities.[399] Finally, the court found that the fourth factor, the effect of the use upon the potential market for and value of the copyrighted work, weighed slightly in Perfect 10's favor because of the court's finding that Google's use of thumbnails likely would harm the potential market for the downloading of Perfect 10's reduced-size images onto cell phones. On balance, then, the court found that the fair use doctrine likely would not cover Google's use of the thumbnails.[400]

On appeal, the Ninth Circuit reached the opposite conclusion under the fair use doctrine. Before beginning its specific analysis of the four fair use factors, the Ninth Circuit made some important preliminary rulings concerning the burden of proof with respect to the fair use doctrine. The district court had ruled that, because Perfect 10 had the burden of showing a likelihood of success on the merits, it also had the burden of demonstrating a likelihood of overcoming Google's fair use defense. The Ninth Circuit held the district court's ruling on this

---

court noted, however, that Google had not presented any information regarding the extent to which the purported policy was enforced nor had it provided examples of AdSense partners who were terminated because of violations of the policy. In contrast, Perfect 10 submitted numerous screenshots of third party web sites that served infringing content and also appeared to be receiving and displaying AdSense ads from Google. Id. at 846-47.

[395] Id. at 847-49.

[396] Id. at 849.

[397] Id.

[398] Id. at 849-50.

[399] Id. at 850.

[400] Id. at 850-51.

point to be erroneous. Citing cases from the Supreme Court and the Federal Circuit holding that the burdens at the preliminary injunction stage track the burdens at trial, the Ninth Circuit ruled that, once Perfect 10 had shown a likelihood of success on the merits, the burden shifted to Google to show a likelihood that its affirmative defenses – including that of fair use – would succeed.[401]

The Ninth Circuit's analysis of the fair use factors is significant in its recognition of the need, when judging the transformative nature of the use, to balance the public benefit from the use against the potential harm to the rights holder from superseding commercial uses, as well as in its requirement of a showing that alleged potential superseding commercial uses are both real and significant in their impact. Specifically, with respect to the first factor, the Ninth Circuit, citing the Kelly v. Arriba Soft case, noted that Google's use of the thumbnails was highly transformative because its search engine transformed each image into a pointer directing a user to a source of information.[402] In addition, "a search engine provides social benefit by incorporating an original work into a new work, namely, an electronic reference tool."[403]

In a significant ruling, the Ninth Circuit disagreed, on two grounds, with the district court's conclusion that Google's use of thumbnail images was less transformative than the video search engine at issue in Kelly v. Arriba Soft because Google's use of thumbnails superseded Perfect 10's right to sell its reduced-size images for use on cell phones. First, the Ninth Circuit noted that the alleged superseding use was not significant at the present time, because the district court had not found that any downloads of Perfect 10's photos for mobile phone use had actually

---

401 Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1158 (9th Cir. 2007). This holding was the opposite of one the Ninth Circuit had reached in an earlier issued opinion in the appeal, which the instant opinion replaced. In the earlier opinion, the Ninth Circuit had concluded that, because a plaintiff has the burden of showing a likelihood of success on the merits in order to obtain a preliminary injunction, the plaintiff should also have the burden of demonstrating a likelihood of overcoming the defendant's fair use defense. However, because the defendant in an infringement action has the burden of proving fair use, the Ninth Circuit had ruled in its earlier opinion that the defendant is responsible for introducing evidence of fair use in the first instance in responding to a motion for preliminary relief, whereupon the burden would then shift to the plaintiff to demonstrate that it will overcome the fair use defense. Perfect 10 v. Amazon.com, Inc., 487 F.3d 701, 714 (9th Cir. 2007) (superseded by 508 F.3d 1146 (9th Cir. 2007)). The court further elaborated its rationale in the earlier opinion as follows: "In order to demonstrate its likely success on the merits, the moving party must necessarily demonstrate it will overcome defenses raised by the non-moving party. This burden is correctly placed on the party seeking to demonstrate entitlement to the extraordinary remedy of a preliminary injunction at an early stage of the litigation, before the defendant has had the opportunity to undertake extensive discovery or develop its defenses." 487 F.3d at 714. The Ninth Circuit apparently concluded that this earlier holding was inconsistent with established precedent that the burdens at the preliminary injunction stage track the burdens at trial, leading the court to issue a revised opinion.

402 508 F.3d at 1165.

403 Id. The Ninth Circuit rejected Perfect 10's argument that providing access to infringing web sites cannot be deemed transformative and is inherently not fair use. The court noted that Google was operating a comprehensive search engine that only incidentally indexed infringing web sites. "This incidental impact does not amount to an abuse of the good faith and fair dealing underpinnings of the fair use doctrine. Accordingly, we conclude that Google's inclusion of thumbnail images derived from infringing websites in its Internet-wide search engine activities does not preclude Google from raising a fair use defense." Id. at 1164 n.8.

taken place.[404] Second, the court concluded "that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case."[405] Accordingly, the first fair use factor weighed in favor of Google.

The Ninth Circuit found that the district court had correctly analyzed the second and third factors.[406] With respect to the fourth factor, Perfect 10 challenged the district court's finding of no harm to the market for the full sized images on the ground that likelihood of market harm may be presumed if the intended use of an image is for commercial gain. The court noted, however, that this presumption does not arise when a work is transformative because market substitution is less certain. Because Google's use of thumbnails for search engine purposes was highly transformative and market harm could therefore not be presumed, and because Perfect 10 had not introduced evidence that Google's thumbnails would harm its existing or potential market for full size images, the Ninth Circuit rejected Perfect 10's argument.[407]

With respect to harm to Perfect 10's alleged market for reduced size images, the Ninth Circuit noted that the district court did not make a finding that Google users had actually downloaded thumbnail images for cell phone use, so any potential harm to that alleged market remained hypothetical. Accordingly, the court concluded that the fourth factor favored neither party.[408] Balancing the four factors, and particularly weighing Google's highly transformative use and its public benefit against the unproven use of thumbnails for cell phone downloads, the court concluded that Google's use of Perfect 10's thumbnails was a fair use. Accordingly, the court vacated the preliminary injunction regarding Google's use of thumbnail images.[409]

Contributory Infringement. Perfect 10 argued to the district court that Google was contributing to the infringement of two direct infringers – third party web sites hosting and serving infringing copies of Perfect 10 photographs, and Google Image Search users downloading such images. The district court ruled as a preliminary matter that Perfect 10 could not base its contributory infringement claim on users' actions, because Perfect 10 had demonstrated only that users of Google search were *capable* of directly infringing by downloading the images, but had not submitted sufficient evidence showing the extent to which users were in fact downloading Perfect 10's images through Google Image Search. Thus, the

---

[404] Id. at 1166.

[405] Id.

[406] Id. at 1167-68

[407] Id. at 1168.

[408] Id.

[409] Id. In a side, but significant, issue, Google argued that the Ninth Circuit lacked jurisdiction over the preliminary injunction to the extent it enforced unregistered copyrights. The court rejected this argument: "Once a court has jurisdiction over an action for copyright infringement under section 411 [of the copyright statute], the court may grant injunctive relief to restrain infringement of any copyright, whether registered or unregistered." Id. at 1154 n.1.

contributory infringement claim had to be based on knowledge and material contribution by Google to the infringing activities of third party web sites hosting Perfect 10's images.[410]

With respect to the knowledge prong, the district court, citing the Supreme Court's Grokster case, noted that either actual or constructive knowledge is sufficient for contributory liability. The court rejected Perfect 10's argument that Google had actual knowledge from the presence of copyright notices on Perfect 10's images or from the fact that Google's AdSense policy stated that it monitored the content of allegedly infringing sites. The court noted that Google would not necessarily know that any given image on the Internet was infringing someone's copyright merely because the image contained a copyright notice. With respect to the alleged monitoring by Google, Google had changed its AdSense policy to remove the language reserving to Google the right to monitor its AdSense partners. The court further noted that, in any event, merely because Google may have reserved the right to monitor its AdSense partners did not mean that it could thereby discern whether the images served by those web sites were subject to copyright.[411]

The district court then turned to an analysis of whether numerous notices of infringement sent by Perfect 10 to Google were sufficient to give Google actual knowledge of infringing activity. Google challenged the adequacy of those notices on the grounds that they frequently did not describe in sufficient detail the specific URL of an infringing image and frequently did not identify the underlying copyrighted work. Some notices listed entire web sites as infringing, or entire directories within a web site. Google claimed that despite these shortcomings, it promptly processed all of the notices it received, suppressing links to specific web pages that it could confirm displayed infringing Perfect 10 copies. The court concluded, however, that it need not resolve the question of whether Google had adequate actual knowledge of infringement, in view of the court's conclusion that Google had not materially contributed to the infringing activity of third party web sites.[412]

The district court articulated the following grounds for its finding that Perfect 10 had not adequately met its burden to show that Google sufficiently contributed to the infringing activity for contributory liability. First, the court set forth numerous differences between Google's activity and the activity that had been found to materially contribute to infringement in the Napster cases. For example, unlike in the case of the Napster system, in the instant case the infringing third party web sites existed, were publicly accessible, and engaged in the infringing activity irrespective of their inclusion or exclusion from Google's index. Unlike Napster, Google did not provide the means of establishing connections between users' computers to facilitate the downloading of the infringing material. Even absent Google, third party web sites would continue to exist and would continue to display infringing content (an observation which would seem true of all search engines). And unlike Napster, Google did not boast about how

---

410 Perfect 10 v. Google, 416 F. Supp. 2d 828, 851-52 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

411 Id. at 853-54.

412 Id. at 854.

users could easily download infringing content, nor did it facilitate the transfer of files stored on users' otherwise private computers.[413]

In sum, the district court found that Perfect 10 had overstated Google's actual conduct and confused the mere provision of search technology with active encouragement and promotion of infringing activity. The court also rejected Perfect 10's argument based on the Supreme Court's Grokster case that Google had materially contributed to the infringing activity by providing through AdSense a revenue stream to the infringing web sites. The court held that, although the AdSense program might provide some level of additional revenue to the infringing web sites, Perfect 10 had not presented any evidence establishing what that revenue was, much less that it was material, either in its own right or relative to those web sites' total income. Accordingly, the court ruled that Perfect 10 was not likely to prevail on its claim for contributory liability.[414]

In an important ruling on appeal,[415] the Ninth Circuit reversed and remanded for factual findings under a specialized test for contributory infringement for computer system operators. The Ninth Circuit began its analysis by examining the issue of whether Perfect 10 had adequately proved direct infringements to which Google could potentially contribute. Perfect 10 alleged that three parties directly infringed its images – third party web sites that copied, displayed and distributed unauthorized Perfect 10 images, individual users of Google's search engine who stored full size Perfect 10 images on their computers, and users who linked to infringing web sites, thereby automatically making cache copies of full size images in their computers. Google did not dispute that third party web sites directly infringed Perfect 10's copyrights by copying, displaying and distributing unauthorized copies of Perfect 10 images.[416]

The Ninth Circuit agreed, however, with the district court that Perfect 10 failed to provide any evidence directly establishing that users of Google's search engine had stored infringing images on their computers. Finally, the Ninth Circuit agreed with the district court that any cache copies of full size images made by users who linked to infringing web sites were a fair use. The copying performed automatically by a user's computer to assist in accessing the Internet was a transformative use and did not supersede the copyright holder's exploitation of the work.[417] "Such automatic background copying has no more than a minimal effect on Perfect 10's rights, but a considerable public benefit."[418] Accordingly, the Ninth Circuit assessed Google's secondary liability based solely with respect to activities of third party web sites that reproduced, displayed, and distributed unauthorized copies of Perfect 10's images on the Internet.[419]

---

[413] Id.

[414] Id. at 855-56.

[415] Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

[416] Id. at 1169.

[417] Id.

[418] Id.

[419] Id. at 1170.

Turning to whether Google could be secondarily liable for the infringing acts of those third party web sites, the Ninth Circuit first noted that under the Sony doctrine, Google could not be held liable for contributory infringement based solely on the fact that the design of its search engine facilitated such infringement. Nor, under footnote 12 of the Supreme Court's Grokster decision, could Google be held liable solely because it did not develop technology that would enable its search engine to automatically avoid infringing images.[420]

The Ninth Circuit next held that Google could not be liable under the Supreme Court's inducement test in Grokster, because Google had not promoted the use of its search engine specifically to infringe copyrights.[421] In reaching this result, however, the Ninth Circuit appears to have put a gloss on the Supreme Court's test for inducement liability, for in addition to noting that inducement liability could result from intentionally encouraging infringement through specific acts, the Ninth Circuit stated that intent could be imputed "if the actor knowingly takes steps that are substantially certain to result in … direct infringement."[422]

Finally, turning to whether Google could have secondary liability under the traditional common law doctrine of contributory liability, the Ninth Circuit, citing its Napster decisions, noted that it had "further refined this test in the context of cyberspace to determine when contributory liability can be imposed on a provider of Internet access or services."[423] The Ninth Circuit noted that under both Napster and Netcom, a service provider's knowing failure to prevent infringing actions could be the basis for imposing contributory liability, because under such circumstances, the intent required under the Supreme Court's Grokster decision may be imputed. Accordingly, the Ninth Circuit articulated the following test for contributory liability in the context of cyberspace:

> [W]e hold that a computer system operator can be held contributorily liable if it "has *actual* knowledge that *specific* infringing material is available using its system," *Napster*, 239 F.3d at 1002, and can "take simple measures to prevent further damage" to copyrighted works, *Netcom*, 907 F. Supp. At 1375, yet continues to provide access to infringing works.[424]

This articulated test leaves open at least the following questions, with respect to which the Ninth Circuit's decision gives little guidance:

-- Is this the exclusive test for contributory infringement in "the context of cyberspace"?

-- What are the boundaries of "the context of cyberspace" within which this test will apply?

---

[420] Id.

[421] Id. at 1171 n.11.

[422] Id. at 1171.

[423] Id.

[424] Id. at 1172 (emphasis in original).

-- Does the reference to "actual" knowledge preclude secondary liability on the alternative traditional common law formulation of "reason to know" in the context of cyberspace?

-- Do "simple measures" extend only to taking down specific infringing material, or to preventing its recurrence also?

Applying this specialized test, the Ninth Circuit ruled that the district court had erred in concluding that, even if Google had actual knowledge of infringing material available on its system, it did not materially contribute to infringing conduct because it did not undertake any substantial promotional or advertising efforts to encourage visits to infringing web sites, nor provide a significant revenue stream to the infringing web sites.[425] The Ninth Circuit stated:

> There is no dispute that Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials. We cannot discount the effect of such a service on copyright owners, even though Google's assistance is available to all websites, not just infringing ones. Applying our test, Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps.[426]

Noting that there were factual disputes over whether there are "reasonable and feasible means" for Google to refrain from providing access to infringing images, the Ninth Circuit remanded the contributory infringement claim for further consideration of whether Perfect 10 would likely succeed in establishing that Google was contributorily liable for in-line linking to full size infringing images under the test the court had enunciated.[427]

Similarly, the Ninth Circuit remanded for further proceedings on whether Amazon.com, which Perfect 10 had also sued based on its offering of the A9.com search engine, should be held contributorily liable. "It is disputed whether the notices gave Amazon.com actual knowledge of specific infringing activities available using its system, and whether Amazon.com could have taken reasonable and feasible steps to refrain from providing access to such images, but failed to do so."[428]

Vicarious Liability. Perfect 10 also asserted claims against Google for vicarious liability. With respect to the financial benefit prong, the district court found that Google obtained a direct financial benefit from the infringing activity through its AdSense revenues under the standard articulated in the Ninth Circuit's Fonovisa decision,[429] in which it held that the financial benefit

---

[425] Id.

[426] Id.

[427] Id. at 1172-73

[428] Id. at 1176.

[429] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

prong can be satisfied where the availability of infringing material acts as a "draw" for customers to the site. Under that standard, the district court found it likely that at least some users were drawn to Google Image Search because they knew that copies of Perfect 10's photos could be viewed for free, and Google derived a direct financial benefit when users visited AdSense partners' web sites that contained such infringing photos.[430]

Notwithstanding the financial benefit to Google, however, the district court found that Google had insufficient control over the infringing activity to impose vicarious liability because the Web is an open system. "Google does not exercise control over the environment in which it operates – i.e., the web. Google's ability to remove a link from its search index does not render the linked-to site inaccessible. The site remains accessible both directly and indirectly (i.e., via other search engines, as well as via the mesh of websites that link to it). If the phrase 'right and ability to control' means having substantial input into or authority over the decision to serve or continue serving infringing content, Google lacks such right or ability."[431] Moreover, Google's software lacked the ability to analyze every image on the Internet, compare each image to all other copyrighted images that existed in the world, or even to that much smaller subset of images that had been submitted to Google by copyright owners such as Perfect 10, and determine whether a certain image on the web infringed someone's copyright.[432] Finally, the court ruled that the "right and ability to control" prong required more than Google's reservation in its AdSense policy of the right to monitor and terminate partnerships with entities that violated others' copyrights. Accordingly, the district court held that Perfect 10 had not established a likelihood of proving the second prong necessary for vicarious liability.[433]

Based on its various rulings, the district court concluded that it would issue a preliminary injunction against Google prohibiting the display of thumbnails of Perfect 10's images, and ordered the parties to propose jointly the language of such an injunction.[434]

On appeal, the Ninth Circuit affirmed the district court's ruling that Perfect 10 had not shown a likelihood of establishing Google's right and ability to stop or limit the directly infringing conduct of third party web sites. The Ninth Circuit began its analysis by noting that, under *Grokster*, "a defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so."[435] With respect to the first part of this test, the court noted that, unlike in Fonovisa where the swap meet operator had contracts with its vendors giving it the right to stop the vendors from selling counterfeit recordings on its premises, Perfect 10 had not shown that Google had contracts with third party web sites that empowered Google to stop or limit them from reproducing, displaying and distributing infringing copies of Perfect 10's images. Although Google had AdSense

---

430 Perfect 10 v. Google, 416 F. Supp. 2d at 856-57.

431 Id. at 857-58.

432 Id. at 858.

433 Id.

434 Id. at 859.

435 Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007).

agreements with various web sites, an infringing third party web site could continue to reproduce, display, and distribute its infringing copies after its participation in the AdSense program was ended.[436] And unlike the Napster system, in which Napster's control over its closed system that required user registration and enabled Napster to terminate its users' accounts and block their access to the Napster system, Google could not terminate third party web sites distributing infringing photographs or block their ability to host and serve infringing full size images on the Internet.[437]

The Ninth Circuit also affirmed the district court's findings that Google lacked the practical ability to police the third party web sites' infringing conduct. "Without image-recognition technology, Google lacks the practical ability to police the infringing activities of third-party websites."[438] Google's inability to police distinguished it from the defendants held liable in the Napster and Fonovisa cases. Accordingly, Perfect 10 had failed to establish the right and ability to control prong of vicarious liability.[439] Having so concluded, the Ninth Circuit determined that it need not reach Perfect 10's argument that Google received a direct financial benefit.[440]

Based on its rulings, the Ninth Circuit reversed the district court's determination that Google's thumbnail versions of Perfect 10's images likely constituted a direct infringement. It also reversed the district court's conclusion that Perfect 10 was unlikely to succeed on the merits of its secondary liability claims because the district court failed to consider whether Google and Amazon.com knew of infringing activities yet failed to take reasonable and feasible steps to refrain from providing access to infringing images. Accordingly, the Ninth Circuit remanded the case to the district court for further proceedings on this point, as well as to consider whether Google and Amazon.com would qualify for any of the safe harbors of the DMCA, an issue which the district court did not consider because of its rulings. Because the district court would need to reconsider the appropriate scope of injunctive relief after addressing the secondary liability issues, the Ninth Circuit decided that it need not address the parties' dispute over whether the district court abused its discretion in determining that Perfect 10 satisfied the irreparable harm element of a preliminary injunction.[441]

On remand, Google asserted various safe harbors under the DMCA. Analysis of the rulings with respect to whether Google was entitled to any of the safe harbors may be found in Section III.C.6(b)(1)(ii).c.

---

[436] Id.

[437] Id. at 1174.

[438] Id.

[439] Id. The Ninth Circuit also stated, without analysis, that it agreed with the district court's conclusion that Amazon.com did not have the right and ability to supervise the infringing activity of Google or third parties, and that the district court did not clearly err in concluding that Amazon.com lacked a direct financial interest in such activities. Id. at 1176.

[440] Id. at 1175 n.15.

[441] Id. at 1176-77.

5. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey

In Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey,[442] the court ruled that display of copyrighted images on computer monitors within a law office constituted a public display, but was permitted under the fair use doctrine. Healthcare Advocates had filed a lawsuit alleging that a competitor infringed trademarks and copyrights and misappropriated trade secrets belonging to Healthcare Advocates. The defendants in that case were represented by the boutique IP law firm of Harding, Earley, Follmer & Frailey. To aid in preparing a defense, on two occasions employees of the Harding firm accessed screenshots of old versions of Healthcare Advocates' web sites that had been archived by the Internet Archive's web site (www.archive.org). The old versions of the web site were accessed through the "Wayback Machine," an information retrieval system offered to the public by the Internet Archive that allowed users to request archived screenshots contained in its archival database. Viewing the content that Healthcare Advocates had included on its public web site in the past was very useful to the Harding firm in assessing the merits of the trademark and trade secret allegations brought against the firm's clients. The Harding firm printed copies of the archived screenshots of interest and used the images in the litigation against their clients. Healthcare Advocates then sued the Harding firm, alleging that viewing the screenshots of the old versions of their web site on computers within the firm constituted an infringing public display, and that printing of copies of those screenshots and storing them on hard drives at the firm also infringed the company's copyrights.[443]

The court ruled that, "[u]nder the expansive definition of a public display, the display of copyrighted images on computers in an office constitutes a public display."[444] The court concluded, however, that the Harding firm's display and copying of those images for purposes of defending its clients in the litigation brought by Healthcare Associates constituted a fair use. With respect to the purpose of the use, the court noted that the images were used to better understand what Healthcare Associates' complaint, which did not specify what had been infringed nor have any documents attached to it depicting the infringement, was based on.[445] Only a small group of employees were able to see the images within the law firm's office, which the court found was "similar to a family circle and its acquaintances."[446] The purpose of the printing was only to make a record of what had been viewed and for use as supporting documentation for the defense the firm planned to make for its clients.[447] "It would be an absurd result if an attorney defending a client against charges of trademark and copyright infringement

---

442 2007 U.S. Dist. LEXIS 52544 (E.D. Pa. July 20, 2007).

443 Id. at *2-10.

444 Id. at *19.

445 Id. at *22-23.

446 Id. at *24. The copyright statute defines a "public" display as one made in a place "where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered." 17 U.S.C. § 101.

447 Id. at *24.

was not allowed to view and copy publicly available material, especially material that his client was alleged to have infringed."[448]

The second fair use factor weighed in favor of the firm because the nature of Healthcare Associates' web sites was predominantly informational. The third factor weighed in favor of the firm because, although entire images were copied, employees at the firm needed to copy everything they viewed because they were using the screenshots to defend their clients against copyright and trademark infringement claims. The firm also had a duty to preserve relevant evidence. Finally, the court found that the fourth fair use factor also favored the firm, because the value of Healthcare Associates' web sites was not affected by the Harding's firm's use, and the images viewed and copied were archived versions of the web site that Healthcare Associates no longer utilized, suggesting their worth was negligible. Accordingly, the court held that the Harding firm's use of the images obtained through the Wayback Machine constituted a fair use.[449]

6. ICG-Internet Commerce Group, Inc. v. Wolf

In ICG-Internet Commerce Group, Inc. v. Wolf,[450] the court held that the defendant had infringed the plaintiff's copy and public display rights in an adult video by posting the video to the defendant's web site. The court also ruled that the insertion into the plaintiff's video of a URL link to the defendant's web site constituted the creation of an infringing derivative work.[451]

D. The Right of Public Distribution

Section 106(3) of the copyright statute grants the copyright owner the exclusive right to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending. Thus, to implicate the right of public distribution, three conditions must obtain: (a) a "copy" must be distributed; (b) the distribution must be to the "public"; and (c) the distribution must be by sale, rental, lease, lending or "other transfer of ownership."

1. The Requirement of a "Copy"

Whether transmissions of a work on the Internet implicate the public distribution right turns in the first instance on whether there has been a distribution of a "copy" of the work. The broadcasting and cable industries have traditionally treated broadcasts and cable transmissions as *not* constituting distributions of copies of a work. With respect to Internet transmissions,

---

448 Id. at *24-25.

449 Id. at *26-29. The court also ruled that the firm's failure to preserve temporary cache files of the screenshots that were automatically created by the computers used by the firm's employees to view the images through the Internet, and were also automatically deleted by the computers' operating system, did not constitute spoliation of evidence. Id. at *30-38.

450 519 F. Supp. 2d 1014 (E.D. Pa. 2007).

451 Id. at 1018.

however, if a complete copy of a work ends up on the recipient's computer, it may be easy to conclude that a "copy" has been distributed. Indeed, to remove any doubt from this issue, the NII White Paper proposed to include "transmission" within the copyright owner's right of distribution,[452] where transmission is defined essentially as the creation of an electronic copy in a recipient system.[453]

It is less clear whether other types of transmissions constitute distributions of "copies." For example, what about an artistic work that is transmitted and simultaneously performed live at the recipient's end? Although the public performance right may be implicated, has there been a distribution of a "copy" that would implicate the right of distribution? Should it matter whether significant portions of the work are buffered in memory at the recipient's computer? Many of these distinctions could be rendered moot by the potentially broader right of "communication to the public" contained in the WIPO treaties discussed below, were that right ever to be expressly adopted in implementing legislation in the United States (the DMCA does not contain such a right).

Even if a "copy" is deemed to have been distributed in the course of an Internet transmission of an infringing work, difficult questions will arise as to who should be treated as having made the distribution – the original poster of the unauthorized work, the OSP or BBS through which the work passes, the recipient, or some combination of the foregoing? Thus, the same issue of volition arises with respect to the distribution right as was discussed above in connection with the reproduction right.

(a) Cases Addressing Whether Mere Posting Is a Distribution

Several decisions have addressed the question of whether the mere posting – i.e., the "making available" – of a work on a BBS or other Internet site, or in a "shared file" folder within peer-to-peer client software, from which it can be downloaded by members of the public constitutes a public distribution of the work, and have reached quite contrary results, as detailed in the next two subsections. In addition to those decisions, several other decisions have declined to reach the issue and/or left the question open, often acknowledging the existence of conflicting authority:

– In Arista Records LLC v. Greubel, 453 F. Supp. 2d 961 (N.D. Tex. 2006), the court, although not deciding on a motion to dismiss whether the electronic transmission over a computer network (here, transmission of copyrighted recordings through a file sharing network) or the mere listing of such copyrighted recordings in a directory as available for download, is sufficient to violate a copyright owner's distribution right, the court cited numerous decisions so holding or suggesting that either of such acts is sufficient for infringement of the distribution

---

[452] The copyright statute currently defines "transmission" or "transmit" solely in reference to performances or displays of a work. The NII White Paper does not, however, argue for removal of the requirement that an offending distribution be one to the "public." NII White Paper at 213-15.

[453] NII White Paper at 213. Appendix 1 of the NII White Paper proposes the following definition: "To 'transmit' a reproduction is to distribute it by any device or process whereby a copy or phonorecord of the work is fixed beyond the place from which it was sent." Id. App. 1, at 2.

right, and concluded that such decisions were sufficient to deny the defendant's motion to dismiss the complaint on the pleadings.[454] The court stated, "[M]aking copyrighted works available to other *may* constitute infringement by distribution *in certain circumstances*."[455]

– Maverick Recording Co. v. Goldshteyn, 2006 U.S. Dist. LEXIS 52422 at *3 (E.D.N.Y. July 31, 2006) ("[T]he 'making available' argument need not be decided here.").

– Fonovisa, Inc. v. Alvarez, 2006 U.S. Dist. LEXIS 95559 at *8 (N.D. Tex. July 24, 2006) ("This Court is not making a determination as to whether 'making works available' violates the right of distribution.").

– Warner Bros. Records, Inc. v. Payne, 2006 U.S. Dist. LEXIS 65765 at *4 (W.D. Tex. July 17, 2006) (declining to "rule out the Plaintiffs' 'making available' theory as a possible ground for imposing liability").

– Atlantic Recording Corp. v. Brennan, 2008 U.S. Dist. LEXIS 23801 at *3 (D. Conn. Feb. 13, 2008) (denying plaintiffs' entry of default against defendant, in part, by finding that defendant may have a meritorious defense against plaintiffs' "problematic" make available argument).

– Electra Entertainment Group, Inc. v. Doe, 2008 U.S. Dist. LEXIS 98145 at *8-9 (E.D.N.C. Dec. 4, 2008) (court need not decide whether "making available" a sound recording over the Internet constitutes a distribution because the plaintiffs' complaint sufficiently alleged an actual dissemination of copies of the recordings had occurred).

– Warner Bros. Records, Inc. v. Doe, 2008 U.S. Dist. LEXIS 98143 at *8-9 (E.D.N.C. Dec. 4, 2008) (same).

(1) Cases Holding That Mere Posting Is a Distribution

In Playboy Enterprises, Inc. v. Frena,[456] the court, with very little analysis of the issue, held a BBS operator liable for infringement of the public distribution right for the making of photographs available through the BBS that were downloaded by subscribers, even though the defendant claimed he did not make copies of the photographs himself. But because the BBS was apparently one devoted to photographs, much of it of adult subject matter, and subscribers routinely uploaded and downloaded images therefrom, the court seems to have viewed the defendant as a direct participant in the distributions to the public that took place through the BBS.

Similarly, in Playboy Enterprises, Inc. v. Chuckleberry Publishing Inc.,[457] the court ruled that uploading copyrighted pictorial images onto a computer in Italy which could be accessed by

---

[454] Id. at 967-71.

[455] Id. at 969 (emphasis added).

[456] 839 F. Supp. 1552 (M.D. Fla. 1993).

[457] 939 F. Supp. 1032, 1039 (S.D.N.Y. 1996).

users in the United States constituted a public distribution in the United States. In contrast to the Netcom case, the court noted that the defendant did more than simply provide access to the Internet. Instead, the defendant provided services and supplied the content for those services, which gave users the option to either view or download the images. By actively soliciting United States customers to the services, the court concluded that the defendant had distributed its product within the United States.

In Playboy Enterprises, Inc. v. Webbworld, Inc.,[458] the court held the defendants directly liable for infringing the distribution right by making copyrighted images available through a website for downloading by subscribers. The court found that, in contrast to the Netcom case, the defendants took "affirmative steps to cause the copies to be made."[459]

The court in Marobie-FL, Inc. v. National Association of Fire Equipment Distributors[460] ruled that the placement of three files containing copyrighted clip art on the Web page of the defendant constituted a direct violation of the plaintiff's distribution right because the files were available for downloading by Internet users and were transmitted to Internet users upon request.

In all of the preceding four cases, it was apparent that actual downloads of complete copies of the copyrighted material had taken place, and this fact, coupled with affirmative steps taken by the defendants to promote the acts of downloading, seem to have led those courts to find a violation of the distribution right. The more difficult cases of line drawing have arisen in the peer-to-peer file sharing cases, many of which are discussed in the remainder of this subsection and the next subsection, in which the defendant often merely makes available copyrighted files for sharing (through a "shared file" folder used by the peer-to-peer client software), but does not take additional affirmative steps to promote the downloading of copies of those files. In addition, there often is not clear proof in those cases whether actual downloads have taken place from the defendant's particular shared file folder, and if so, to what extent – including whether complete copies have been downloaded from the defendant's shared file folder or only bits and pieces of files, as is the inherent nature of the peer-to-peer protocol mechanisms.

In its decision in Napster I, the Ninth Circuit held, without any discussion, that "Napster *users* who upload files names to the search index for others to copy violate plaintiff's distribution rights."[461] Although the Ninth Circuit's opinion addressed whether Napster could be secondarily liable for the infringing acts of its users through the system, it did not address the question of whether Napster itself directly violated the plaintiff's distribution rights by maintaining its search index. That question was subsequently adjudicated by the district court in the Napster litigation, which answered the question in the negative, as discussed in the next subsection.

---

458 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

459 Id. at 1647.

460 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

461 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001) (emphasis added).

In Interscope Records v. Duty,[462] the court held that the mere placement of copyrighted works in a share folder connected to the Kazaa peer-to-peer service constituted a public distribution of those works. The court noted that, although "distribute" is not defined in the copyright statute, the right of distribution is synonymous with the right of publication, which is defined to include the "*offering* to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display."[463] The court also cited the Ninth Ciruit's decision in Napster I, which held that "Napster users who upload files names to the search index for others to copy violate plaintiff's distribution rights."[464]

In Warner Bros. Records, Inc. v. Payne,[465] the court ruled, on a motion to dismiss the plaintiff's complaint against a defendant who was making the plaintiff's recordings available through the Kazaa network, that "[l]isting unauthorized copies of sound recordings using an online file-sharing system constitutes an offer to distribute those works, thereby violating a copyright owner's exclusive right of distribution."[466] The court relied on the Supreme Court's equating of the term "distribute" with "publication" in Harper & Row Publishers, Inc. v. Nation Enterprises,[467] noting that publication is defined to include the "offering to distribute copies." The court also relied on the logic of Hotaling v. Church of Jesus Christ of Latter-Day Saints,[468] which held a library engages in the distribution of a copyrighted work when it adds the work to its collections, lists the work in its index or catalog and makes the work available for borrowing or browsing.[469] Accordingly, the court denied the defendant's motion to dismiss: "Making an unauthorized copy of a sound recording available to countless users of a peer-to-peer system for free certainly contemplates and encourages further distribution, both on the Internet and elsewhere. Therefore, the Court is not prepared at this stage of the proceedings to rule out the Plaintiffs' 'making available' theory as a possible ground for imposing liability. A more detailed understanding of the Kazaa technology is necessary and Plaintiffs may yet bring forth evidence of actual uploading and downloading of files, rendering use of the 'making available' theory unnecessary."[470]

In Universal City Studios Productions v. Bigwood,[471] the court granted summary judgment of infringement against the defendant, a user of Kazaa who had made two of the plaintiffs' copyrighted motion pictures available in his shared folder. Citing Hotaling and Napster I and no contrary authority, and without any further analysis of its own, the court ruled

---

462 2006 U.S. Dist. LEXIS 20214 (D. Ariz. Apr. 14, 2006).

463 Id. at *7 (citing 17 U.S.C. § 101) (emphasis by the court).

464 Id. at *8 (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001)).

465 2006 U.S. Dist. LEXIS 65765 (W.D. Tex. July 17, 2006).

466 Id. at *8.

467 471 U.S. 539 (1985).

468 118 F.3d 199 (4th Cir. 1997).

469 2006 U.S. Dist. LEXIS at *9-10.

470 Id. at *11.

471 441 F. Supp. 2d 185 (D. Me. 2006).

that "by using KaZaA to make copies of the Motion Pictures available to thousands of people over the internet, Defendant violated Plaintiffs' exclusive right to distribute the Motion Pictures."[472]

In Motown Record Co. v. DePietro,[473] the court, citing the Ninth Circuit's Napster I case, held that a "plaintiff claiming infringement of the exclusive-distribution right can establish infringement by proof of actual distribution or by proof of offers to distribute, that is, proof that the defendant 'made available' the copyrighted work [in this case, via a peer-to-peer system]."[474]

In United States v. Carani,[475] the court ruled that storing child pornography in a shared folder on the Kazaa peer-to-peer network where it could be downloaded by others qualified as an illegal "distribution" of child pornography, thus justifying an enhanced punishment.[476]

In ICG-Internet Commerce Group, Inc. v. Wolf,[477] the court denied a motion for summary judgment that the defendant had infringed the plaintiff's distribution right in an adult video by posting the video to the defendant's web site, because it was unclear from a screenshot of the defendant's web site showing a hyperlink to "[s]ex tape download souces [sic]" whether the hyperlink linked to a streaming or downloadable source file containing the plaintiff's video. The court did, however, find that the plaintiff's copy and public display rights had been violated by the posting of the video on the defendant's site from which it could be viewed publicly.[478]

In Maverick Recording Co. v. Harper,[479] in considering a copyright infringement claim against the defendant for having copies of the plaintiffs' copyrighted sound recordings in a shared folder on a peer-to-peer network, the court held that a complete download of a given work over the network is not required for copyright infringement to occur. Citing the Warner Bros. v. Payne and Interscope decisions, the court stated, "The fact that the Recordings were available for download is sufficient to violate Plaintiffs' exclusive rights of reproduction and distribution. It is not necessary to prove that all of the Recordings were actually downloaded; Plaintiffs need only prove that the Recordings were available for download due to Defendant's actions."[480]

On appeal, the Fifth Circuit ruled that it need not address whether merely making available files for download violates the distribution right because the defendant did not appeal the district court's finding that she had infringed the plaintiffs' copyrights by downloading and

---

[472] Id. at 190.

[473] 2007 U.S. Dist. LEXIS 11626 (E.D. Pa. Feb. 16, 2007).

[474] Id. at *12.

[475] 2007 U.S. App. LEXIS 16148 (7th Cir. July 6, 2007).

[476] Id. at *21-23; accord United States v. Shaffer, 472 F.3d 1219, 1123-24 (10th Cir. 2007).

[477] 519 F. Supp. 2d 1014 (E.D. Pa. 2007).

[478] Id. at 1018-19.

[479] Order, Maverick Recording Co. v. Harper, No. 5:07-CV-026-XR (W.D. Tex. Aug. 7, 2008).

[480] Id., slip op. at 10.

therefore reproducing the audio files. Thus, the distribution issue was moot since the defendant's liability would remain even if the Fifth Circuit were to agree with the district court on the distribution issue.[481] The Fifth Circuit also ruled that the defendant was not entitled to an innocent infringer defense as a matter of law because Section 402(d) makes that defense unavailable when a proper copyright notice appears on the published phonorecords to which a defendant had access. There was no dispute that each of the published phonorecords from which the shared audio files were taken had proper copyright notices on them, and lack of legal sophistication as to what the notices meant was irrelevant.[482] (The court does not mention whether the audio files themselves that the defendant shared had copyright notices on them.) Accordingly, the court concluded that the plaintiffs must be awarded statutory damages of $750 per infringed work.[483]

In Columbia Pictures Industries, Inc. v. Fung,[484] the court ruled, in the context of a BitTorrent site, that "uploading a copyrighted content file to other users (regardless of where those users are located) violates the copyright holder's § 106(3) distribution right."[485] Because of the nature of the BitTorrent protocol, users were not uploading the infringing content itself to the defendants' site, but rather were uploading dot-torrent files that contained only information about hosts from which the infringing content could be downloaded using the BitTorrent protocol. The dot-torrent files were indexed on the defendants' site for searching. Thus, the quoted language seems to implicitly hold that an actual distribution of infringing content is not required to infringe the distribution right, since the mere upload of the dot-torrent file through which the infringing content could be located was sufficient to infringe.

(2) Cases Holding That Mere Posting Is Not a Distribution

In Religious Technology Center v. Netcom On-Line Communication Services,[486] the court refused to hold either an OSP or a BBS operator liable for violation of the public distribution right based on the posting by an individual of infringing materials on the BBS. With respect to the BBS, the court stated: "Only the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are automatic and indiscriminate."[487] With respect to the OSP, the court noted: "It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration."[488]

---

[481] Maverick Recording Co. v. Harper, 598 F.3d 193, 197 (5th Cir. 2010).

[482] Id. at 198-99.

[483] Id. at 199.

[484] 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009).

[485] Id. at *29.

[486] 907 F. Supp. 1361, 1372 (N.D. Cal. 1995).

[487] Id. at 1372.

[488] Id.

In In re Napster, Inc. Copyright Litigation,[489] the district court rejected the plaintiffs' argument that Napster's indexing of MP3 files that its users posted on the Napster network made Napster a direct infringer of the plaintiffs' exclusive distribution rights. The plaintiffs relied on Hotaling v. Church of Jesus Christ of Latter-Day Saints,[490] which held a library engages in the distribution of a copyrighted work when it adds the work to its collections, lists the work in its index or catalog and makes the work available for borrowing or browsing. The Napster court distinguished the Hotaling case, arguing that the library had itself made actual, unauthorized copies of copyrighted materials made available to its borrowers. By contrast, Napster did not itself have a "collection" of recordings on its servers, but rather merely an index of recordings.[491] "This might constitute evidence that the listed works were available to Napster users, but it is certainly not conclusive proof that the songs identified in the index were actually uploaded onto the network in a manner that would be equivalent to the way in which the genealogical materials at issue in Hotaling were copied and distributed to the church's branch libraries."[492]

The court further noted that the definition of "publication" in the copyright statute, which the Supreme Court observed in a 1985 case that the legislative history equated with the right of distribution,[493] requires the distribution of copies or phonorecords of a work to the public or the offering to distribute copies of that work for purposes of further distribution, public performance, or public display. The court held that merely by indexing works available through its system, Napster was not offering to itself distribute copies of the works for further distribution by its users.[494]

The plaintiffs argued that the requirement of a transmission of a material object in order to find a violation of the distribution right was no longer viable in view of the recently enacted Artists' Rights and Theft Prevention Act of 2005 (the ART Act).[495] The plaintiffs cited Section 103(a)(1)(C) of the ART Act, codified at 17 U.S.C. § 506(a), which provides criminal sanctions for any person who willfully infringes a copyright by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public. The plaintiffs interpreted this provision as imposing criminal liability on any person who willfully makes an unauthorized copy of a copyrighted work available on a publicly accessible computer network while that work is being prepared for commercial distribution, and argued that Congress must have understood civil liability for copyright infringement to be equally broad.[496]

---

489 377 F. Supp. 2d 796 (N.D. Cal. 2005).

490 118 F.3d 199 (4th Cir. 1997).

491 In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 802-03.

492 Id. at 803.

493 Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985).

494 In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 803-05.

495 Pub. L. No. 109-9, 119 Stat. 218 (2005).

496 In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 804.

The court rejected this argument, noting that the ART Act did not amend Section 106(3) of the copyright statute, and in any event Section 103(a)(1)(C) of the ART Act makes clear that willful copyright infringement and making the work available on a computer network are separate elements of the criminal offense. Hence, the mere making available of an unauthorized work on a computer network should not be viewed as sufficient to establish a copyright infringement.[497] Accordingly, the court ruled that the defendants were entitled to summary judgment on the issue of direct liability on Napster's part by virtue of its index.[498] However, note that the Ninth Ciruit's earlier decision in Napster I held that "Napster users [as opposed to Napster itself] who upload files names to the search index for others to copy violate plaintiff's distribution rights."[499]

In Perfect 10 v. Google,[500] discussed in detail in Section II.C.4 above, the district court ruled that Google did not publicly distribute infringing copies of Perfect 10's copyrighted images that could be located through the Google Image Search function. "A distribution of a copyrighted work requires an 'actual dissemination' of copies. … In the internet context, an actual dissemination means the transfer of a file from one computer to another. Although Google frames and in-line links to third-party infringing websites, it is *those* websites, not Google, that transfer the full-size images to users' computers [upon clicking on a thumbnail version of the image displayed in the Google search results]. Because Google is not involved in the transfer, Google has not actually disseminated – and hence, [] has not distributed – the infringing content."[501]

On appeal, the Ninth Circuit affirmed this ruling. Because Google's search engine communicated only HTML instructions telling a user's browser where to find full size images on web site, and Google did not itself distribute copies of the infringing photographs, Google did not have liability for infringement of the right of distribution with respect to full size images that could be located and displayed through the Image Search function.[502] Perfect 10 argued that, under the Napster I and Hotaling cases discussed above, the mere making available of images violates the copyright owner's distribution right. The Ninth Circuit held that this "deemed distribution" rule did not apply to Google, because, unlike the users of the Napster system or the

---

497 Id. at 804-05.

498 Id. at 805. The court held, however, that the plaintiffs had submitted sufficient evidence of direct infringement by Napster's users in the form of a showing of massive uploading and downloading of unauthorized copies of works, together with statistical evidence strongly suggesting that at least some of the plaintiffs' copyrighted works were among them. Id. at 806. "It may be true that the link between such statistical evidence of copyright infringement and the uploading or downloading of specific copyrighted works is at the moment a weak one. However, to avoid summary judgment, plaintiffs need only establish that triable issue of material fact preclude entry of judgment as a matter of law. … Here in particular, the court is mindful of the fact that the parties have not even completed discovery relating to issues of copyright ownership and infringement." Id. at 806-07.

499 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001).

500 416 F. Supp. 2d 828 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

501 Id. at 844 (citing In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d 796, 802-04 (N.D. Cal. 2005)).

502 Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

library in Hotaling, Google did not own a collection of stored full size images that it made available to the public.[503]

In Latin American Music Co. v. Archdiocese of San Juan,[504] although not a case involving online activity, the First Circuit held that the defendant's mere listing in its licensing catalog of songs that it did not own the copyright for did not constitute infringement. The court ruled that mere authorization of an infringing act is insufficient basis for copyright infringement, as infringement depends upon whether an actual infringing act, such as copying or performing, has taken place.[505]

In London-Sire Records, Inc. v. Doe 1,[506] the court ruled that merely listing recordings as available for downloading on a peer-to-peer service did not infringe the distribution right. The court held that authorizing a distribution is sufficient to give rise to liability, but only if an infringing act occurs after the authorization.[507] The court rejected the plaintiff's argument to the contrary based on the Supreme Court's equating of the term "distribute" with "publication" in Harper & Row Publishers, Inc. v. Nation Enterprises.[508] The court noted that the Supreme Court stated only that Section 106(3) recognized for the first time a distinct statutory right of first publication, and quoted the legislative history as establishing that Section 106(3) gives a copyright holder the right to control the first public distribution of an authorized copy of his work.[509] The court went on to state, however, "That is a far cry from squarely holding that publication and distribution are congruent."[510]

The court noted that the statutory language itself suggests the terms are not synonymous. Noting that "publication" incorporates "distribution" as part of its definition ("publication" is "the distribution of copies or phonorecords of a work to the public"), the court reasoned:

> By the plain meaning of the statute, all "distributions … to the public" are publications. But not all publications are distributions to the public – the statute explicitly creates an additional category of publications that are not themselves distributions. For example, suppose an author has a copy of her (as yet unpublished) novel. If she sells that copy to a member of the public, it constitutes both distribution and publication. If she merely offers to sell it to the same member of the public, that is neither a distribution nor a publication. And if the author offers to sell the manuscript to a publishing house "for purposes of further

---

503 Id. at 1162-63. Cf. National Car Rental Sys. v. Computer Assocs. Int'l, Inc., 991 F.2d 426, 434 (8th Cir. 1993) (stating that infringement of the distribution right requires the actual dissemination of copies or phonorecords).

504 499 F.3d 32 (1st Cir. 2007).

505 Id. at 46-47.

506 542 F. Supp. 2d 153 (2008).

507 Id. at 166.

508 471 U.S. 539 (1985).

509 London-Sire, 542 F. Supp. 2d at 168.

510 Id.

distribution," but does not actually do so, that is a publication but not a distribution.[511]

Accordingly, the court concluded that the defendants could not be liable for violating the plaintiffs' distribution right unless a "distribution" actually occurred.[512] But that conclusion, did not, however, mean that the plaintiffs' pleadings and evidence were insufficient: "The Court can draw from the Complaint and the current record a reasonable inference in the plaintiffs' favor – that where the defendant has completed all the necessary steps for a public distribution, a reasonable fact-finder may infer that the distribution actually took place."[513]

The court also made the following additional rulings:

-- That the Section 106(3) distribution right is not limited to physical, tangible objects, but also confers on copyright owners the right to control purely electronic distributions of their work. The court reasoned that electronic files are "material objects" in which a sound recording can be fixed, and electronic distributions entail the movement of such electronic files, thereby implicating the distribution right.[514]

-- That actual downloads of the plaintiffs' works made by the plaintiffs' investigator were "sufficient to allow a statistically reasonable inference that at least one copyrighted work was downloaded at least once [by persons other than the investigator]. That is sufficient to make out a prima facie case for present purposes."[515]

In Elektra Entertainment Group, Inc. v. Barker,[516] contrary to the London-Sire Records decision (which incidentally was decided on the same day), the court ruled that, based on the legislative history of the copyright statute and the Supreme Court's Harper & Row decision, the words "distribution" and "publication" should be construed as synonymous, and therefore the right of distribution should be equated to the right of publication.[517] Accordingly, the court ruled that the same acts that would constitute a publication as defined in Section 101 of the copyright statute – namely, the "offer[] to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display" – would also violate the distribution right, and that proof of an actual transfer need not be shown.[518]

---

511 Id. at 169.

512 Id.

513 Id.

514 Id. at 169-71 & 172-74.

515 Id. at 176. "As noted above, merely exposing music files to the internet is not copyright infringement. The defendants may still argue that they did not know that logging onto the peer-to-peer network would allow others to access these particular files, or contest the nature of the files, or present affirmative evidence rebutting the statistical inference that downloads occurred."Id.

516 551 F. Supp. 2d 234 (S.D.N.Y. 2008).

517 Id. at 239-41.

518 Id. at 242 (quoting 17 U.S.C. § 101's definition of "publication").

However, the court rejected the plaintiff's argument that a violation of the distribution right could be established by a mere showing of the "making available" of copyrighted works by the defendant, as the plaintiffs had pled in their complaint. The court rejected the plaintiffs' argument that Congress' adoption of the WIPO Copyright Treaty, which contains an express right of "making available" a copyrighted work to the public, should control the interpretation of Section 106(3)'s distribution right. The court noted that, because the WIPO treaties were not self-executing, they created no private right of action on their own. The court was also unwilling to infer the intent of an earlier Congress when enacting amendments to the definition of the distribution right from the acts of a later Congress in ratifying the WIPO Copyright Treaty.[519] Accordingly, the court was unwilling to equate Congress' words, that the distribution right may be infringed by "[t]he offer[] to distribute copies or phonorecords to a group of person for purposes of further distribution, public performance, or public display," to what the court described as "the contourless 'make available' right proposed by Plaintiff."[520]

The court also rejected the argument in an amicus brief submitted by the MPAA that the plaintiffs' "make available" claim was supported by the introductory clause of Section 106, which gives the owner of a copyright the exclusive right "to authorize" the enumerated rights. The court cited and followed authority noting that Congress had added the "authorize" language to Section 106 in order to avoid any confusion that the statute was meant to reach contributory infringers, not to create a separate basis for direct infringement.[521]

The court did, however, give the plaintiffs the opportunity to amend their complaint to be faithful to the language of the copyright statute by alleging that the defendant had made an offer to distribute, and that the offer to distribute was for the purpose of further distribution, public performance, or public display.[522] In addition, the court denied the defendant's motion to dismiss the complaint entirely because the plaintiffs had adequately alleged that, in addition to making their works available, the defendant had actually distributed the plaintiffs' copyrighted works in direct violation of the distribution right.[523] In August of 2008 the case settled.[524]

In Atlantic Recording Corp. v. Howell,[525] seven major recording companies brought suit against the defendants, who had allegedly made over 4,000 files available for download in a shared folder on Kazaa. The private investigation company MediaSentry took screen shots showing the files that were available for download. The plaintiffs owned registered copyrights in 54 of the sound recordings in the folder. MediaSentry downloaded 12 of the copyrighted recordings from the defendants' computer, and the plaintiffs traced the computer to the

---

519 Id. at 242 n.7.

520 Id. at 243.

521 Id. at 245-46.

522 Id. at 244-45.

523 Id. at 245.

524 "RIAA Settles Pending 'Making Available' Claim," *BNA's Electronic Commerce & Law Report* (Aug. 27, 2008) at 1160.

525 554 F. Supp. 2d 976 (D. Ariz. 2008).

defendants and filed an action for copyright infringement. The plaintiffs filed a motion for summary judgment of infringement.[526]

The court denied the motion. Citing numerous decisions and two copyright treatises, the court noted the general rule that infringement of the distribution right requires an actual dissemination of either copies or phonorecords. The court rejected the plaintiffs' reliance on the Hotaling case and the Ninth Circuit's Napster I decision. With respect to Hotaling, the court noted that in that case the plaintiff had already proved that the library made unlawful copies and placed them in its branch libraries, so there had been actual distributions of copies in addition to listing of the unlawful copies in the library's catalog. With respect to the Napster I decision, the court noted that the Ninth Circuit in the later Perfect 10 v. Amazon case had grouped the holdings of Hotaling and Napster I together based upon the factual similarity that in both cases the owner of a collection of works made them available to the public. Only in such a situation could the holding of Hotaling potentially apply to relieve the plaintiff of the burden to prove actual dissemination of an unlawful copy of a work. The defendant in the Perfect 10 case did not own a collection of copyrighted works or communicate them to the public, so the Ninth Circuit found Hotaling inapplicable.[527] The Howell court went on to note the following:

> However, the court did hold that "the district court's conclusion [that distribution requires an 'actual dissemination'] is consistent with the language of the Copyright Act." That holding contradicts Hotaling and casts doubt on the single unsupported line from Napster upon which the recording companies rely.[528]

After surveying the many decisions addressing the issue, the court concluded that it agreed "with the great weight of authority that § 106(3) is not violated unless the defendant has actually distributed an unauthorized copy of the work to a member of the public. … Merely making an unauthorized copy of a copyrighted work available to the public does not violate a copyright holder's exclusive right of distribution."[529] In reaching its conclusion, the court rejected the plaintiffs' argument that "distribution" and "publication" are synonymous terms in the statute for all purposes. Rather, the court noted it was not clear that "publication" and "distribution" are synonymous outside the context of first publication, which was the subject of discussion in the Supreme Court's Harper & Row decision. Citing London-Sire, the court noted that while all distributions to the public are publications, not all publications are distributions.[530] The court concluded: "A plain reading of the statute indicates that a publication can be either a distribution or an offer to distribute for the purposes of further distribution, but that a distribution

---

526 Id. at 978.

527 Id. at 981-82.

528 Id. at 982 (quoting Perfect 10 v. Amazon.com, Inc., 487 F.3d 701, 718 (9th Cir. 2007) (superseded by 508 F.3d 1146 (9th Cir. 2007)).

529 554 F. Supp. 2d at 983.

530 Id. at 984.

must involve a 'sale or other transfer of ownership' or a 'rental, lease, or lending' of a copy of the work."[531]

Finally, the court noted that the plaintiffs' motion for summary judgment must also fail because they had not proved that a Kazaa user who places a copyrighted work into the shared folder distributes a copy of that work when a third party downloads it. The court noted that in the Kazaa system the owner of the shared folder does not necessarily ever make or distribute an unauthorized copy of the work. And if the owner of the shared folder simply provides a member of the public with access to the work and the means to make an unauthorized copy, the owner would not be liable as a primary infringer of the distribution right, but rather would be potentially liable only as a secondary infringer of the reproduction right.[532] The court therefore concluded that the plaintiffs' motion for summary judgment must fail because "they have not explained the architecture of the KaZaA file-sharing system in enough detail to determine conclusively whether the owner of the shared folder distributes an unauthorized copy (direct violation of the distribution right), or simply provides a third-party with access and resources to make a copy on their own (contributory violation of the reproduction right)."[533]

In Capitol Records Inc. v. Thomas,[534] the court sua sponte raised the issue of whether it had erred in instructing the jury that making sound recordings available for distribution on a peer-to-peer network, regardless of whether actual distribution was shown, qualified as distribution under the copyright act. The court concluded that it had erred and ordered a new trial for the defendant.[535] The parties agreed that the only evidence of actual dissemination of copyrighted works was that plaintiffs' infringement policing agent, MediaSentry, had downloaded songs. The defendant argued that dissemination to an investigator acting as an agent for the copyright owner cannot constitute infringement. The court rejected this argument, noting that Eighth Circuit precedent clearly approved of the use of investigators by copyright owners, and distribution to an investigator can constitute infringement.[536]

The court then turned to the issue of whether merely making available recordings for download constitutes unauthorized distribution. The court first noted that the plain language of Section 106(3) does not state that making a work available for sale, transfer, rental, lease or lending constitutes distribution, and two leading copyright treatises (Nimmer and Patry) agree that making a work available is insufficient to establish distribution. Congress' choice not to

---

[531] Id. at 985.

[532] Id. at 986.

[533] Id.

[534] 579 F. Supp. 2d 1210 (D. Minn. 2008).

[535] Id. at 1212 & 1227. The instruction to the jury read: "The act of making copyrighted sound recordings available for electronic distribution on a peer-to-peer network, without license from the copyright owners, violates the copyright owners' exclusive right of distribution, regardless of whether actual distribution has been shown." Id. at 1212.

[536] Id. at 1214-15.

include offers to do the acts enumerated in Section 106(3) further indicated its intent that an actual distribution or dissemination is required by Section 106(3).[537]

The court rejected the holding of other courts that the definition of "distribution" should be taken to be the same as that of "publication," noting that the legislative history does not expressly state that distribution should be given the same broad meaning as publication, and in any case, even if the legislative history indicated that some members of Congress equated publication with distribution under Section 106(3), that fact could not override the plain meaning of the statute. The court concluded that the statutory definition of publication is broader than the term "distribution" as used in Section 106(3). Specifically, under the definition in Section 101, a publication can occur by means of the distribution of copies of a work to the public, but it can also occur by offering to distribute copies to a group of persons for purposes of further distribution, public performance, or public display. Thus, while a publication effected by distributing copies of the work is a distribution, a publication effected by merely offering to distribute copies to the public is merely an offer of distribution, an actual distribution.[538]

The court rejected the plaintiffs' argument that Section 106 affords an exclusive right to authorize distribution (based on Section 106's language that "the owner of copyright under this title has the exclusive rights to do and to authorize any of the following …") and that making sound recordings available on a peer-to-peer network would violate such an authorization right. The court concluded that the authorization clause merely provides a statutory foundation for secondary liability, not a means of expanding the scope of direct infringement liability. The court reasoned that if simply making a copyrighted work available to the public constituted a distribution, even if no member of the public ever accessed that work, copyright owners would be able to make an end run around the standards for assessing contributory copyright infringement.[539]

Finally, the court rejected the arguments of the plaintiffs and various amici that the WIPO treaties require the U.S. to provide a making-available right and that right should therefore be read into Section 106(3). The court noted that the WIPO treaties are not self-executing and lack any binding legal authority separate from their implementation through the copyright act. The contents of the WIPO treaties would be relevant only insofar as Section 106(3) was ambiguous, and there was no reasonable interpretation of Section 106(3) that would align with the United States' treaty obligations. Concern for compliance with the WIPO treaties could not override the clear congressional intent in the language of Section 106(3).[540]

The defendant in this case, Jammie Thomas-Rasset, ultimately became the first peer-to-peer file sharer to defend infringement litigation all the way to a jury verdict. In July 2007, a jury concluded that she should pay $220,000 in statutory damages, but she was granted a motion for a new trial based on the erroneous jury instruction discussed above. In the second trial, the

---

[537] Id. at 1217-18.

[538] Id. at 1219-20.

[539] Id. at 1220-21.

[540] Id. at 1225-26.

jury returned a verdict for $1.92 million. The court later reduced the award to $54,000 but granted the plaintiffs' request for a new trial on damages. After a third trial, the jury again returned a special verdict that included a statutory damages award of $1.5 million ($62,500 for each shared song, multiplied by 24 songs).[541]

(3) Cases Refusing To Decide the Issue

In Arista Records LLC v. Does 1-16,[542] several record labels brought a copyright infringement claim against 16 unidentified defendants for illegally downloading and distributing the plaintiffs' copyrighted music through a peer-to-peer network and issued a subpoena seeking information from the State University of New York at Albany sufficient to identify each defendant. The defendants sought to quash the subpoena, in part on the basis that the plaintiffs' complaint was defective in that, in essence, according to the defendants, it alleged that the defendants were infringers because they were making available copyrighted song files, but without any evidence of actual distribution of those files to the public. The court refused to decide whether the mere "making available" of song files would be sufficient to violate the distribution right because the complaint did not use that language, but rather alleged that each defendant downloaded and/or distributed to the public copies of sound recordings.[543] "We are persuaded by the majority of cases and the school of thought that Plaintiffs have adequately pled that Defendants distributed Plaintiffs' copyrighted work, by merely stating, within the four corners of the Complaint, the distribution allegation alone. The tasks of pleading and proving that each Defendant actually distributed the copyright work do not necessarily collide at this juncture of the case, and dismissal of the Complaint would not be appropriate at this stage."[544]

2. The Requirement of a "Public" Distribution

Unlike the case of the public performance and public display rights, the copyright statute does not define what constitutes a "public" distribution. However, one might expect courts to afford a similarly broad interpretation of "public" with respect to the right of public distribution. Some distributions will clearly be "public," such as the posting of material on a Usenet newsgroup, and some will clearly not, such as sending e-mail to a single individual. Many other Internet distributions will fall in between. However, one might expect courts to treat distribution to members of the public by Internet access at different times and places as nevertheless "public," by analogy to the public performance and public display rights.

As previously discussed with respect to the public display right, the court in Playboy Enterprises, Inc. v. Hardenburgh,[545] held the defendant operators of a BBS directly liable for infringement of the public distribution right by virtue of making available photographs to

---

[541] "On Third Shot, Jury Returns $1.5 Million Statutory Damages Verdict Against P2P User," *BNA's Electronic Commerce & Law Report* (Nov. 10, 2010) at 1692.

[542] 2009 U.S. Dist. LEXIS 12159 (N.D.N.Y. Feb. 18, 2009).

[543] Id. at *15-16.

[544] Id. at *16-17.

[545] 982 F. Supp. 503 (N.D. Ohio 1997).

subscribers of the BBS for a fee, many of which were copyrighted photographs of the plaintiff Playboy Enterprises. The court's basis for finding liability was derived principally from the fact that the defendants had a policy of encouraging subscribers to contribute files, including adult photographs, to an "upload file" on the BBS and the defendants' practice of using a screening procedure in which its employees screened all files in the upload file to remove pornographic material and moved them into the generally available files for subscribers. These facts led the court to conclude that the defendants were active participants in the process of copyright infringement.

With respect to the requirement that the distributions be "to the public" in order to infringe the distribution right, the court ruled that "Defendants disseminated unlawful copies of [the plaintiff's] photographs to the public by adopting a policy in which [the defendants'] employees moved those copies to the generally available files instead of discarding them."[546] The court also concluded that the defendants were liable for contributory infringement by virtue of their encouraging of subscribers to upload information to the BBS with at least constructive knowledge that infringing activity was likely to be occurring on their BBS.[547]

3. The Requirement of a Rental or Transfer of Ownership

The public distribution right requires that there have been either a rental or a transfer of ownership of a copy. If material is distributed free, as much of it is on the Internet, there is no sale, rental, or lease, and it is therefore unclear whether a sale or a "transfer of ownership" has taken place. With respect to distributions in which the recipient receives a complete copy of the work on the recipient's computer, perhaps a "transfer of ownership" should be deemed to have taken place, since the recipient has control over the received copy.

It is unclear precisely what a "rental" means on the Internet. For example, is a download of an on-demand movie a "rental"? In a sense, the user pays a "rental" fee to watch the movie only once. However, the downloaded bits of information comprising the movie are never "returned" to the owner, as in the case of the usual rental of a copy of a work. These unanswered questions lend uncertainty to the scope of the distribution right on the Internet.

4. The Right of Distribution Under the WIPO Treaties

Article 6 of the WIPO Copyright Treaty provides that authors of literary and artistic works shall enjoy "the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership." This right seems potentially broader than the public distribution right under current U.S. law, because it includes the mere "making available" of copies of works to the public, whereas U.S. law currently reaches only the actual distribution of copies.

It is unclear whether this "making available" right reaches the mere posting of copies on the Internet. The Agreed Statement for Article 6 provides: "As used in these Articles, the

---

[546] Id. at 513.

[547] Id. at 514.

expressions 'copies' and 'original and copies,' being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects." One interpretation of the Agreed Statement is that a copy posted on the Internet, being electronic in format, is not capable of being "put into circulation as tangible objects."

On the other hand, one might argue that at least complete copies downloaded to permanent storage at recipient computers should be treated as the equivalent of circulation of copies "as tangible objects." If, for example, copies of a book were sold on floppy disks rather than on paper, such floppy disks might well be treated as the placement of copies into circulation as tangible objects. Yet a network download can result in a copy on a floppy disk (or a hard disk) at the recipient's computer. One could therefore argue that the transmission of electronic copies to "physical" storage media at the receiving end should be treated as within the distribution right of the WIPO treaty.

In any event, this "making available" right might more easily reach BBS operators and OSPs through which works are "made available" on the Internet. It is unclear whether a requirement of volition will be read into Article 6 for liability, as some U.S. courts have required for liability under the current rights of public distribution, display and performance. Moreover, because the WIPO Copyright Treaty does not define the "public," the same ambiguities will arise as under current U.S. law concerning what type of availability will be sufficient to be "public," particularly with respect to the "making available" of works to limited audiences.

Articles 8 and 12 of the WIPO Performances and Phonograms Treaty contain rights of distribution very similar to that of Article 6 of the WIPO Copyright Treaty,[548] so the same ambiguities noted above will arise.

5. The Right of Distribution Under WIPO Implementing Legislation

(a) United States Legislation

The DMCA does not contain any provisions that would modify the right of distribution as it exists under current United States law. Thus, the DMCA implicitly deems the current right of public distribution to be equivalent to the Article 6 right.

---

[548] Article 8(1) provides, "Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership." Article 12(1) provides, "Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their phonograms through sale or other transfer of ownership."

Like the Agreed Statement for the WIPO Copyright Treaty quoted in the text, the Agreed Statement for Articles 8 and 12 of the WIPO Performances and Phonograms Treaty provides: "As used in these Articles, the expressions 'copies' and 'original and copies,' being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects."

(b) The European Copyright Directive

Article 4(1) of the European Copyright Directive requires member states to "provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorize or prohibit any form of distribution to the public by sale or otherwise." Use of the phrase "any form" of distribution suggests that a broad right is intended, although, as in the United States, the right applies only with respect to the distribution of "copies."[549] Consistent with the Agreed Statement of the WIPO Copyright Treaty, the comments to Article 4(1) of the European Copyright Directive recite that "the expressions 'copies' and 'originals and copies,' being subject to the distribution right, refer exclusively to fixed copies that can be put into circulation as tangible objects."[550]

Thus, although use of the phrase "any form" of distribution might suggest that all online transmissions of copyrighted works would fall within the distribution right of the European Copyright Directive, the comments limit the distribution right "to fixed copies that can be put into circulation as tangible objects." It seems that the drafters of the European Copyright Directive intended the right of communication to the public, rather than the right of distribution, to cover online transmissions of copyrighted works, for Recital (23) states that the right of communication to the public "should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts."

E. The Right of Importation

Section 602(a) of the copyright statute provides that "importation into the United States ... of copies or phonorecords of a work that have been acquired outside the United States is an infringement of the exclusive right to distribute copies ...." One purpose of Section 602(a) was to allow a copyright owner to prevent distribution into the United States of copies of works that, if made in the United States, would have been infringing, but were made abroad outside the reach of United States copyright law.

Section 602(a) was obviously drafted with a model of physical copies in mind. "Importation" is not defined in the copyright statute, but the requirement that copies of a work be "acquired outside the United States" might suggest that "importation" means the movement of physical copies into the United States.[551] It is unclear how this right will be applied to Internet transmissions into the United States, with respect to which no physical copies in a traditional sense are moved across national borders. Because the NII White Paper takes the position that the stream of data sent during a transmission does not constitute a "copy" of a copyrighted work, the NII White Paper concludes that the Section 602(a) importation right does not apply to network

---

[549] Art. 4(2) deals with exhaustion of the distribution right under the first sale doctrine, and will be discussed in Section III.F below.

[550] Commentary to Art. 4, ¶ 1.

[551] Lemley, supra note 6, at 564.

transmissions into the United States,[552] and recommends that Section 602 be amended to include importation by transmission of copies, as well as by carriage or shipping of them.[553]

However, because physical copies often end up on a computer in the United States as a result of network transmissions into the United States, it is possible that the importation right will be construed analogously to the distribution right with respect to transmissions, especially since the importation right is defined in Section 602(a) in terms of the distribution right. Thus, if a transmission is deemed to be within the distribution right, then it is possible that the importation right will be construed to apply when transmissions of copies are made into the United States from abroad.

In any event, the new right of communication to the public afforded under the WIPO treaties, discussed in the next section, could help plug any hole that may exist in the traditional importation right, at least with respect to transmissions into the United States that qualify as "communications to the public," if the such right is adopted in implementing legislation (as noted in the next section, however, the DMCA does not contain an explicit right of communication to the public).

F. The New Right of Transmission and Access Under the WIPO Treaties

The WIPO treaties each afford a broad new right of transmission and access to a copyrighted work. The right is denominated a "right of communication to the public" in the WIPO Copyright Treaty, and is denominated a "right of making available to the public" in the WIPO Performances and Phonograms Treaty. Despite the difference in denomination, the rights appear to be very similar.

1. The Right of Communication to the Public in the WIPO Copyright Treaty

Article 8 of the WIPO Copyright Treaty provides a new right of "communication to the public" as follows:

> Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.

This new extended right of communication to the public is clearly meant to cover online dissemination of works, and in that sense is broader than the existing rights of communication to the public in the Berne Convention, which are confined to performances, broadcasts, and

---

[552] NII White Paper at 68.

[553] Id. at 135.

recitations of works. Specifically, Article 11(1)(ii) of the Berne Convention provides that authors of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorizing "any communication to the public of the performance of their works." Article 11*bis*(1)(ii) provides that authors of literary and artistic works shall enjoy the exclusive right of authorizing "any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one." Finally, Article 11*ter*(1)(ii) provides that authors of literary works shall enjoy the exclusive right of authorizing "any communication to the public of the recitation of their works."

The new right of communication to the public in the WIPO Copyright Treaty appears to be broader than the existing rights of reproduction, display, performance, distribution, and importation under current United States law in the following ways:

- No Requirement of a Copy. The right does not require the making or distribution of "copies" of a work. It therefore removes the potential limitations on the rights of reproduction and distribution under United States law stemming from the requirement of a "copy."

- Right of Transmission. It affords the exclusive right to control any "communication to the public" of a work "by wire or wireless means." Although "communication" is not defined in the WIPO Copyright Treaty, the reference to a communication "by wire or wireless means" seems clearly applicable to electronic transmissions of works (a right of transmission). This conclusion is bolstered by the fact that Article 2(g) of the WIPO Performances and Phonograms Treaty does contain a definition of "communication to the public," which is defined in terms of "transmission to the public by any medium, other than broadcasting."[554] This transmission right will potentially site the infringement at the place of transmission, in addition to the point of receipt of a transmitted work (under the reproduction right).

- Right of Authorization. It also affords the exclusive right of "authorizing" any communication to the public. No actual communications to the public are apparently necessary to infringe the right.

- Right of Access. The right of authorizing communications to the public explicitly includes "making available to the public" a work "in such a way that members of the public may access" the work "from a place and a time individually chosen by them" (a right of access).[555] This access right would seem to allow the copyright holder to

[554] Article 2(f) of the WIPO Performances and Phonograms Treaty defines "broadcasting" to mean "the transmission by wireless means for public reception of sounds or of images and sounds or of the representations thereof ...." This definition seems to contemplate isochronous transmission.

[555] Although "public" is not defined in the WIPO Copyright Treaty, the reference in Article 10 to access by members of the public "from a place and at a time individually chosen by them" is very similar to the definition of display or performance of a work "publicly" in Section 101 of the U.S. copyright statute, which applies "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."

remove an infringing posting of a work prior to any downloading of that work. This right may also expand potential liability beyond just posters or recipients of infringing material on the Internet to include OSPs and BBS operators, who could be said to make a work available to the public in such a way that members of the public may access it.

The Agreed Statement for Article 8, however, appears aimed at limiting the breadth of the net of potential liability that Article 8 might establish. The Agreed Statement provides: "It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11*bis*(2)." It is unclear who the "mere" provider of "physical facilities" was meant to reference – only the provider of telecommunications lines (such as phone companies) through which a work is transmitted, or other service providers such as OSPs or BBS operators, who may provide "services" in addition to "facilities."

Another unclear point with respect to the scope of the right of communication to the public is who the "public" is. Neither the WIPO Copyright Treaty nor the European Copyright Directive provide any explanation of "to the public," although the Commission in its 1997 commentary to one of the earlier drafts of the Directive stated that "public" included "individual members of the public," but went on to state that "the provision does not cover mere private communications."[556]

The right of transmission and access under Article 8 of the WIPO Copyright Treaty is similar to (and potentially broader than) the amendment to U.S. copyright law proposed in the NII White Paper "to expressly recognize that copies or phonorecords of works can be distributed to the public by transmission, and that such transmissions fall within the exclusive distribution right of the copyright owner."[557] The NII White Paper's proposal would expand the distribution right, as opposed to creating a wholly new right, as the WIPO Copyright Treaty does. The amendment proposed by the NII White Paper proved to be very controversial, and implementing legislation introduced in Congress in 1996 ultimately did not win passage.

2. The Right of Making Available to the Public in the WIPO Performances and Phonograms Treaty

Articles 10 and 14 of the WIPO Performances and Phonograms Treaty grant analogous rights for performers and producers of phonograms to the right of "communication to the public" contained in Article 8 of the WIPO Copyright Treaty. The WIPO Performances and Phonograms Treaty, however, casts these rights as ones of "making available to the public." Specifically, Article 10 of the WIPO Performances and Phonograms Treaty provides:

---

[556] Harrington & Berking, supra note 206, at 4.

[557] NII White Paper at 130.

> Performers shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

Thus, Article 10 provides an exclusive right with respect to analog and digital on-demand transmission of fixed performances.[558]

> Similarly, Article 14 provides:
>
> Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

No Agreed Statements pertaining to Articles 10 and 14 were issued.

Article 2(b) of the WIPO Performances and Phonograms Treaty defines a "phonogram" to mean "the fixation of the sounds of a performance or of other sounds, or of a representation of sounds other than in the form of a fixation incorporated in a cinematographic or other audiovisual work." Article 2(c) defines "fixation" broadly as "the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device." Under this definition, storage of sounds on a computer would constitute a "fixation," and the fixed copy of such sounds would therefore constitute a "phonogram." Accordingly, the making available to the public of sounds stored on a computer would seem to fall within the access rights of Articles 10 and 14.

Because there were no Agreed Statements generated in conjunction with Sections 10 and 14 of the WIPO Performances and Phonograms Treaty, there is no Agreed Statement similar to that accompanying Article 8 in the WIPO Copyright Treaty for limiting liability for the mere provision of physical facilities for enabling or making transmissions. Accordingly, one will have to await the implementing legislation in the various countries to know how broadly the rights set up in Articles 10 and 14 will be codified into copyright laws throughout the world.

---

[558] Rebecca F. Martin, "The WIPO Performances and Phonograms Treaty: Will the U.S. Whistle a New Tune?", J. Copyright Soc'y U.S.A., Spring 1997, at 157, 178. Art. 8 provides a correlative distribution right with respect to more traditional forms of distribution: "Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership." The WIPO Performances and Phonograms Treaty also grants to authors in Art. 6 the exclusive right of authorizing "the broadcasting and communication to the public of their unfixed performances except where the performance is already a broadcast performance" as well as "the fixation of their unfixed performances."

3. The Right of Transmission and Access Under WIPO Implementing Legislation

(a) United States Legislation

The DMCA does not contain any express implementation of a right of "communication to the public" or of "making available to the public." In view of this, the uncertainties discussed previously concerning whether the mere transmission or access of a copyrighted work through an online medium falls within existing United States rights of reproduction, distribution, public display, or public performance remain under the DMCA.

With respect to the Article 10 right of making available to the public of fixed performances, the recently enacted Digital Performance Rights in Sound Recordings Act grants these rights for digital transmissions, although not for analog transmissions.[559] However, because the WIPO Performances and Phonograms Treaty grants these rights with respect to both digital and analog transmissions, as well as with respect to spoken or other sounds in addition to musical works, it would seem that the United States might have to amend its copyright laws to comply with the requirements of Article 10.[560]

Although the DMCA does not contain any express rights of transmission or access, recent case law suggests that courts may interpret existing copyright rights to afford the equivalent of a right of transmission and access. For example, in the recent case of Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,[561] discussed previously, the court concluded that the mere making available of the files for downloading was sufficient for liability, because "once the files were uploaded [onto the Web server], they were available for downloading by Internet users and … the [OSP] server transmitted the files to some Internet users when requested."[562] From this statement, it appears that the court construed the distribution and public display rights to cover both the making available of the clip art to the public on the Web page (a right of access), as well as subsequent downloads by users (a right of transmission).

(b) The European Copyright Directive

The European Copyright Directive explicitly adopts both the right of communication to the public of copyrighted works and the right of making available to the public of fixed performances, by wire or wireless means, in language that parallels that of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. Specifically, Article 3(1) of the European Copyright Directive provides the following with respect to copyrighted works:

> Member States shall provide authors with the exclusive right to authorize or prohibit any communication to the public of their works, by wire or wireless

---

559 17 U.S.C. § 106(6).

560 Martin, supra note 558, at 178-79.

561 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

562 Id. at *12.

> means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

The comments to Article 3 define "communication to the public" to cover "any means or process other than the distribution of physical copies. This includes communication by wire or by wireless means,"[563] which clearly encompasses a right of transmission. Indeed, the comments explicitly note: "One of the main objectives of the provision is to make it clear that interactive 'on-demand' acts of transmissions are covered by this right."[564] This theme is picked up in Recital (25) of the European Copyright Directive, which states, "It should be made clear that all rightholders recognized by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterized by the fact that members of the public may access them from a place and at a time individually chosen by them." Recital (27), however, echoes similar statements in the WIPO Copyright Treaty when it states that the "mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive." The Recitals do not clear up the ambiguity previously noted in the WIPO Treaty as to who the "mere" provider of "physical facilities" was meant to reference – only the provider of telecommunications lines (such as phone companies) through which a work is transmitted, or other service providers such as OSPs or BBS operators.

The comments to the European Copyright Directive also make clear that Article 3(1) affords a right to control online access to a work, apart from actual transmissions of the work:

> As was stressed during the WIPO Diplomatic Conference, the critical act is the "making available of the work to the public," thus the offering a work on a publicly accessible site, which precedes the stage of its actual "on-demand transmission." It is not relevant whether it actually has been retrieved by any person or not. The "public" consists of individual "members of the public."[565]

Similarly, Article 3(2) of the European Copyright Directive affords a right of making available to the public of fixed performances by wire or wireless means:

> Member States shall provide for the exclusive right to authorize or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
>
> (a) for performers, of fixations of their performances;

---

[563] Commentary to Art. 3, ¶ 1.

[564] Id. ¶ 2.

[565] Id.

(b) for phonogram producers, of their phonograms;

(c) for the producers of the first fixation of films, of the original and copies of their films;

(d) for broadcasting organizations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

The right of Article 3(2) of the European Copyright Directive is actually broader than the right required under Article 10 of the WIPO Performances and Phonograms Treaty. The Article 10 right of making available to the public applies only to performances fixed in "phonograms," which Article 2 defines to mean the fixation of the "sounds of a performance or of other sounds other than in the form of a fixation incorporated in a cinematographic or other audiovisual work." The Article 3(2) right of the European Copyright Directive goes further, covering fixed performances of audiovisual material as well. The comments to Article 3(2) of the European Copyright Directive justify this extension of the right on the ground that audiovisual productions or multimedia products are as likely to be available online as are sound recordings.[566]

In sum, the European Copyright Directive explicitly grants a right of transmission and access to copyrighted works and fixed performances, whereas the DMCA does not. It remains to be seen how broadly these rights mandated under the European Copyright Directive will be adopted in implementing legislation in EC member countries. However, this disparity between the express rights afforded under United States law and the European Copyright Directive raises considerable potential uncertainty. First, at a minimum, use of different language to denominate the various rights among countries may breed confusion. Second, differences of scope of the rights of transmission and access are likely to arise between the United States and the EC by virtue of the fact that these rights are spelled out as separate rights in the EC, whereas, if they exist at all, they are subsumed under a collection of various other rights in the United States. Adding further to the potential confusion is the possibility that some EC member countries may adopt these rights expressly, as mandated by the European Copyright Directive, whereas other countries may, like the United States, deem them to be subsumed in other rights already afforded under that country's laws.

Because online transmissions through the Internet are inherently global, these disparities raise the possibility that rights of varying scope will apply to an online transmission as it travels through computers in various countries on the way to its ultimate destination. Similarly, legal rights of varying scope may apply depending upon in which country a work is actually first accessed. Given the ubiquitous nature of caching on the Internet, the site of the access may be arbitrary from a technical point of view, but significant from a legal point of view. Such a situation would not afford the international uniformity that the WIPO treaties seek to establish.

---

[566] Id. ¶ 3.

G. New Rights and Provisions Under The Digital Millennium Copyright Act, the European Copyright Directive & Legislation That Did Not Pass

This Section discusses a number of new rights and provisions related to various areas of copyright law that are contained in the DMCA and the European Copyright Directive. In addition, this Section discusses a number of interesting rights and provisions concerning copyright in the online context that were contained in proposed legislation that did not pass Congress. These provisions are indicators of areas where future legislation and/or debate may arise.

1. Circumvention of Technological Measures and Rights Management Information Under the DMCA

Both the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty require signatories to establish certain obligations with respect to circumvention of technological measures to protect copyrighted works and the preservation and use of certain "rights management information."

With respect to the circumvention of technological measures, Article 11 of the WIPO Copyright Treaty and Article 18 of the WIPO Performances and Phonograms Treaty require treaty signatories to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures" that are used by authors, performers and producers of phonograms to restrict acts with respect to their copyrighted works that are not authorized by the rights holders or permitted by law.[567]

With respect to the preservation and use of rights management information, Article 12 of the WIPO Copyright Treaty and Article 19 of the WIPO Performances and Phonograms Treaty require treaty signatories to provide adequate and effective legal remedies against any person performing any of the following acts knowing (or, with respect to civil remedies, having reasonable grounds to know) "that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention": (i) removing or altering any electronic rights management information without authority or (ii) distributing, importing for distribution, broadcasting or communicating to the public, without authority, copies of works knowing that electronic rights management information has been removed or altered without authority. The treaties define "rights management information" as "information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public."

---

[567] Shortly after the WIPO treaties were adopted, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks Bruce Lehman, who headed the U.S. delegation at the WIPO Conference, noted that this provision is somewhat broader than the statutory language proposed on the subject in Congress before adoption of the treaties. He noted that implementation of this treaty provision would therefore require new legislation. "WIPO Delegates Agree on Two Treaties," *BNA's Electronic Information Policy & Law Report* (Jan. 3, 1997) at 23.

This subsection 1 discusses the implementation of these rights in the DMCA. The following subsection 2 discusses the implementation of these rights under the European Copyright Directive.

The four bills that were introduced in Congress to implement the WIPO treaties adopted one of two approaches to the circumvention of technological measures and rights management information. The first approach, contained in H.R. 2281 and S. 2037 and ultimately adopted in the DMCA, outlawed both conduct and devices directed toward or used for circumventing technological copyright protection mechanisms. The second approach, contained in S. 1146 and H.R. 3048 but not passed by Congress, outlawed only conduct involving the removal or deactivation of technological protection measures. Although Bruce Lehman conceded that the WIPO treaties do not mandate adoption of a device-based approach, he and other supporters of this approach argued that a conduct-only approach would be difficult to enforce and that meaningful legislation should control the devices used for circumvention.[568]

The DMCA adds several new provisions to the Copyright Act, which are contained in a new Chapter 12.

(a) Circumvention of Technological Protection Measures

(1) Prohibition on Conduct

Section 1201(a)(1) of the DMCA outlaws conduct to circumvent protection mechanisms that control access to a copyrighted work: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Note that this provision does not expressly require either knowledge or intent, and is therefore potentially very broad in its reach – the language states that the mere act of circumvention is a violation, and does not expressly require that an infringement follow the circumvention act (although some courts have grafted such a requirement as discussed below). Section 1201(a)(3) defines "circumvent a technological measure" as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." That section further provides that a technological protection measure "effectively controls access to a work" if "the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."

Section 1201(a)(1) provides that the prohibition on circumventing a technological measure to gain unauthorized access to a work does not take effect until the end of a two-year period beginning on the date of enactment of the bill – the two year waiting period expired on October 28, 2000, and the prohibition is now in effect.

---

[568] Cunard & Coplan, "WIPO Treaty Implementation: Debate Over OSP Liability," *Computer Law Strategist* (Oct. 1997) 1, 3.

(i) Exemptions Adopted by the Librarian of Congress

Section 1201(a)(1) requires the Librarian of Congress, upon recommendation of the Register of Copyrights and in consultation with the Assistant Secretary of Commerce for Communications and Information, to conduct a rulemaking[569] during the initial two-year period, and during each succeeding three-year period, to determine whether certain types of users of copyrighted works are, or are likely to be, adversely affected by the prohibition in Section 1201(a)(1).[570] The Librarian must publish a list of particular classes of copyrighted works for which the rulemaking determines that noninfringing uses have been, or are likely to be, adversely affected, and the prohibitions of Section 1201(a) shall not apply to such users with respect to such class of works for the ensuing three-year period.

The Exemptions of 2000. On Oct. 27, 2000, the Copyright Office published the first set of classes of copyrighted works that the Librarian of Congress determined would be exempt from the anti-circumvention provisions of Section 1201(a)(1), with the exemption to be in effect until Oct. 28, 2003.[571] Those classes, which were only two in number and very narrowly defined, were as follows:

1. Compilations consisting of lists of websites blocked by filtering software and applications. The Librarian determined that an exemption was necessary to avoid an adverse effect on persons who wish to criticize and comment on such lists, because they would not be able to ascertain which sites are on the lists unless they circumvented encryption protecting the contents of the lists.[572]

2. Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness. The Librarian determined that an exemption was necessary to gain access to literary works protected by access control mechanisms, such as dongles or other mechanisms, that malfunction or become obsolete.[573]

The Exemptions of 2003. On Oct. 27, 2003, the Copyright Office issued the second determination of the classes of copyrighted works that the Librarian decided should have an

---

569 As originally passed by Congress, section 1201(a)(1) required that the rulemaking be on the record. However, the Intellectual Property and Communications Omnibus Reform Act of 1999, P.L. 106-113, passed by Congress on Nov. 19, 1999 and signed by the President in late 1999, removed the requirement that the rulemaking be "on the record."

570 Section 1201(a)(C) provides that in conducting the rulemaking, the Librarian shall examine the availability for use of copyrighted works; the availability for use of works for nonprofit archival, preservation, and educational purposes; the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; and the effect of circumvention of technological measures on the market for or value of copyrighted works.

571 65 Fed. Reg. 64556 (Oct. 27, 2000).

572 Id. at 64564.

573 Id. at 64564-66. For the Copyright Office's rationale for rejecting an exemption for a host of other proposed classes of works, see id. at 64566-74.

exemption, with the exemption to be in effect until Oct. 27, 2006.[574] The classes, which were only four in number and even more specifically defined than the first set of classes,[575] were as follows:

1. Compilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of email.[576] The Librarian defined "Internet locations" to "include domains, uniform resource locators (URLs), numeric IP addresses or any combination thereof.[577] This class is similar to the first class of exemptions in the Librarian's first determination, but was narrowed so as to exclude the ability to circumvent blocked lists associated with firewalls, anti-virus software and anti-spam software.[578]

2. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. This class is similar to the second class of exemptions in the Librarian's first determination, but was narrowed to cover only the case of obsolete dongles because the Librarian found that this was the only class for which adequate factual support of potential harm had been submitted in the second rulemaking proceeding.[579] The Librarian defined "obsolete" as "no longer manufactured or reasonably available in the commercial marketplace."[580]

3. Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial

---

574 68 Fed. Reg. 62011 (Oct. 31, 2003).

575 A statement accompanying the Librarian's decision with respect to the exempted classes partially explained the narrowness of the classes: "It is important to understand the purposes of this rulemaking, as stated in the law, and the role I have in it. The rulemaking is not a broad evaluation of the successes or failures of the DMCA. The purpose of the proceeding is to determine whether current technologies that control access to copyrighted works are diminishing the ability of individuals to use works in lawful, noninfringing ways. The DMCA does not forbid the act of circumventing copy controls, and therefore this rulemaking proceeding is not about technologies that control copying. Some of the people who participated in the rulemaking did not understand that and made proposals based on their dissatisfaction with copy controls. Other participants sought exemptions that would permit them to circumvent access controls on all works when they are engaging in particular noninfringing uses of those works. The law does not give me that power." Statement of the Librarian of Congress Relating to Section 1201 Rulemaking, available as of Oct. 30, 2003 at www.copyright.gov/1201/docs/librarian_statement_01.html.

576 68 Fed. Reg. at 62013.

577 Id.

578 Id.

579 Id. at 62013-14.

580 Id. at 62018.

marketplace. The Librarian determined that this exemption is necessary to allow archiving or continued use of computer programs and video games that are subject to "original media only" restrictions, are stored on media no longer in use, such as 5.25" floppy disks, or require use of an obsolete operating system.[581]

4. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format. The Librarian defined "specialized format," "digital text" and "authorized entities" to have the same meaning as in 17 U.S.C. § 121.[582] The Librarian determined that this exemption is necessary in response to problems experienced by the blind and visually impaired in gaining meaningful access to literary works distributed as ebooks.[583]

For the Copyright Office's rationale for rejecting an exemption for a host of other proposed classes of works, see 68 Fed. Reg. at 62014-18. One of the more interesting proposed exemptions that the Copyright Office rejected was one submitted by Static Control Components, Inc. in response to the district court's ruling in the case of Lexmark International, Inc. v. Static Control Components, Inc.,[584] discussed in Section II.G.1(o)(1) below. In that case, the district court ruled on a motion for a preliminary injunction that Static Control violated Section 1201(a)(2) by distributing microchips that were used to replace the microchip found in plaintiff Lexmark's toner cartridges so as to circumvent Lexmark's authentication sequence that prevented the printer engine software on the Lexmark printer from allowing the printer to operate with a refilled toner cartridge. In view of this ruling, Static Control submitted a proposed exemption to the Copyright Office to permit circumvention of access controls on computer programs embedded in computer printers and toner cartridges and that control the interoperation and functions of the printer and toner cartridge. The Copyright Office concluded that the statutory exemption set forth in Section 1201(f), discussed in Section II.G.1(g) below, already adequately addressed the concerns of toner cartridge re-manufacturers.[585] The rationale for the Copyright Office's conclusion is discussed further in Section II.G.1(g) below.

The Exemptions of 2006. On Nov. 27, 2006, the Copyright Office issued the third determination of the classes of copyrighted works that the Librarian decided should have an exemption, with the exemption to be in effect until Oct. 27, 2009.[586] In previous rulemakings,

---

[581] Id. at 62014.

[582] Id.

[583] Id.

[584] 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003), rev'd, 387 F.3d 522 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27,422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6rh Cir. Feb. 15, 2005).

[585] 68 Fed. Reg. at 62017.

[586] 71 Fed. Reg. 68472 (Nov. 27, 2006). On Oct. 27, 2009, the Librarian of Congress extended the 2006 exemptions on an interim basis until the Copyright Office and Librarian of Congress could complete their decision with respect to the next classes of exemptions to be granted. See 74 Fed. Reg. 55139 (Oct. 27, 2009). The extension period turned out to be 9 months, ending on July 26, 2010.

the Copyright Office had determined that an exempted class must be based primarily on attributes of the work itself and not the nature of the use or the user. In its 2006 ruling, the Copyright Office determined for the first time that in certain circumstances it would be permissible to refine the description of a class of works by reference to the type of user who may take advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption, and the Copyright Office applied this refinement to some of the classes of works exempted.[587]

The exempted classes of works in the 2006 ruling were the following:

1. "Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors."[588] This exemption was the first one to define the class by reference to particular types of uses and users.

2. "Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace."[589] This exemption is the same as the third class in the 2003 ruling, except that a definition of what renders constitutes an obsolete format was added.

3. "Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace."[590] This exemption is the same as the second class in the 2003 ruling.

4. "Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format."[591] This exemption is similar to the fourth class in the 2003 ruling, except that the two requirements in the description of the access controls is phrased in the disjunctive, whereas in the 2003 ruling it was phrased in the conjunctive.

5. "Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished

---

[587] Id. at 68473-74.

[588] Id.

[589] Id. at 68474.

[590] Id. at 68475.

[591] Id.

for the sole purpose of lawfully connecting to a wireless telephone communication network."[592] This is a new exemption, and is another one defined by reference to a particular type of use. The purpose of this exemption is to address the use of software locks that prevent customers from using their handsets on a competitor's network, even after all contractual obligations to the original wireless carrier have been satisfied, by controlling access to the firmware that operates the mobile phone. The Copyright Office justified the exemption by noting that "in this case, the access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to switch to other carriers, a business decision that has nothing whatsoever to do with the interests protected by copyright. … When application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third party who may use § 1201 to control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted."[593] The rationale underlying this class is an important one, and may be applied to justify more exempted classes in future rulemakings by the Copyright Office.

6. "Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."[594] This exemption was prompted by the notorious case of the DRM technology that Sony BMG Music added to some music CDs distributed in 2005 and that went awry, causing damage to users' computers.

Among the proposed classes that the Copyright Office rejected was the interesting one of an exemption for "space-shifting" to permit circumvention of access controls applied to audiovisual and musical works in order to copy these works to other media or devices and to access these works on those alternative media or devices. The Copyright Office rejected the proposal on the ground that those proposing the exemption "uniformly failed to cite legal precedent that establishes that such space-shifting is, in fact, a noninfringing use. The Register concludes that the reproduction of those works onto new devices is an infringement of the exclusive reproduction right unless some exemption or defense is applicable. In the absence of any persuasive legal authority for the proposition that making copies of a work onto any device of the user's choosing is a noninfringing use, there is no basis for recommending an exemption to the prohibition on circumvention."[595] The Copyright Office also rejected a proposed exemption for all works protected by access controls that prevent the creation of backup copies,

---

[592] Id. at 68476.

[593] Id.

[594] 71 Fed. Reg. 68477.

[595] Id. at 68478.

reasoning that "the proponents offered no legal arguments in support of the proposition that the making of backup copies is noninfringing."[596]

The Exemptions of 2010. On July 27, 2010, the Librarian of Congress issued the fourth determination of the classes of copyrighted works that should have an exemption, with the exemption to be in effect until Oct. 27, 2012.[597] The 2010 ruling continued the approach of the 2006 ruling in refining the description of a class of works by reference to the type of user who may take advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption. Indeed, in announcing the exemption, the Copyright Office stated that the prohibitions against circumvention "shall not apply to persons who are users of a copyrighted work which is in a particular class of works" granted an exemption.[598]

The six exempted classes of works in the 2010 ruling are the following:

1. "Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

(i) Educational uses by college and university professors and by college and university film and media studies students;

(ii) Documentary filmmaking;

(iii) Noncommercial videos."

2. "Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset."

3. "Computer programs, in the form of firmware or software, that enable used[599] wireless telephone handsets to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network."

---

596 Id. at 68479.

597 75 Fed. Reg. 43825 (July 27, 2010).

598 Id. at 43826.

599 The limitation of this exemption to "used" wireless telephone handsets was a narrowing of the network connection exemption granted in the 2006 rulemaking.

4. "Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if:

(i) The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and

(ii) The information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law."

5. "Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace."

6. "Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format."[600]

a. Scope of the Network Connection Exemption – The TracFone Cases

In TracFone Wireless, Inc. v. Dixon,[601] the court ruled that this exemption did not apply to the defendants' resale of unlocked TracFone phones that would work on wireless services other than TracFone's, because the defendants' unlocking activity "was for the purpose of reselling those handsets for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'"[602] Thus, under this court's view, the exemption appears to be targeted to acts by individual owners of handsets who circumvent the phone's lock to enable their personal use of their own handset on another wireless network. It is unclear from the court's brief analysis whether the exemption would cover those who sell the "computer firmware" referenced in the exemption (and not the unlocked phone itself) that enables an individual to accomplish unlocking of his or her phone. It also unclear whether the reference in the exemption only to "computer firmware" means that it would not apply to services rendered by a third party in assisting an individual to unlock a phone for a fee.

In TracFone Wireless, Inc. v. Riedeman,[603] TracFone brought claims under Section 1201 of the DMCA based on the defendant's resale of TracFone phones for which the prepaid software had been disabled. The defendant failed to file a response to the complaint and the

---

600 75 Fed. Reg. at 43849.

601 475 F. Supp. 2d 1236 (M.D. Fla. 2007).

602 Id. at 1238.

603 2007 Copyr. L. Dec. ¶ 29,500 (M.D. Fla. 2007).

clerk entered a default against the defendant. The court entered a judgment finding that the defendant had violated Section 1201 by circumventing technological measures that controlled access to proprietary software in the phones and by trafficking in services that circumvented technological measures protecting the software. The court also ruled that the Copyright Office exemption did not apply to the defendant's activities because the defendant's "purchase and resale of the TracFone handsets was for the purpose of reselling those handsets for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'"[604] The court entered a judgment against the defendant for statutory damages in the amount of $1,020,800.[605] Interestingly, the court entered an injunction against the defendant that prohibited the defendant from even "purchasing … any wireless mobile phone that they know or should know bears any TracFone Trademark …."[606]

In TracFone Wireless, Inc. v. GSM Group, Inc.,[607] the defendant was engaged in bulk purchase, reflashing, and redistributing TracFone phones. The plaintiff brought claims under Section 1201 for circumvention and trafficking in circumvention technology, and the defendant moved to dismiss for failure to state a claim, relying on the Copyright Office exemption. The court denied the motion, ruling that the exemption did not apply because, citing the Dixon case, the purpose of the defendant's circumvention was to resell wireless telephone handsets for profit and not for the sole purpose of lawfully connecting to a wireless telephone communications network.[608] The court subsequently entered final judgment and a permanent injunction against the defendants based on the DMCA claims on the same rationale. The permanent injunction prohibited the defendants from purchasing or selling any wireless mobile phone that the defendants knew or should have known bore any TracFone trademark and from reflashing or unlocking any such phone. The court retained jurisdiction over the matter to punish any violation of the permanent injunction in an amount of not less than $5,000 for each TracFone handset that a defendant was found to have purchased, sold, or unlocked in violation of the injunction, or $250,000, whichever was greater.[609]

Similarly, in TracFone Wireless, Inc. v. Bitcell Corp.,[610] the court found the defendant's unlocking and resale of TracFone phones to constitute a violation of Section 1201. The court noted that TracFone phones were sold subject to terms and conditions restricting use and sale of the phones that were set forth in printed inserts included in the packaging with the phones, were available to the public on TracFone's web site, and were referenced in printed warnings placed on the outside of the retail packaging of the phones.[611] With no legal analysis, the court simply

---

[604] Id. at p. 40,531.

[605] Id.

[606] Id.

[607] 555 F. Supp. 2d 1331 (S.D. Fla. 2008).

[608] Id. at 1336-37.

[609] TracFone Wireless, Inc. v. GSM Groups, Inc., No. 07-23166-C1V Martinez-Brown, slip op. at 4-6 (S.D. Fla. Aug. 15, 2008).

[610] 2008 U.S. Dist. LEXIS 41955 (S.D. Fla. May 28, 2008).

[611] Id. at *3.

stated that the "Terms and Conditions and language on the packaging constitute a valid binding contract."[612] The court ruled that the Copyright Office exemption did not apply because the defendant's conduct "was for the purpose of reselling those Phones for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'"[613] As in the Riedeman case, the court entered an injunction against the defendant that prohibited the defendant from even "purchasing … any wireless mobile phone that they know or should know bears any Registered TracFone Trademark …."[614] The court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater of $250,000 or $5,000 for each TracFone handset purchased, sold, unlocked, altered in any way, or shipped.[615]

In a virtually identical opinion under similar facts, in TracFone Wireless, Inc. v. Anadisk LLC,[616] the same court found a violation of Section 1201, imposed the maximum statutory damages award of $2,500 per phone on 4,990 phones for a total award of $12,375,000, and entered a similar injunction. The court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater of $1,000,000 or $5,000 for each TracFone handset purchased, sold, unlocked, altered in any way, or shipped.[617]

And again in TracFone Wireless, Inc. v. SND Cellular, Inc., the same court imposed the maximum statutory damages award of $11,370,000 based on trafficking in a minimum of 4,548 phones and entered a similar injunction. Again the court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater of $1,000,000 or $5,000 for each TracFone handset purchased, sold, unlocked, re-flashed, altered in any way, or shipped.[618]

In TracFone Wireless, Inc. v. Zip Wireless Products, Inc.,[619] the court denied a motion to dismiss TracFone's claims of copyright infringement on the ground that the Copyright Office exemption applied. TracFone had adequately alleged in its complaint that lawful connection to a wireless telephone network was not the sole purpose of the defendants' circumvention efforts, and that factual allegation was sufficient to overcome the defendants' argument that TracFone's DMCA claims fell within the scope of the exemption.[620]

---

612 Id.

613 Id. at *8.

614 Id. at *9.

615 Id. at *12.

616 685 F. Supp. 2d 1304 (S.D. Fla. 2010).

617 Id. at 1317-18 & 1319-20.

618 TracFone Wireless, Inc. v. SND Cellular, Inc., 715 F. Supp. 2d 1246, 1263-64 (S.D. Fla. 2010).

619 716 F. Supp. 2d 1275 (N.D. Ga. 2010).

620 Id. at 1285.

In TracFone Wireless, Inc. v. Bequator Corp., the court rejected the applicability of the Copyright Office's July 2010 exemption to the defendant's bulk resale of unlocked or reflashed TracFone phones. The court noted that the July 2010 exemption applied only to used wireless telephone handsets and therefore did not cover the defendant's activities. The court granted a maximum statutory damages award of $46,540,000 ($2500 per phone sold) and entered a permanent injunction against the defendants. Any violation of the injunction would incur liquidated damages in the amount of the greater of $1,000,000 or $5,000 for each TracFone handset purchased, sold, unlocked, reflashed, altered, rekitted, advertised, solicited and/or shipped in violation of the injunction.[621]

(ii) Epic Games v. Altmeyer

In this case, the court issued a TRO enjoining the defendant from offering services to modify Microsoft's Xbox 360 to play pirated copies of the plaintiff's video game *Gears of War 2*. The Xbox contained the capability to allow users to play the game live online, and to do so, players were required to connect through an official web site. The software involved in playing live was programmed to detect modifications to the Xbox and to recognize pirated games. If modification or piracy was detected, the user would be banned from playing live. The defendant offered a service to modify the Xbox to that neither the system itself nor the live software could recognize pirated games or any modification. The court found a likelihood of establishing that the offered services violated Section 1201(a)(2), and issued a TRO enjoining the defendant from performing, advertising, marketing, distributing, or selling game console modification services.[622]

(iii) Facebook v. Power Ventures

In this case, the defendants operated an Internet service called Power.com that collected user information from Facebook's web site outside of the "Facebook Connect" application programmer's interface (API). After a user provided his or her user names and passwords, the Power.com service used the access information to scrape user data from those accounts. Facebook's Terms of Use broadly prohibited the downloading, scraping, or distributing of any content on the web site, except that a user was permitted to download his or her own user content. Facebook alleged that it had implemented specific technical measures to block access by Power.com after the defendants informed Facebook that they intended to continue their service without using Facebook Connect, and that the defendants then attempted to circumvent those technological measures in violation of the anti-circumvention provisions of the DMCA. The defendants brought a motion to dismiss the DMCA claims, arguing that the unauthorized use requirement of a Section 1201(a)(1) claim was not met because it was the users who were controlling access (via Power.com) to their own content on the Facebook web site. The court denied the motion, in view of the fact that the defendants' argument relied on an assumption that Facebook users were authorized to use Power.com or similar services to access their user

---

[621] TracFone Wireless, Inc. v. Bequator Corp., 2011 U.S. Dist. LEXIS 42314 at *32-35, *41-44 (S.D. Fla. Apr. 13, 2011).

[622] Epic Games, Inc. v. Altmeyer, 2008 U.S. Dist. LEXIS 89758 at * 3-4, 9-10 & 19 (S.D. Ill. Nov. 5, 2008).

accounts, and the Terms of Use barred users from using automated programs to access the Facebook web site.[623]

(iv) Bose v. Zavala

In this case, the defendant sold Bose Lifestyle Media Centers in auctions on eBay. In his auctions, he offered to unlock the region coding within the Media Center's DVD player by altering Bose's firmware in the device or to give the purchaser directions on how to do so. Unlocking the region code would permit the Media Centers to play DVDs distributed anywhere in the world. Bose brought claims against the defendant under Section 1201 of the DMCA and the defendant moved to dismiss them under Fed. R. Civ. Pro. 12(b)(6) on the ground that Bose lacked standing to assert the claims because it was not the type of party protected by the DMCA, since it did not sell digital media or region code-changing services. The court rejected this argument, ruling that a party who controls the technological measures that protect copyrighted works is a "person injured" by the circumvention of the measures within the meaning of Section 1203(c).[624] The court concluded, "Bose controls region coding, a technological measure that protects copyrighted DVDs. This is sufficient to allege that it is a 'person injured' within the meaning of the DMCA."

(v) MGE UPS Systems v. GE

In MGE UPS Systems Inc. v. GE Consumer & Industrial Inc.,[625] the Fifth Circuit ruled that mere use of a copyrighted work subsequent to an illegal circumvention does not violate Section 1201(a). The plaintiff distributed uninterruptible power supplies (UPS's), some of which required the use of MGE's copyrighted software programs during servicing. The software required connection of a security dongle to a laptop serial port during servicing. Software hackers had published information on the Internet disclosing general instructions on how to defeat the external security features of the dongle, thereby rendering the hacked software accessible for use without limitation. The defendant's employees obtained a hacked copy of MGE's software and used it to service the plaintiff's UPS's. The Fifth dismissed the plaintiff's claim that such use violated Section 1201(a). The court ruled that because Section 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works after the technological measure has been circumvented. There was no evidence showing that a representative or employee of the defendant had altered the software such that a dongle was not required to use it, and hence the defendant had not itself engaged in any circumvention.[626]

---

623 Facebook, Inc. v. Power Ventures, Inc., 2009 U.S. Dist. LEXIS 42367 (N.D. Cal. May 11, 2009) at *1-2, 9-10 & 13-14.

624 Bose BV v. Zavala, 2010 U.S. Dist. LEXIS 2719 (D. Mass. Jan. 14, 2010) at *1-5.

625 622 F.3d 361 (5th Cir. 2010).

626 Id. at 364-66.

(vi) Granger v. One Call Lender Services

In this case, the plaintiff was the owner of a computer program that estimated the rate or cost of real estate title insurance sold by title insurance agents. The defendants placed an infringing version of the rate calculator program on their website, though later took it down upon receipt of a demand letter from the plaintiff. The plaintiffs had embedded within the computer program copyright tag lines and a watermark that, if not removed carefully, could leave a tell-tale sign as to the origin of the work. The plaintiff argued that removal of the watermark constituted circumvention in violation of Section 1201 and sought statutory damages. The court rejected this argument, citing authority that in the Third Circuit, the legal theory of circumvention had been applied solely to circumstances where the conduct complained of entailed circumventing protective measures such as passwords, server software, or other technological barriers, as opposed to the embedded copyright tag lines and watermark at issue in the present case. Accordingly, the plaintiff could not recover damages for circumvention, although it could recover damages for removal of CMI.[627]

(2) Prohibition on Devices

The DMCA also outlaws devices and technology directed to circumvention of technological copyright protection measures. Specifically, Sections 1201(a)(2) and 1201(b) prohibit the manufacture, import, offer to the public, or trafficking in any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of circumventing a technological measure that effectively "controls access to" a copyrighted work or "protects a right of a copyright owner," or has only limited commercially significant purpose or use other than to circumvent such technological measure, or is marketed for use in circumventing such technological protection measure. Section 1201(b)(2) provides that a technological measure "effectively protects a right of a copyright owner" if the measure "in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner." Although trafficking in these types of prohibited devices might well constitute contributory infringement, Sections 1201(a)(2) and 1201(b) make it a direct statutory violation subject to criminal and civil penalties.

It should be noted that, although Sections 1201(a)(2) and 1201(b) in combination prohibit devices designed to circumvent both technological measures that control access to a copyrighted work and that protect a right of a copyright owner, Section 1201(a)(1) prohibits conduct that is directed only to the former, but not the latter. The rationale for this distinction was apparently a belief that anyone should be free to circumvent a measure protecting rights of a copyright owner in order to make fair use of a work,[628] whereas gaining access in the first instance to a copyrighted work without the owner's permission cannot be a fair use.[629]

---

627 Granger v. One Call Lender Services, LLC, 2012 U.S. Dist. LEXIS 104885 at *2-4, 14-15 (E.D. Pa. July 26, 2012).

628 See The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary (Dec. 1998) at 4 (explaining that the distinction between Section 1201(a) and (b) as to the act of circumvention in itself was "to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying may

Unlike the case of the prohibition of circumvention to gain unauthorized access to a work under Section 1201(a)(1), the prohibitions of Sections 1201(a)(2) and 1201(b) were not suspended for a two year period and went into effect immediately under the DMCA. Thus, the DMCA set up the curious situation in which, for the initial two year period, it did not directly prohibit circumvention of a technological measure to gain access to a work, but did prohibit the manufacture, sale or importation of devices that would enable or assist one to gain such access.

Another curious aspect of the DMCA is that it authorizes the Librarian to create additional exceptions via rulemaking only to Section 1201(a)(1), but not to Sections 1201(a)(2) and 1201(b). Thus, the DMCA appears to allow the Librarian to permit acts of circumvention in additional situations, but not the devices necessary to enable or assist such acts.

(i) Sony Computer Entertainment America v. Gamemasters

In this lawsuit, Sony Computer Entertainment America (SCEA) obtained a preliminary injunction against the defendants, who were distributing a device called the "Game Enhancer" that enabled players to play Sony PlayStation games sold in Japan or Europe, and intended by SCEA for use exclusively on Japanese or European PlayStation consoles, on U.S. PlayStation consoles.[630] The Sony PlayStation console was designed to operate only when encrypted data was read from a game CD-ROM verifying that the CD was an authorized, legitimate product licensed for distribution in the same geographical territory of the console's sale.[631]

The Game Enhancer enabled a player to trick a U.S. PlayStation console into playing a Japanese or European authorized game CD by the following method. After inserting an authorized CD game, the user was instructed to hold down the disk cover switch of the console while keeping the lid or disk cover open. The Game Enhancer was then turned on and its internal operating system selected for execution, thereby replacing the PlayStation console's internal operating system. The validity and territorial codes were read from the authorized CD, thereby instructing the console that the inserted CD was valid and authorized. The user was then instructed to hit the "select" button on the game controller to signal the console to stop the CD motor, enabling the player to remove the U.S. authorized game CD and replace it with a CD that

---

be a fair use under appropriate circumstances, *section 1201* does not prohibit the act of circumventing a technological measure that prevents copying."). Similarly, the Copyright Office noted in its rationale for the first set of exemptions it established from the prohibition against circumvention of technological measures controlling access to a work: "The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use." 65 Fed. Reg. 64556, 64557 (Oct. 27, 2000).

629 Realnetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913, 942 (N.D. Cal. 2009) ("The prohibition on individual circumvention conduct only applies with respect to access protection technologies (because fair use can never be an affirmative defense to the act of gaining unauthorized access), not to technologies that prevent copying."); Inna Fayenson, "Anti-Circumvention Provisions of The Digital Millennium Copyright Act," *Journal of Internet Law*, Apr. 1999, at 9, 10.

630 Sony Computer Entertainment America v. Gamemasters, 87 F. Supp. 2d 976, 981 (N.D. Cal. 1999).

631 Id.

was authorized for play only on a Japanese or European console. Once the game was loaded, the Game Enhancer then returned control to the PlayStation's operating system, and the unauthorized game could be played.

The court ruled that, because the Game Enhancer was a device whose primary function was to circumvent the mechanism on the PlayStation console that ensured the console operated only when encrypted data was read from an authorized CD-ROM, the Game Enhancer had a primary function to circumvent a technological measure that effectively controls access to a copyrighted work and was therefore a violation of Section 1201(a)(2)(A). The court ruled that SCEA was therefore entitled to a preliminary injunction against sale of the device under Section 1203.[632]

(ii) The DirecTV Cases

a. DirecTV, Inc. v. Borow

This straightforward case found defendant Randy Borow in violation of Section 1201(a)(1) for using an emulator to circumvent DirecTV's encryption on its signals and to simulate certain functions of the DirecTV access card in order to watch DirecTV's programming without paying subscription fees.[633]

b. DirecTV, Inc. v. Carrillo

In this case, the court found the defendant liable under Section 1201 based on his possession and transfer of equipment used to pirate satellite TV signals. The court found that the devices were primarily designed to intercept encrypted signals.[634]

(iii) Sony Computer Entertainment America v. Divineo

In Sony Computer Entertainment America, Inc. v. Divineo,[635] the court granted summary judgment to the plaintiff that several devices sold by the defendant violated the anti-circumvention provisions of the DMCA. The devices all could be used to circumvent an authentication process designed by Sony into the Playstation system to verify that an inserted disc was authentic before the Playstation would play it. If a user burned a copy of a copyrighted Playstation game, a unique code that was part of every authentic disc would not be copied, thus preventing the user from playing the copy on the Playstation. The defendant sold the following devices that could be used to circumvent this process: (i) HDLoader, software that permitted a user to make an unauthorized copy of Playstation-compatible video games onto a separate hard drive connected to the Playstation system; (ii) mod chips that, when wired to a Playstation

---

632 Id. at 987-88. A similar case finding a violation of the DMCA as a result of sales of a cable descrambler and decoder is CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000).

633 DirecTV, Inc. v. Borow, 2005 U.S. Dist. LEXIS 1328 (N.D. Ill. Jan. 6, 2005), at *3 & *12-13.

634 DirecTV, Inc. v. Carrillo, 227 Fed. Appx. 588, 589-90 (9th Cir. 2007).

635 457 F. Supp. 2d 957 (N.D. Cal. 2006).

console, circumvented the authentication system and allowed the system to play the unauthorized software; and (iii) devices that allowed a user to boot up a Playstation console and perform a disc swap without triggering the software and hardware mechanisms within the Playstation that initiated the authentication system.[636]

The defendant argued against liability on the ground that there were several ways in which the devices could be used that did not result in infringement of the plaintiff's copyrighted video games. First, the devices could be used to allow more than 150 items of "homemade" software to execute on the Playstation. Second, software developers could use the devices to test their own games as a less expensive alternative to purchasing a specialized Sony console that would run any game. Third, HDLoader made playing games more convenient by allowing users to avoid having to swap out discs to change games and because the Playstation could read hard drive data more quickly than data stored on CDs or DVDs. The defendant also gave a legal notice on its web site warning users that they were responsible for the legality of their own use of materials obtained through the web site.[637] The defendant also invoked the reverse engineering defense of Section 1201(f) of the DMCA, arguing that users of mod chips could use them to ensure the interoperability of an independently created computer program with the Playstation.[638]

The court rejected all of these arguments, holding that the challenged devices were primarily designed for the purpose of circumventing the Playstation authentication system which otherwise controlled access to software played on the system, and that "downstream customers' lawful or fair use of circumvention devices does not relieve [defendant] from liability for trafficking in such devices under the DMCA."[639] The court also ruled that the defendant's legal notice to users of its devices was not relevant to its own liability under the DMCA.[640] The application of the court's ruling to the Section 1201(f) interoperability rights is interesting. It means that, even though it may be permissible to circumvent a technological measure to obtain information necessary for interoperability of an independently developed computer program, or for the user of an independently developed computer program to circumvent an access control measure in order to interoperate with a program controlled by the measure, it is nevertheless illegal for a third party to sell such user a device that would enable the circumvention, if the device is designed primarily for circumvention. Another implication of the ruling is that legal uses that may result after use of a device to accomplish circumvention are not to be factored into whether the device is primarily designed for circumvention. Under this decision, the DMCA focuses only on the capability of the device to accomplish circumvention in the first instance, and if that is its primary technical function, it is illegal.

---

[636] Id. at 958-59.

[637] Id. at 961.

[638] Id. at 965.

[639] Id.

[640] Id.

(iv) Ticketmaster L.L.C. v. RMG Technologies, Inc.

In this case, the plaintiff Ticketmaster alleged the defendant had violated Sections 1201(a)(2) and 1201(b)(1) by distributing an automated tool that enabled users (such as ticket brokers) to access and navigate rapidly through the Ticketmaster site and purchase large quantities of tickets. The tool enabled users to bypass Ticketmaster's "CAPTCHA" system, a security system designed to distinguish between human users and automated programs by requiring the user to read a distorted sequence of letters and numbers on the screen and enter those letters and numbers correctly into the system in order to gain access to the ticket purchase page.[641]

On a motion for a preliminary injunction, the court found the plaintiff likely to prevail on these claims. The court rejected the defendant's argument that CAPTCHA was not a system or a program that qualified as a technological measure under the DMCA because it was simply an image, and it was designed to regulate ticket sales, not to regulate access to a copyrighted work. The court ruled that the DMCA does not equate its use of the term "technological measure" with the defendant's terms "system" or "program," and that in any case the CAPTCHA system was a technological measure within the DMCA because most automated devices could not decipher and type the stylized random characters the system generated in order to proceed to the copyrighted ticket purchase pages.[642] Thus, CAPTCHA qualified as a technological measure that restricted access to copyrighted works within the purview of Section 1201(a)(2). Similarly, it also fell within the purview of Section 1201(b)(1) because it protected rights of the copyright owner by preventing automated access to the Ticketmaster ticket purchase web pages, thereby preventing users from copying those pages. Accordingly, the court issued a preliminary injunction prohibiting the defendant from trafficking in any computer program or other automatic devices to circumvent copy protection systems in Ticketmaster's web site and from using any information gained from access to Ticketmaster's web site to create computer programs to circumvent Ticketmaster's copy protection and web site regulation systems.[643]

(v) The Tracfone Cases

In TracFone Wireless, Inc. v. Pak China Grup Co., Ltd.,[644] the defendants were engaged in bulk purchase, reflashing, and redistributing TracFone phones. The plaintiff brought claims under Section 1201 for circumvention and trafficking in circumvention technology. The defendants failed to answer and were in default. The court found the defendants guilty of the alleged violations of Section 1201 and imposed the maximum statutory damages of $37,707,500 based on the sale of at minimum 15,083 reflashed TracFone prepaid phones.[645]

---

641 Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096, 1102, 1111-12 (C.D. Cal. 2007).

642 Id. at 1112.

643 Id. at 1112, 1116.

644 2012 U.S. Dist. LEXIS 48492 (S.D. Fla. Feb. 6, 2012).

645 Id. at *36-37.

In TracFone Wireless, Inc. v. Technopark Co., Ltd.,[646] the court found the defendants liable under Section 1201 for the unauthorized unlocking or reflashing of TracFone phones and for trafficking in certain unlocking devices known as "Octopus Boxes" in furtherance of its unlocking scheme. The court also found the defendants liable for facilitating co-conspirators who were trafficking in the service of circumventing TracFone's technological measures. The court imposed a maximum statutory damages award of $10,000 for the four unlocking or reflashing devices manufactured by the defendants and sold by distributors that TracFone was aware of.[647]

In addition, see the numerous TracFone cases discussed in Section II.G.1(a)(1) above.

(vi) Movida Communications, Inc. v. Haifa

In this case, the court ruled that the defendant's actions of tampering with or altering pre-paid control software resident on Movida pre-paid wireless handsets, entering unauthorized PIN numbers into the phones for purposes of unlocking or re-flashing the phones, and reselling the phones for use on networks other than Movida's, violated Section 1201 of the DMCA. The court issued a permanent injunction against the defendant, prohibiting him even from purchasing any model of Movida handsets, in addition to re-flashing or unlocking any Movida handset, and accessing, altering, erasing, tampering with, deleting or otherwise disabling Movida's proprietary prepaid cellular software contained within any model of Movida handset. The order also provided that any violation would be punished in an amount of not less than $5,000 per Movida handset.[648]

(vii) Microsoft Corp. v. EEE Business Inc.

In this case, the defendant engaged in the unauthorized distribution of Microsoft software that was available only under a Volume License Agreement. The agreement permitted only authorized volume licensees to install software to unlock the media programming to enable the user to enter a 25-character alphanumeric code, called the Volume License Key (VLK), which was unique to the licensee and required to be kept confidential under the terms of the Volume License Agreement. The court ruled that, by distributing a VLK without authorization, the defendant had effectively circumvented Microsoft's technological measure to control access to a copyrighted work in violation of Section 1201(a)(2) of the DMCA.[649]

(viii) MDY Industries v. Blizzard Entertainment

In this case, the defendant distributed bot software called "Glider" that was able to play Blizzard Entertainment's multiplayer online role-playing game known as World of Warcraft (WoW) for its owner while the owner was away from his or her computer, thereby enabling the

---

646 2012 U.S. Dist. LEXIS 58449 (S.D. Fla. Apr. 9, 2012).

647 Id. at *4, 13-14 & 15-16.

648 Movida Communications, Inc. v. Haifa, 2008 Copyr. L. Dec. ¶ 29,528 (C.D. Cal. 2008).

649 Microsoft Corp. v. EEE Business Inc., 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008).

owner to advance more quickly within WoW than would otherwise be possible.[650] Blizzard Entertainment brought claims under the DMCA, alleging that Glider evaded Blizzard technologies known as "Warden" to detect and prevent the use of bots by WoW players. Warden included two different software components. The first component, known as "scan.dll," scanned the user's computer for unauthorized programs such as Glider before the user logged onto the WoW servers to play the game, and if it detected such programs, scan.dll would deny the user access to the game servers. The second component, known as the "resident" component of Warden, ran periodically while a user played WoW and if it detected the use of a bot program, Blizzard would revoke access to the game.[651]

Blizzard argued that scan.dll and the resident software controlled access to copyrighted software, as required by Section 1201(a)(2) of the DMCA, in two ways. First, when scan.dll prevented a user from playing WoW, or when the resident software terminated a user's playing of WoW, they prevented additional code in the game client software from being written to RAM. Second, scan.dll and the resident software barred access to WoW's non-literal elements (the multi-media presentation of the WoW universe and character interactions) generated by the code's interaction with the computer hardware and operating systems.[652]

The court rejected Blizzard's claim under Section 1201(b)(2). With respect to access to the code of WoW, the court, citing the Lexmark case, ruled that a holder of Blizzard's game client software had full and complete access to that code on both the CD that contained it and on the user's hard drive once the software had been loaded onto the user's computer. The user thereafter could view a copy of the game client software code, regardless of whether the user actually played WoW or encountered Warden. The user did not need to pass through Blizzard's security devices to gain access to the code. Accordingly, the court granted summary judgment to the defendant on this issue. The court ruled that it could not similarly grant summary judgment with respect to the non-literal elements of WoW because the parties' statement of facts filed in conjunction with their motions for summary judgment said virtually nothing about this aspect of the game. Finally, the court noted that neither scan.dll nor the resident software appeared to require the application of information by the game user, or the application of a process or a treatment by the game user, before granting access to copyrighted information, as required by Section 1201(b)(2). Instead, they merely scanned for unauthorized programs. However, because neither party had addressed this issue in their briefs, the court noted that it would be a factual issue for trial.[653]

The court also rejected a claim by Blizzard under Section 1201(b)(1) of the DMCA. Blizzard asserted that scan.dll and the resident software prevented users from copying software code to RAM and accessing the non-literal elements of the game once they were caught using Glider. MDY disputed this factual assertion, contending that code from the game client software

---

650 MDY Industries, LLC v. Blizzard Entertainment, Inc., 2008 U.S. Dist. LEXIS 53988 (D. Ariz. 2008 July 14, 2008) at *2.

651 Id. at *34.

652 Id. at *34-35.

653 Id. at 18*35-40.

was not written to RAM after a user passed by scan.dll or the resident software. The court concluded that, because there was a factual dispute with respect to the extent to which Blizzard's Warden software protected against the copying of software code to RAM, and because the parties did not submit sufficient facts from which the court could decide whether the protective measures protected Blizzard's rights in the non-literal elements of the game, summary judgment on the Section 1201(b)(1) claim was denied.[654]

In a subsequent opinion issued after a bench trial, the court held that Blizzard's circumvention claims against Glider under Sections 1201(a)(2) and 1201(b)(1) failed with respect to the discrete nonliteral components of the games stored on the game player's hard drive, because they could be accessed and viewed without signing onto the server (and therefore involving the Warden software) by independently purchased computer programs that could call up the individual visual images or recorded sounds within the game client software. However, the circumvention claims were valid with respect to the "dynamic" nonliteral elements of WoW – i.e., the real-time experience of traveling through different worlds, hearing their sounds, viewing their structures, encountering their inhabitants and monsters, and encountering other players – because those dynamic elements could be accessed and copied only when the user was connected to a Blizzard server that controlled their dynamic display, which in turn required the user successfully to pass scan.dll when logging on and to survive the periodic scrutiny of the resident component.[655]

Six weeks later, the court entered two permanent injunctions against the marketing, sale and distribution of Glider for use in connection with WoW – one on the basis of the copyright infringement and DMCA claims, and another on the basis of a tortious interference with contract claim for which the court had ruled in favor of Blizzard. The court stayed the injunction on the copyright and DMCA claims pending their appeal, but refused to stay the injunction on the tortious interference claims.[656] In a subsequent opinion, the court awarded Blizzard statutory damages of $6.5 million.[657]

On appeal, the Ninth Circuit reversed, except as to MDY's liability for violation of Section 1201(a)(2).[658] The Ninth Circuit cast one of the key issues on appeal to be whether the DMCA's anti-circumvention provisions prohibit circumvention of access controls only when unauthorized access leads to copyright liability, as the Federal Circuit had held in the

---

654 Id. at *41-43.

655 MDY Industries, LLC v. Blizzard Entertainment, Inc., 616 F. Supp. 2d 958, 964-68 (D. Ariz. 2009). The court noted that Warden did not prevent all WoW users from copying the dynamic nonliteral elements of the game because players who did not use Glider could copy that content while connected to Blizzard servers. The court noted, however, that Section 1201(b)(1)(A) requires only that the technological measure restrict or otherwise limit *unauthorized* copying. Id. at 968 n.3.

656 MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 24151 (Mar. 10, 2009). The court denied a motion for reconsideration of the denial of the stay of the tortious interference injunction. MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 25650 (Mar. 25, 2009).

657 MDY Industries, LLD v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 38260 (D. Ariz. Apr. 1, 2009).

658 MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 (9th Cir. Feb. 17, 2011).

Chamberlain and Storage Tech cases.[659] The Ninth Circuit reached a conclusion contrary to the Federal Circuit on that issue.[660]

First, the Ninth Circuit noted textual differences between the prohibitions of Section 1201(a) and 1201(b). Section 1201(a) is directed to protecting a "work protected under this title," whereas Section 1201(b) is directed to protecting "a right of a copyright owner."[661] Noting that neither Section 1201(a)(1) nor 1201(a)(2) explicitly refer to traditional copyright infringement under Section 106, the court read Section 1201(a) "as extending a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to works protected under Title 17, i.e., copyrighted works."[662] The court also noted that the two specific examples of unlawful circumvention recited under Section 1201(a) – descrambling a scrambled work and decrypting an encrypted work – are acts that do not necessarily infringe or facilitate infringement of a copyright. Descrambling or decrypting do not necessarily result in someone's reproducing, distributing, publicly performing, or publicly displaying the copyrighted work, or creating derivative works based on the copyrighted work.[663]

In addition, the court noted another significant difference between Section 1201(a) and Section 1201(b) in that Section 1201(a)(1)(A) prohibits circumventing an effective access control measure, whereas Section 1201(b) prohibits trafficking in circumvention devices, but does not prohibit circumvention itself because, as the Senate Judiciary Committee report noted, such conduct was already outlawed as copyright infringement, so no new prohibition was necessary.[664] Accordingly, the court concluded, "This difference reinforces our reading of § 1201(b) as strengthening copyright owners' traditional rights against copyright infringement and of § 1201(a) as granting copyright owners a new anti-circumvention right."[665] The court found the legislative history of the anti-circumvention provisions of the DMCA to reinforce its reading that Section 1201(a) creates a new anti-circumvention right distinct from copyright infringement, while Section 1201(b) strengthens the traditional prohibition against copyright infringement.[666]

---

659 Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004); Storage Technology Corp. v. Custom Hardware Eng'g Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

660 The court also rejected MDY's contention that Warden's scan.dll and resident components were separate, and only scan.dll should be considered as a potential access control measure under Section 1201 (a)(2). The court held that "an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized. Our analysis considers Warden's scan.dll and resident components together because the two components have the same purpose: to prevent players using detectable bots from continuing to access WoW software" MDY Industries, 2011 U.S. App. LEXIS at *27.

661 Id. at *29-30.

662 Id. at *31.

663 Id.

664 Id. at *32.

665 Id. The court also noted that, if a copyright owner puts in place an effective measure that both (1) controls access and (2) protects against copyright infringement, a defendant who traffics in a device that circumvents that measure could be liable under both Sections 1201(a) and 1201(b). Id. at *35.

666 Id. at *35-40.

The Ninth Circuit noted that its reading of the anti-circumvention provisions put it in conflict with the Federal Circuit's decisions in the Chamberlain and Storage Tech cases, in which the Federal Circuit required Section 1201(a) plaintiffs to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff's copyright – what the Ninth Circuit referred to as an "infringement nexus requirement."[667] Although the Ninth Circuit stated that it appreciated the policy considerations expressed by the Federal Circuit in Chamberlain, the Ninth Circuit found itself unable to follow the Federal Circuit's infringement nexus requirement because it is contrary to the plain language of the statute and would lead to statutory inconsistencies in the DMCA. For example, under the Federal Circuit's construction, Congress's creation of a mechanism in Section 1201(a)(1)(B)-(D) for the Librarian of Congress to grant exemptions to certain non-infringing behavior from Section 1201(a)(1) liability would be unnecessary if an infringement nexus requirement existed.[668]

Turning to application of its construction of the anti-circumvention provisions to the facts of the case, the Ninth Circuit agreed with the district court that Glider did not violate Section 1201(a)(2) with respect to WoW's literal elements and individual non-literal elements, because Warden did not effectively control access to those WoW elements. The literal elements (the game client's software code) were available on a player's hard drive once the game client software was installed, and the non-literal components could be accessed by a user without signing on to the server by using independently purchased computer programs to call up the visual images or the recorded sounds within the game client software stored in files on the hard disk. Because a player needed not encounter Warden to access WoW's individual non-literal elements, Warden did not effectively control access to those elements.[669] On this point, the Ninth Circuit founds its conclusion in accord with the Sixth Circuit's decision in the Lexmark case,[670] in which mere purchase of one of the plaintiff's printers allowed "access" to the copyrighted program, because it could be read directly from the printer memory without encountering the printer's authentication sequence.[671]

The court next found Blizzard to be liable for trafficking in violation of Section 1201(a)(2) with respect to WoW's dynamic non-literal elements, which constituted a copyrighted work available only through the WoW server. The Ninth Circuit noted a split between other circuits with respect to the meaning of the phrase "circumvent a technological measure … without the authority of the copyright owner." The Federal Circuit concluded in Chamberlain that the definition of "circumvent a technological measure" imposes an additional requirement on a Section 1201(a)(2) plaintiff: to show that the defendant's circumventing device enables third parties to access the copyrighted work without the copyright owner's authorization (citing

---

667 Id. at *40.

668 Id. at *45-46. The Ninth Circuit noted, that like the Chamberlain court, it need not reach the question of the relationship between fair use and violations of Section 1201. MDY had not claimed that Glider use was a fair use of WoW's dynamic non-literal elements. Accordingly, the court left open the question whether fair use might serve as an affirmative defense to a prima facie violation of Section 1201. Id. at *48 n.12.

669 Id. at *52-53.

670 See Section II.G.1(a)(15)(i) below.

671 Id. at *53-54.

Chamberlain, 381 F.3d at 1193).[672] The Second Circuit adopted a different view, "that § 1201(a)(3)(A) plainly exempts from § 1201(a) liability those whom a copyright owner authorizes to circumvent an access control measure, not those whom a copyright owner authorizes to access the work" (citing Corley, 273 F.3d at 333 & n.15).[673] The Ninth Circuit found "the Second Circuit's view to be the sounder construction of the statute's language, and [we] conclude that § 1201(a)(2) does not require a plaintiff to show that the accused device enables third parties to access the work without the copyright owner's authorization. Thus, Blizzard has satisfied the 'circumvention' element of a § 1201(a)2) claim, because Blizzard has demonstrated that it did not authorize MDY to circumvent Warden."[674]

The Ninth Circuit found, however, that MDY was not liable under Section 1201(b)(1) because Warden did not protect MDY's reproduction right against unauthorized copying. Although WoW players copied the software code into RAM while playing the game, Blizzard's end user license agreement and Terms of Use authorized all licensed WoW players to do so. Because the court had found that the prohibition in the Terms of Use on use of bots was a contractual covenant rather than a condition to the license,[675] violation of the covenant by a Glider user did not make the user a copyright infringer by continuing to copy code into RAM. Second, although WoW players could theoretically record game play by taking screen shots, there was no evidence that Warden detected or prevented such allegedly infringing copying. Warden had been designed to reduce the presence of cheats and bots, not to protect WoW's dynamic non-literal elements against copying. Accordingly, the court ruled that Warden did not effectively protect any of Blizzard's rights under the copyright act, and MDY was therefore not liable under Section 1201(b)(1) for Glider's circumvention of Warden.[676]

(ix) Coupons, Inc. v. Stottlemire

The plaintiff offered coupon printing software that enabled online, printable coupons to be delivered to consumers. The software placed a registry key file on the user's personal computer that acted as a counter, limiting the number of times each coupon could be printed on that computer (typically, two prints per coupon). The defendant discovered how to remove the counter, created a computer program that automated its removal, and distributed the program. The plaintiff alleged that, because each coupon had its own unique bar code and date stamp, the coupons were subject to copyright protection, and the defendant's distribution of its computer program violated the DMCA by allowing users to access more than the limit for each coupon. The plaintiff also claimed that the act of printing constituted unauthorized copying. The defendant brought a motion to dismiss.[677] The court found fault with the plaintiff's DMCA claims:

---

672 Id. at *56 n.16.

673 Id.

674 Id.

675 See Section III.C.2(i) below.

676 2011 U.S. App. LEXIS 3428 at *60-61.

677 Coupons, Inc. v. Stottlemire, No. CV 07-03457 HRL (N.D. Cal. July 2, 2008), slip op. at 1, 4.

> These concepts seem to be logically inconsistent and, when asserted together, do appear to blur the carefully constructed distinction between "access controls" and "rights controls." If the court accepts Coupons' argument that each coupon is "unique," then can there be a claim of improper copying ….? On the other hand, if the coupons are not unique, then the allegations against Stottlemire appear to fall within the "rights controls" (i.e., permitting users to print more copies of coupons than were authorized by Plaintiff).[678]

The court was also not convinced that the addition of a bar code or other functional device on the coupon qualified it as a unique copyrighted work. But in any event, if Coupons wanted to make the argument, then the court noted that it needed to actually allege it in the complaint, and the plaintiff's reference to "unique coupons" in the complaint was not sufficient to put the defendant on notice of the claims against him. The court ruled that the plaintiff needed to clarify which theory it was pursuing (a "unique" coupon theory or a "general" coupon theory). Accordingly, the court dismissed the DMCA cause of action with leave to amend the complaint to clarify whether the plaintiff was asserting a claim under a Section 1201(b) "rights controls" theory (i.e., allowing users to print more than the authorized number of copies) or a claim under a Section 1201(a) "access controls" theory (i.e., "unique" coupons).[679]

After the plaintiff amended its complaint, the defendant again brought a motion to dismiss, which the court denied.[680] In the amended complaint, the plaintiff claimed that each printed coupon's identification number marked it as an authorized copy of a copyrighted work, and did not create a derivative work. The plaintiff asserted claims under both Sections 1201(a) and 1201(b). The court ruled that the plaintiff had sufficiently alleged facts that its software controlled access to the printing of the copyrighted coupon to state a claim under Section 1201(a). With respect to Section 1201(b), the court ruled that the plaintiff had adequately alleged that its software controlled copying and distribution in two ways: the registry key limited the number of coupons distributed to a single computer (simultaneously limiting the number of authentic copies that the computer could print), and the software's counter limited the number of authentic coupons distributed as a whole. The court held that, although the plaintiff would have to prove that its software actually worked as both an access and use control, it had sufficiently alleged facts that supported its theory that the defendant had violated Section 1201(b), and the motion to dismiss was denied.[681]

(x) CoxCom, Inc. v. Chafee

CoxCom leased cable boxes to its subscribers that enabled them to descramble incoming signals for viewing and that transmitted certain information from subscribers back to CoxCom, including billing information association with purchase of pay-per-view programming. The defendant sold a digital cable filter that filtered out low-frequency signals, including the return

---

678 Id. at 4-5.

679 Id. at 5.

680 Coupons, Inc. v. Stottlemire, 588 F. Supp. 2d 1069, 1072 (N.D. Cal. 2008).

681 Id. at 1073-75.

transmissions from the cable box containing purchase information. The court noted that the filters were not illegal, and had innocuous uses, such as allowing cable television subscribers to enhance viewing quality by filtering out interference from FM radio broadcast towers, shortwave radios, and home appliances. However, the defendants marketed the filters to their customers as capable of filtering out pay-per-view charges.[682] The plaintiffs brought claims under the DMCA anti-circumvention provisions and the district court granted summary judgment to the plaintiffs on those claims.[683]

On appeal, the First Circuit affirmed, rejecting the defendants' argument that their filters did not "circumvent" technological measures. The court found the technological measure at issue to be CoxCom's pay-per-view delivery and billing system that scrambled pay-per-view programming to make it not viewable unless subscribers chose to purchase it.[684] Without further analysis, the First Circuit simply concluded: "A digital cable filter allows subscribers to 'avoid' or 'bypass' that technological measure. Given the factual record, we have little trouble concluding that the district court properly granted summary judgment to CoxCom as to appellants' liability under the DMCA."[685]

(xi) The DISH Network Cases

a. Dish Network v. Sonicview

DISH Network transmitted encrypted programming signals that were then received by an EchoStar receiver, which processed and decrypted the signals using data and encryption technology stored in a DISH Network access card loaded into the receiver. The access card communicated with the receiver to assure that only signals the subscriber was authorized to received would be decrypted. DISH Network brought anti-circumvention claims against the defendants, whom DISH Network alleged were involved in the manufacture of receivers, software and other devices used to intercept and steal DISH Network's encrypted signals. Upon a motion for a TRO, the court ruled that DISH Network's security access cards functioned as both access controls and copyright controls, and that the defendants' distribution of software files through a website that allowed individuals to decrypt and view DISH Network content likely violated both Section 1201(a)(2) and 1201(b)(1).[686]

b. Dish Network v. SatFTA

In Dish Network v. SatFTA,[687] the court found the defendant liable under Section 1201(a)(2) for trafficking in circumvention devices that aided in circumvention of Dish

---

682 CoxCom, Inc. v. Chafee, 536 F.3d 101, 104-05 (1st Cir. 2008).

683 Id. at 106.

684 Id. at 110.

685 Id.

686 Dish Network L.L.C. v. Sonicview USA, Inc., 2009 U.S. Dist. LEXIS 63429 at *2-3,*7-8 (S.D. Cal. July 23, 2009).

687 2011 U.S. Dist. LEXIS 25038 (N.D. Cal. Mar. 9, 2011).

Network's signal and content security measures in its receivers, including software that facilitated the unauthorized re-programming of Dish Network smartcards, circuit diagrams that could be used to build a connector to interface with the EEPROM in a Dish Network receiver to erase the data created by Dish Network's electronic countermeasures and continue receiving unauthorized programming, and diagrams depicting the storage locations of data that secured communication between receivers and smartcards.[688] The court also found the defendant liable under Section 1201(b)(1) for trafficking in a program that allowed users to copy the programming of a Dish Network satellite receiver to a computer hard drive. Dish Network protected against unauthorized copying and distribution of recorded programming by saving the copyrighted content in an unrecognizable format, and the court found that to be a sufficient technological measure to invoke the protection of Section 1201(b)(1). The defendant contended that his program served a legitimate function by allowing individuals to create backup copies of their Dish Network recordings. The court rejected this defense, citing the case of Realnetworks, Inc. v. DVD Copy Control Ass'n[689] for the rule that, although the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers. Because the defendant's program allowed a computer to overcome Dish Network's copy-control measures, it violated Section 1201(b)(1).[690]

c. Dish Network v. Dimarco

The case of Dish Network LLC v. Dimarco[691] involved the impoundment of technology that could be used to gain unauthorized access to Dish Network signals. When an authorized EchoStar receiver received a Dish Network signal, it forwarded part of the signal called the "entitlement control message" to a NagraStar smart card in the receiver. If the subscriber was tuned to a channel he was authorized to receive, the smart card retrieved a decryption key from its read-only memory and used the key to unlock the "control word" from the entitlement control message. The smart card then transmitted the control word back to the receiver, and the receiver used it to decode the incoming signal so the subscriber could watch the programming. Content providers like Dish Network routinely changed their decryption keys to help thwart piracy. A new form of piracy was developed called "Internet key sharing" or "IKS" whereby a pirate kept his unauthorized receiver connected to the Internet for automatic re-flashing with the newest keys, which were retrieved from an IKS server connected to multiple legitimate NagraStar smart cards. Control words obtained from the authorized smart cards were sent from the IKS server over the Internet to unauthorized receivers.[692]

---

688 Id. at *3-6, *12-13. The court also found the defendant liable for personal violations of Section 1201(a)(1) for his admitted modification of Dish Network smartcards. The court rejected the defendant's defense that he had modified the smartcards only for the purpose of testing the operation of various receivers, not to receive an unauthorized satellite signal. Id. at *10-11.

689 641 F. Supp. 2d 913 (N.D. Cal. 2009).

690 Dish Network, 2011 U.S. Dist. LEXIS 25038 at *13-14.

691 2012 U.S. Dist. LEXIS 33889 (D. Nev. Mar. 14, 2012).

692 Id. at *3-4.

The defendants sold unauthorized receivers with decryption software and hardware, cables to connect the unauthorized receivers to the Internet for use with an IKS server, and passwords to access the IKS server which were euphemistically referred to as "extended warranty codes." The defendants admitted that the receivers they sold were capable of being used for piracy, but argued that because they did not themselves traffic in illegal encryption keys, their products amounted to "modern day rabbit ears" for their customers to receive free satellite programming. The receivers had no built-in means of connecting to the Internet, but the defendants sold an adapter called a "WizHub" that enabled connection to the Internet.[693]

The defendants argued that the court should not impound its WizHubs or extended warranty codes because the WizHub was simply an adapter and one could not engage in piracy without the piracy software and IKS servers. The court rejected this argument, noting that a device such as the WizHub permitting the connection of an otherwise legitimate receiver to the Internet along with a password permitting access to a server with illegally trafficked decryption keys could be said to constitute a product designed to circumvent a technological measure that effectively controlled access to a protected work. The court could not see any possible need for a person using a free-to-air satellite receiver in a legitimate way to connect that receiver to the Internet and enter a password to connect to a server whose sole purpose was the trafficking of decryption keys. The court therefore ordered the impoundment of the WizHub connectors and the extended warranty codes under Section 1203(b)(2), although not of the receivers themselves (for which the plaintiffs had not sought impoundment). The court refused, however, to seize the defendants' web sites, which appeared to be used for the legitimate sale of free-to-air receivers.[694]

d. Dish Network v. Sonicview

This case, a follow-on decision of the case described in subsection a. above, involved the same kind of "Internet Key Sharing" (or "IKS") piracy of Dish Network signals described in the Dimarco case in the previous subsection. To enable IKS piracy, the defendants sold their Sonicview receivers, each model of which contained firmware having more than one exact match of the proprietary code and data that resided on the plaintiffs' smart card, a particular algorithm important for encrypting and decrypting Dish Network satellite signals, and a graphical user interface. There were also strong similarities between the Sonicview receivers' firmware and that of existing piracy firmware. The defendants also sold a serial Ethernet adapter called the iHub, which came with a 16-digit code that enabled the Sonicview receiver to access the IKS server through a dongle and an add-on module that worked in conjunction with the receiver, when loaded with piracy software, to receive Dish Network's high-definition programming. Sonicview also operated a web site that contained piracy software available for download which was intended for use with Sonicview receivers to decrypt Dish Network's satellite television programming.[695]

---

693 Id. at *4, 11-12.

694 Id. at *12-15, 17.

695 Dish Network, LLC v. Sonicview USA, Inc., 2012 U.S. Dist. LEXIS 75663 at *10-11, 13.

The court found the defendants in violation of Section 1201(a)(2) by trafficking in the receivers, iHubs, add-on modules, and piracy software. The combination of a Sonicview receiver, iHub, and add-on module, when loaded with the piracy software, permitted unauthorized access to Dish Network's satellite programming. The court, citing two other district court decisions to the same effect, noted that potential lawful or fair use is not a defense to Section 1201(a) when its requirements are established. The court awarded statutory damages of $200 per violation for 324,901 violations (at least 307,401 receivers and 17,500 iHubs sold), for a total award of $64,980,200.[696]

e. Dish Network v. Alejandri

In Dish Network v. Alejandri,[697] the court granted summary judgment to the plaintiffs that the defendants' sale of free-to-air receivers together with referral to service providers who could program them using the IKS piracy technology to receive Dish Network signals without payment of subscriber fees violated Section 1201(a)(1)(A) of the DMCA. The court noted that the defendants' equipment used for unlawful circumvention, which had been impounded, would be disposed of by the U.S. Marshals' Service upon order of the court at the conclusion of the proceedings.[698] The court also found a violation of Section 605(a) of the Communication Act (47 U.S.C. § 605(a)) and awarded statutory damages under that Act. The court did not award statutory damages under the DMCA – although the court's opinion does not make clear, it appears that the plaintiffs did not seek statutory damages under the DMCA.[699]

(xii) Realnetworks v. DVD Copy Control Association.

In Realnetworks, Inc. v. DVD Copy Control Association, Inc.,[700] the DVD Copy Control Association (DVDCCA) brought claims alleging that distribution of Realnetworks' RealDVD product violated the anti-trafficking provisions of the DMCA. DVDCCA licenses the Content Control System (CSS) technology, which combines multiple layers of encryption with an authentication process to protect the content on DVDs. CSS requires that a DVD drive lock upon insertion of a CSS-protected DVD and prevent access to its contents until a CSS-authorized player engages in an authentication procedure, akin to a secret handshake, to establish mutual trust. It also requires that players authenticate themselves to DVD drives to establish mutual trust, both to unlock the DVD and gain access to its protected video contents and also separately to gain access to keys stored in secure areas of the DVD, which then decrypt and descramble the DVD content. The process of authentication with the DVD drive, and subsequent content decryption, will fail if a DVD is not in the DVD drive. Finally, the CSS technology creates a

---

696 Id. at *22, 24-25 & 40-41.

697 2012 U.S. Dist. LEXIS 106839 (D. Puerto Rico July 30, 2012).

698 Id. at *10-14, 21-25 & 28-29.

699 Id. at *16-21, 25-28.

700 641 F. Supp. 2d 913 (N.D. Cal. 2009).

system whereby content on a DVD may be played back only in decrypted and unscrambled form from the physical DVD and not any other source, such as a computer hard drive.[701]

The RealDVD product provided a variety of functions, including playing back DVDs placed in a computer's DVD drive, looking up information about the DVD from Internet databases, providing links to various information web sites relevant to the chosen DVD, and – the function at issue in the lawsuit – saving an image of the copy-protected content on the device's hard drive for later playback without the physical DVD being present.[702]

The court ruled that the CSS technology was both an access control and a copy control (the authentication process functioned as an access control and the encryption functioned as a copy control),[703] and that distribution of RealDVD therefore violated the anti-trafficking provisions of both Sections 1201(a)(2) and 1201(b). RealDVD circumvented the access controls of CSS in violation of Section 1201(a)(2) by allowing access of CSS content on the hard drive without going through most of the CSS protection steps, such as DVD drive-locking, CSS authentication, and CSS bus encryption. Once RealDVD had copied a DVD, it did not authenticate the DVD drive or receive encrypted keys for playback from the hard drive. Accordingly, the process of authentication with the DVD drive, and subsequent content decryption, were thereby circumvented by RealDVD.[704] RealDVD circumvented the copy controls of CSS in violation of Section 1201(b) by using the CSS authentication codes and algorithms to make an unauthorized copy of the DVD content.[705]

The court rejected a number of defenses asserted by Realnetworks. First, Realnetworks argued that CSS was not an "effective" technological measure because it had been widely cracked. The court found this fact of no moment, because the DMCA is predicated on the authority of the copyright owner, not whether or not the technological measure is a strong means of protection. The court held that it is sufficient under the statutory language if an access control prevents the easy creation *at the consumer level* of widely available and usable copies of copyrighted works.[706]

The court rejected Realnetworks' argument that the copyright holder plaintiffs (the movie studios) could not bring a DMCA claim against a co-licensee to CSS technology. Realnetworks cited cases holding that copyright licenses are governed by contract law and copyright owners who enter into such licenses waive their rights to sue the licensee for copyright infringement and are limited to breach of contract claims. The court distinguished those cases, noting that the

---

701 Id. at 919-20.

702 Id. at 924. The RealDVD und user license agreement provided, "You may use the saving functionality of the Software only with DVDs that you own. You may not use the Software to save DVDs that you do not own, such as rental or borrowed DVDs." Id. at 926.

703 Id. at 935.

704 Id. at 933.

705 Id. at 935.

706 Id. at 932.

studios were not bringing copyright infringement claims, nor were they the direct licensors of CSS technology. Because Realnetworks had acted outside the scope of its license with the DVDCCA, the studios were permitted to bring circumvention claims under the DMCA.[707]

The court also rejected Realnetworks defenses that distribution of RealDVD was protected by the Sony doctrine because it was capable of substantial noninfringing uses and by virtue of the fact that the copying it permitted fell within the fair use rights of users who made copies for personal, noncommercial use. First, the court held that the DMCA supersedes Sony to the extent that the DMCA broadened copyright owners' rights beyond the Sony holding. Second, the court ruled that whether consumer copying of a DVD for personal use is a fair use was not at issue, because while the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers of the devices prohibited by Section 1201(a)(2).[708] "So while it may well be fair use for an individual consumer to store a backup copy of a personally-owned DVD on that individual's computer, a federal law has nonetheless made it illegal to manufacture or traffic in a device or tool that permits a consumer to make such copies."[709]

Accordingly, the court granted a preliminary injunction against the distribution of RealDVD.[710]

(xiii) Apple v. Psystar

In Apple, Inc. v. Psystar Corp.[711] Apple contended that Psystar's distribution of modified copies of its Mac OS X operating system on non-Apple computers constituted copyright infringement and illegal trafficking in circumvention devices. Apple distributed Mac OS X subject to a license agreement that prohibited its use on any non-Apple-labeled computer. Apple used lock-and-key technological measures to prevent Mac OS X from operating on non-Apple computers. Specifically, it encrypted the files of Mac OS X and used a kernel extension that communicated with other kernel extensions to locate a decryption key in the hardware and use that key to decrypt the encrypted files of Mac OS X. Psystar distributed a line of computers called Open Computers that contained copies of Mac OS X, modified to run on Psystar's own hardware, which was not authorized by Apple.[712]

Psystar's had engaged in the following conduct at issue. It bought a copy of Mac OS X and installed it on an Apple Mac Mini computer. It then copied Mac OS X from the Mac Mini onto a non-Apple computer for use as an "imaging station." Once on the imaging station, Mac

---

[707] Id. at 933.

[708] Id. at 941-43.

[709] Id. at 942.

[710] Id. at 952.

[711] 673 F. Supp. 2d 931 (N.D. Cal. 2009), aff'd, 658 F.3d 1150 (9th Cir. 2011), cert. denied, 2012 U.S. LEXIS 3593 (May 14, 2012).

[712] Id. at 933-34.

OS X was modified. Psystar then replaced the Mac OS X bootloader (a program that runs when a computer first powers up and locates and loads portions of the operating system into random access memory) and disabled and/or removed Mac OS X kernel extension files and replaced them with its own kernel extension files. Psystar's modifications enabled Mac OS X to run on non-Apple computers. The modified copy of Mac OS X became a master copy that was used for mass reproduction and installation onto Psystar's Open Computers.[713]

The court first ruled that Psystar had violated Apple's exclusive right to copy Mac OS X by making copies of the modified version of OS X and installing them on non-Apple computers, and by making copies of such software in random access memory when turning on its computers running Mac OS X. The court refused to allow Psystar to assert a defense to such copying under Section 117 of the copyright statute, ruling that Psystar had waived such a defense by failing to plead it.[714] The court also held that distribution of Psystar's computers infringed Apple's exclusive distribution rights with respect to Mac OS X. The court rejected Psystar's defense under the first sale doctrine, based on the fact that it allegedly included a legitimately purchased Mac OS X DVD with every Psystar computer. The court held that the first sale defense under Section 109 provides immunity only when copies are lawfully made, and the master copy of the modified Mac OS X residing on Psystar's imaging station was unauthorized, as were all the many unauthorized copies that were made from such master copy.[715] The court also concluded that Psystar had violated Apple's exclusive right to create derivative works by replacing the Mac OS X bootloader with a different bootloader to enable an unauthorized copy of Mac OS X to run on Psystar's computers, by disabling and removing Apple kernel extension files, and by adding non-Apple kernel extension files. The court rejected Psystar's contention that these modifications did not amount to creation of a derivative work because Apple's source code, object code and kernel extensions had not been modified. The court held that the replacement of entire files within the software while copying other portions resulted in a substantial variation from the underlying copyrighted work and therefore an infringing derivative work.[716]

Turning to Apple's trafficking claim, the court noted that Apple's encryption of the Mac OS X operating system files, although aimed primarily at controlling access, also effectively protected its right to copy, at least for copies made in RAM. Accordingly, the encryption scheme constituted both an access control measure and a copy control measure. Psystar's distribution of "decryption software" (apparently referring to Psystar's substituted kernel extension files that obtained Apple's decryption key from the hardware and then used that key to decrypt the Mac OS X modules) violated both Section 1201(a)(1)(A) and Section 1201(b)(1)

---

713 Id. at 934.

714 Id. at 935. Without giving any reasons why, the court also observed that "the assertion of *Section 117* is so frivolous in the true context of how Psystar has used Mac OS X that a belated attempt to amend the pleadings would not be excused." Id. at 936.

715 Id. at 937.

716 Id. at 938.

because it enabled obtaining unauthorized access to Mac OS X and resulted in an unauthorized copy of Mac OS X being loaded into RAM.[717]

The court rejected Psystar's argument that Apple's technological protection measure was not effective because the decryption key for circumvention was publicly available on the Internet. "The fact that circumvention devices may be widely available does not mean that a technological measure is not, as the DMCA provides, effectively protecting the rights of copyright owners in the ordinary course of its operations."[718] Accordingly, the court granted Apple's motion for summary judgment.[719]

The court also rejected Psystar's argument that Apple's alleged attempt to use copyright to tie Mac OS X to Apple hardware constituted copyright misuse. Because Apple had not prohibited others from independently developing and using their own operating system, it had not violated the public policy underlying copyright law or engaged in copyright misuse. The court noted that Apple had not prohibited purchasers of Mac OS X from using competitor's products. Rather, it had simply prohibited purchasers from using OS X on competitor's products. Thus, Apple's license agreement was simply an attempt to control the use of its own software.[720]

On appeal, the defendant did not challenge the district court's rulings of infringement, but rather challenged the district court's rejection of Psystar's misuse defense. The Ninth Circuit affirmed the district court's copyright misuse rulings.[721] After a review of relevant misuse decisions by courts in the Ninth Circuit, the court concluded, "A software licensing agreement may reasonably restrict use of the software as long as it does not prevent the development of competing products."[722] The court found that Apple's license agreement did not impermissibly do so: "Apple's [license agreement] does not restrict competitor's ability to develop their own software, nor does it preclude customers from using non-Apple components with Apple computers. Instead, Apple's [license agreement] merely restricts the use of Apple's own software to its own hardware. … Psystar produces its own computer hardware and it is free to develop its own computer software."[723] The court also rejected Psystar's reliance on the first sale doctrine, arguing that Apple was attempting to control the use of the Mac OS X software after it had been sold, because Psystar purchased retail-packaged copies of the OS. The court found that the argument falsely assumed that Apple transferred ownership of the Mac OS X when it sold a retail-packaged DVD containing software designed to enable Apple's existing

---

717 Id. at 941.

718 Id. at 942 (quoting Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)).

719 Psystar, 673 F. Supp. 2d at 942.

720 Id. at 939-40.

721 Apple, Inc. v. Psystar Corp., 658 F.3d 1150, 1152 (9th Cir. 2011), cert. denied, 2012 U.S. LEXIS 3593 (May 14, 2012).

722 Id. at 1159.

723 Id. at 1160.

customers to upgrade to the latest version of the OS. The court found that, although buyers of the DVD purchased the disc, they knew they were not buying the software, as Apple's license agreement clearly explained as much. Accordingly, the DVD purchasers were licensees, not owners, of the copies of the software.[724] The Ninth Circuit therefore affirmed the district court's grant of summary judgment in favor of Apple and its entry of a permanent injunction against Psystar's infringement of the Mac OS X.[725]

(xiv) Blizzard Entertainment v. Reeves

In this case, the defendant ran a website that enabled its users to bypass the checks and restrictions for access to the plaintiff's World of Warcraft online gaming environment. After granting a default judgment, the court turned to what the appropriate award of statutory damages should be. The court estimated the number of circumvention violations by looking to the total number of community members on the defendant's website (427,393), each of whom was assumed to have downloaded, access or otherwise used anti-circumvention software, services, or products offered by the defendant. The court then awarded the $200 minimum amount per violation, for a total award of $200 x 427,393 = $85,478,600.[726]

(xv) The Craigslist Cases

a. Craigslist v. Naturemarket

In Craigslist, Inc. v. Naturemarket,[727] the defendants distributed software that bypassed the CAPTCHA system of the Craigslist site and enabled users to post ads automatically in whatever quantity, frequency, and location the user wished, in violation of the Craigslist site Terms of Use.[728] Upon a motion for a default judgment, a magistrate judge issued an opinion recommending that the defendants' distribution of the software be found in violation of Sections 1201(a)(2) and 1201(b)(1) because the software "enabled unauthorized access to and copies of copyright-protected portions of Plaintiff's website controlled by [the CAPTCHA system] – particularly the ad posting and account creation portions of the website."[729] The magistrate judge also recommended an award of statutory damages in the amount of $1,000 per copy of software distributed, estimated at 470 copies (obtained by dividing the defendants' estimated revenue of $40,000 by the list price of $84.95 for the software), for a total statutory damages award of $470,000.[730] The district court adopted the magistrate judge's recommendations and

---

[724] Id. at 1159-60.

[725] Id. at 1162.

[726] Blizzard Entertainment, Inc. v. Reeves, 2010 U.S. Dist. LEXIS 85560 at *7-8 (C.D. Cal. Aug. 10, 2010).

[727] 694 F. Supp. 2d 1039 (N.D. Cal. 2010) (report and recommendation of magistrate judge re plaintiff's motion for default judgment).

[728] Id. at 1048-49.

[729] Id. at 1056.

[730] Id. at 1063-64. The magistrate judge also recommended that an award of actual damages be made against the defendants based on the liquidated damages clause of the Terms of Use, which provided for $200 for every ad the defendants posted as posting agents on behalf of users, for a total of $840,000. Id. at 1064.

opinion in every respect, and entered a permanent injunction against the defendants enjoining them from distributing software that enabled postings on Craigslist without each posting being entered manually or that used automated means to download or otherwise obtain data from Craigslist, from circumventing the CAPTCHA system or other technological measures controlling access to the site, from repeatedly posting the same or similar content on the site or in more than one category, and from accessing or using the site for any commercial purpose whatsoever.[731]

b. Craigslist v. Mesiab

In Craigslist, Inc. v. Mesiab,[732] a magistrate judge recommended that the plaintiff's motion for default judgment and award of statutory damages be granted based on violations of the DMCA anti-circumvention provisions in the following ways:

– Distribution of "EasyAd Suite" software that bypassed the CAPTCHA system of the Craigslist site and enabled users to post ads automatically and in unlimited quantity. The magistrate recommended that an award of $800 per copy sold be increased to $1,500 per copy because the defendants had shown disregard for the injunction entered by the court. Based on 2,983 copies of the software distributed, the magistrate recommended an award of $4,474,500.[733]

– Sale or offer for sale of "CAPTCHA credits," which was a service to circumvent CAPTCHAs through instantaneous outsourcing for occasions when the EasyAd Suite program was unable to decode the CAPTCHA. The defendants also offered CAPTCHA circumventions in bulk for prices ranging from $12.50 for 500 credits to $157.50 for 10,000 credits. The magistrate ruled that damages under the DMCA could properly be calculated based on offers to sell and not actual sales of CAPTCHA credits, as well as credits sold through a third party. Because it was uncontested that defendants' web site offered to sell CAPTCHA credits and those offers were made to at least the number of people who purchased the EasyAd Poster Deluxe software, the magistrate found the defendants liable for damages for 2,983 offers. The magistrate recommended an award of $400 per violation for offers to sell CAPTCHA credits, for an award of $1,193,200.[734]

– Offers of Craigslist telephone-verified accounts. The "Adult" and "Therapeutic Services" categories on Craigslist required telephone verification in order to post ads and the telephone-verified accounts offered by the defendants allowed purchasers to pay to have their accounts fraudulently verified by contracted employees or devices. Again applying the rule that offers for sale were sufficient for damages, the magistrate found that at least 1,000 offers for

---

731 Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039 (N.D. Cal. 2010) at 1046-47.

732 2010 U.S. Dist. LEXIS 134411 (N.D. Cal. Nov. 15, 2010).

733 Id. at *30-32.

734 Id. at *6, 33-35.

telephone-verified accounts were made, and that an award of $400 per offer was reasonable ($400,000 in total).[735]

The district court adopted the magistrate's recommendation in full and entered judgment against the defendants for a total statutory damages award of $6,067,700.[736]

c. Craigslist v. Hubert

In Craigslist, Inc. v. Hubert,[737] the court ruled, on an entry of default judgment after the defendant failed to appear, that the sale of software allowing users to automatically post ads to Craigslist and the provision of a service that automated and circumvented the entry of CAPTCHA passwords violated the ant-circumvention provisions of the DMCA. The court awarded statutory damages of $400 for each of the 3,000 users of the defendant's web site, on the theory that each user received an "offer" to circumvent in the form of an offer to purchase the defendant's software or CAPTCHA credits, for a total award of $1,200,000. The court rejected the plaintiff's request for the statutory maximum of $2,500 per offer, finding that such an award would be vastly disproportional to the actual costs the plaintiff alleged it had incurred as a result of auto-posting, $5,000 per year.[738]

d. Craigslist v. Branley

In this case, the court denied Craigslist's request for a default permanent injunction against a defendant who failed to appear because Craigslist had not alleged facts sufficient to support the allegation that the defendant would continue to act as an agent posting ads for third parties by circumventing Craigslist's CAPTCHA system using software known as "CLAD Genius," in violation of Section 1201 and Craigslist's Terms of Use.[739]

e. Craigslist v. Kerbel

In this case, the court granted the plaintiff's motion for a default judgment, finding that the plaintiff had adequately pled claims for violation of the anti-circumvention provisions based on the defendants' alleged bypassing of Craiglist's CAPTCHA software and its phone verification measures in order to automatically create accounts and post ads to Craigslist. The court awarded statutory damages of $200,000, calculated on the defendants' offer to sell a bundle of 10,000 "credits" used to purchase phone-verified accounts on Craigslist at 10 credits each,

---

735 Id. at *35-37.

736 Craigslist, Inc. v. Mesiab, 2010 U.S. Dist. LEXIS 134381 (N.D. Cal. Dec. 20, 2010).

737 2010 U.S. Dist. LEXIS 143037 (N.D. Cal. Apr. 15, 2010).

738 Id. at *4, 10-13.

739 Craigslist, Inc. v. Branley, 2012 U.S. Dist. LEXIS 36731 at *4-5, 12 (N.D. Cal. Mar. 19, 2012).

representing 1,000 offers to sell the accounts, multiplied by the minimum statutory damages award of $200 per violation.[740]

(xvi) Echostar v. Viewtech

In Echostar Satellite LLC v. Viewtech, Inc.,[741] the court granted the plaintiff summary judgment on its claim under Section 1201(a)(2) against the defendants for the distribution of receivers structurally altered so as to be capable of unauthorized decryption of Echostar satellite TV programming and of software that would enable the piracy of Echostar's programming. The court also found that the defendants' provision of free receiver to moderators on popular piracy web sites and encouragement of the moderators to provide foavorable reviews of the receiver's ability to obtain the plaintiff's protected programming violated the third prong of Section 1201(a)(2), which prohibits marketing a technology used in circumventing an access measure. The court awarded statutory damages of $214,898,600, representing $200 for each of at least 1,074,493 receivers intended for piracy sold by the defendants.[742]

(xvii) Adobe Systems v. Feather

In this case, the defendant offered for sale and distributed pirated copies of the plaintiffs' software via the Internet, including on eBay and through his own website. He also trafficked in and sold product keys or serial numbers designed to circumvent the plaintiffs' copyright protection measures to enable the pirated copies to function. Upon a motion for default judgment, the court found that the defendant's actions, as alleged in the complaint, established violations of Section 1201(a)(2) and of willful copyright infringement. The court awarded statutory damages for willful infringement under Section 504(c)(2) in the amount of $90,000 for each of 28 copyrighted works infringed, for a total award of $2,520,000 in damages. The plaintiffs did not seek separate damages for their DMCA claim, and the court noted in a footnote that they could not do so in any event, citing other authority for the proposition that a plaintiff cannot seek duplicative statutory damages under the Copyright Act and the DMCA.[743] Note that the ruling with respect to "duplicative" statutory damages seems contrary to other cases, such as the Pacific Stock v. MacArthur & Co. case discussed in Section G.1(c)(1)(xi) below, which awarded statutory damages for CMI violations in addition to statutory damages for copyright infringement arising out of the same acts.

---

740 Craigslist, Inc. v. Kerbel, 2012 U.S. Dist. LEXIS 108573 at *26-27, 49-50 (N.D. Cal. Aug. 2, 2012).

741 2011 U.S. Dist. LEXIS 42709 (S.D. Cal. Apr. 20, 2011).

742 Id. at *4-5, *8-11.

743 Adobe Sys v. Feather, 2012 U.S. Dist. LEXIS 146913 at *4, 6-7 & 11 n.5 (D. Conn. Sept. 18, 2012).

(3) What Constitutes an Effective Technological Measure

(i) Auto Inspection Services v. Flint Auto Auction

In Auto Inspection Services v. Flint Auto Auction,[744] the plaintiff was the owner of an automotive inspection program that provided a uniform method of inspecting vehicles after the term of a lease or use had expired. The plaintiff included a quality control feature as part of the program that allowed it to monitor all information collected using the program. For example, when a vehicle inspector collected data for a vehicle and entered it into the program, the data had to be sent to the plaintiff for quality control inspection before the information could be forwarded to the owner of the vehicle. In this way, the plaintiff could monitor who was using the program to protect against unauthorized use.[745]

The defendant, a former licensee of the plaintiff's program, wrote its own automotive inspection program to replace the plaintiff's program. The plaintiff claimed that the defendant's program was a copyright infringement. The plaintiff also claimed that its quality control feature constituted a technical protection measure to restrict access and use of its software, and that the defendant had violated the anti-circumvention provisions of the DMCA by circumventing the quality control feature to gain access to the plaintiff's source code to copy it.[746]

The court found it questionable that the quality control feature was a technical measure that effectively controlled access to a protected work within the purview of the DMCA. The court noted that the protected work at issue was the source code of the program, and the user detection feature was a part of the program itself that in no way controlled access to the source code. Rather, it merely alerted the plaintiff as to who was using the program. Consequently, the user detection feature would not prevent anyone from gaining access to the source code and copying it verbatim. Moreover, the feature came into play only after a user had conducted an inspection, and did not prevent unauthorized users from accessing the program in the first instance.[747]

(ii) Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey

In Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey,[748] the court addressed the issue of whether a robots.txt file applied to a web site to indicate no archival copying by robots should take place constitutes an effective technological measure. Healthcare Advocates had filed a lawsuit alleging that a competitor infringed trademarks and copyrights and misappropriated trade secrets belonging to Healthcare Advocates. The defendants in that case were represented by the boutique IP law firm of Harding, Earley, Follmer & Frailey. To aid in

---

744 2006 U.S. Dist. LEXIS 87366 (E.D. Mich. Dec. 4, 2006).

745 Id. at *1-2.

746 Id. at *4-5, 22.

747 Id. at *23.

748 2007 U.S. Dist. LEXIS 52544 (E.D. Pa. July 20, 2007).

preparing a defense, on two occasions employees of the Harding firm accessed screenshots of old versions of Healthcare Advocates' web sites that had been archived by the Internet Archive's web site (www.archive.org). The old versions of the web site were accessed through the "Wayback Machine," an information retrieval system offered to the public by the Internet Archive that allowed users to request archived screenshots contained in its archival database. Viewing the content that Healthcare Advocates had included on its public web site in the past was very useful to the Harding firm in assessing the merits of the trademark and trade secret allegations brought against the firm's clients.[749]

The Internet Archive had a policy to respect robots.txt files and not to archive sites containing a robots.txt file that indicated the site should not be archived. In addition, for those web sites that did not have a robots.txt file present at the web site's inception, but included it later, the Internet Archive would remove the public's ability to access any previously archived screenshots stored in its database. The archived images were not deleted, but were instead rendered inaccessible to the general public, and the Internet Archive's web crawler was instructed not to gather screenshots of that web site in the future.[750]

Healthcare Advocates had not included a robots.txt file on its web site prior to July 7, 2003. Consequently, Internet Archive's database included screenshots from Healthcare Advocates' web site when the Harding firm's employees accessed that database through the Wayback Machine on July 9, 2003 and July 14, 2003. On those two dates of access, however, the Internet Archive's servers, which checked for robots.txt files and blocked the images from being displayed from the corresponding web site, were malfunctioning due to a cache exhaustion condition. Because of this malfunction, employees of the Harding firm were able to view and print copies of the archived screenshots of Healthcare Advocates' web site stored in Internet Archive's database, contrary to Internet Archives' normal policy. Healthcare Advocates sued the Harding firm, alleging that it has manipulated the Wayback Machine on the two dates in question in a way that rendered useless the protective measure of the robots.txt file that Healthcare Advocates had placed on its web site, in violation of the anti-circumvention provisions of the DMCA.[751]

The court turned first to the question of whether the robots.txt file used by Healthcare Advocates qualified as a technological measure effectively controlling access to its web site as defined in the Section 1201(a)(3)(B) of the DMCA. The court concluded on the particular facts of the case that it did, although the court refused to hold that a robots.txt file universally constitutes a technological protection measure:

> The measure at issue in this case is the robots.txt protocol. No court has found that a robots.txt file universally constitutes a "technological measure effectively controll[ing] access" under the DMCA. The protocol by itself is not analogous to digital password protection or encryption. However, in this case, when all

---

[749] Id. at *1-3.

[750] Id. at *7-8.

[751] Id. at *4, 8-10, 43.

> systems involved in processing requests via the Wayback Machine are operating properly, the placement of a correct robots.txt file on Healthcare Advocates' current website does work to block users from accessing archived screenshots on its website. The only way to gain access would be for Healthcare Advocates to remove the robots.txt file from its website, and only the website owner can remove the robots.txt file. Thus, in this situation, the robots.txt file qualifies as a technological measure effectively controlling access to the archived copyrighted images of Healthcare Advocates. This finding should not be interpreted as a finding that a robots.txt file universally qualifies as a technological measure that controls access to copyrighted works under the DMCA.[752]

However, the court found no violation of the DMCA by the actions of the Harding firm employees because those employees had not acted to "avoid" or "bypass" the technological measure. The court noted that those choice of words in the DMCA "imply that a person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material."[753] The employees of the Harding firm had not taken such affirmative action. As far as they knew, no protective measures were in place with respect to the archived screenshots they were able to view, and they could in fact not avoid or bypass any protective measure because on the dates in question nothing stood in the way of them viewing the screenshots.[754]

Healthcare Advocates argued that liability under the DMCA should be judged on what the Harding firm knew, not what actions it took. Healthcare Advocates argued that the Harding firm knew it was not permitted to view certain archived images, because some of the images were blocked. Healthcare Advocates therefore claimed that the firm knew or should have known that it was not supposed to be able to view any of the screenshots at issue, and that any request made for archived images after the first request resulted in a denial constitute circumvention of its robots.txt file. The court rejected this argument, ruling that simply making further requests is not circumvention under the DMCA. The requests did not alter any computer code to render the robots.txt file void. Internet Archive's servers indicated that no lock existed when the requests were made. Accordingly, the Harding firm could not avoid or bypass a digital wall that was not there.[755]

The court also ruled that Healthcare Advocates' inference that the Harding firm should have known it was not allowed to view any archived images via the Wayback Machine was both unreasonable and irrelevant. When a screenshot was blocked, the Wayback Machine returned a message stating that the page was blocked by the web site owner, but the message also included links, one of which said, "Try another request or click here to search for all pages on healthcareadvocates.com." When this page appeared, the firm's employee clicked on the link

---

[752] Id. at *41-42 (citation omitted).

[753] Id. at *46.

[754] Id. at *47.

[755] Id. at *47-50.

and received a list of all available screenshots.[756] The court held that, even if the firm knew that Healthcare Advocates did not give it permission to see its archived screenshots, "lack of permission is not circumvention under the DMCA."[757] Accordingly, the court granted the Harding firm summary judgment on Healthcare Advocates' claim of a violation of the DMCA.[758]

(iii) Apple v. Psystar

The facts of this case are set forth in Section II.G.1(b)(14) above. The court rejected the defendant's argument that Apple's encryption of its Mac OS X operating system files, which were decrypted by a decryption key stored within Apple's hardware, was not an effective technological protection measure because the decryption key was publicly available on the Internet. "The fact that circumvention devices may be widely available does not mean that a technological measure is not, as the DMCA provides, effectively protecting the rights of copyright owners in the ordinary course of its operations."[759]

(4) No Requirements With Respect to Design of a Product

Section 1201(c)(3) provides that nothing in the bills "shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure …."

(5) Other Rights Not Affected

Sections 1201(c)(1), (2), and (4) provide that Section 1201 is not intended to affect rights, remedies, limitations, or defenses (including fair use) to copyright infringement; or to enlarge or diminish vicarious or contributory liability in connection with any technology or product; or to enlarge or diminish any rights of free speech of the press for activities using consumer electronics, telecommunications, or computing products.

Notwithstanding these provisions, groups such as the Digital Future Coalition (DFC) have criticized the approach of the DMCA. In a position paper dated August 1997,[760] the DFC argued that Section 1201 would effectively negate fair use rights, because it imposes liability for "circumvention" even when the purpose of the activity is permitted by the copyright act (such as reverse engineering or other activities that otherwise constitute fair use). The DFC also argued that Section 1201 would outlaw legitimate devices with substantial noninfringing uses, effectively overruling the Supreme Court's decision in Sony Corp. v Universal City Studios.[761]

---

[756] Id. at *50-51.

[757] Id. at *51.

[758] Id.

[759] Apple, Inc. v. Psystar Corp., 673 F. Supp. 2d 931, 942 (quoting Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)).

[760] The position paper may be found at www.ari.net/dfc/docs/stwip.htm.

[761] 464 U.S. 417 (1984).

The DFC argued that the savings clauses of Section 1201(c) are inadequate because "while Section 1201 will not as a formal matter restrict existing limitations and exceptions to copyright, it will as a practical matter preclude the exercise of these limitations and exceptions by preventing the manufacture and use of the technologies necessary for their existence. Nor would the savings clause protect individuals who gain 'access' to works in violation of 1201(a)(1), even if they do so for entirely lawful purposes."[762]

Another position paper filed on behalf of the Information Technology Industry Council raised concern that Section 1201 will impose liability too broadly in view of the broad definition of "circumvention":

> Thus, if a device does not respond to a technological protection measure that is intended to control copying, which in some cases may be a simple 1 or 0 in header information included with the digital content, the device may be construed as avoiding, bypassing, deactivating or impairing that measure.… Companies that make devices that do not respond to copy flags – because they don't know about the flags or because of technological difficulties associated with complying – could be liable under Section 1201 even though they had no intent to circumvent.[763]

The paper also raised concern about broadening the standard for liability for third party use of devices that infringe copyright owner's rights from that of the Sony case, which imposes liability only for sale of devices having no substantial noninfringing uses, to the prohibition under the bill of devices that are "primarily designed or produced" for circumvention, or have "only limited commercially significant purpose" other than circumvention, or are marketed for use in circumvention.

(6) Exemption for Nonprofit Organizations and Law Enforcement

Section 1201(d) sets up an exemption from the circumvention prohibitions of Section 1201(a)(1) for nonprofit libraries, archives, or educational institutions that gain access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work, provided that a copy of the work is not retained longer than necessary to make the good faith determination, is used for no other purpose, and there is not otherwise reasonably available an identical copy of the work in another form. Section 1201(e) provides that the prohibitions of Section 1201 do not apply to lawfully authorized

---

762 Position paper at 3.

763 Prepared Statement of Chris Byrne of Silicon Graphics, Inc. on Behalf of the Information Technology Industry Council Before the House Judiciary Committee Courts and Intellectual Property Subcommittee (Wed., Sept. 17, 1997) (available from Federal News Service, 620 National Press Building, Washington, D.C. 20045, and on file with the author). Section 1201(c)(3), discussed above, appears to be directed at least in part to addressing this issue.

investigative, protective, information security,[764] or intelligence activity of law enforcement officers.

(7) Reverse Engineering for Interoperability

Section 1201(f) provides three exemptions to the anti-circumvention provisions relating to reverse engineering and interoperability:

Reverse Engineering for Interoperability of an Independently Created Computer Program. Section 1201(f)(1) provides that, notwithstanding the prohibitions in Section 1201(a)(1)(A), "a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title." The language in Section 1201(f) requiring that the reverse engineering be for the sole purpose of "identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs" comes directly from Article 6 of the European Union Software Directive, and appears to be the first time that language from an EU Directive has been incorporated verbatim into the United States Code.[765]

Development and Employment of a Technological Means for Enabling Interoperability. Section 1201(f)(2) provides that, notwithstanding the prohibitions in Sections 1201(a)(2) and 1201(b), "a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title."

The scope of this exemption is uncertain from its language in several respects. First, it is unclear what kinds of "technological means" Congress had in mind for falling within this exemption. The reference to allowing a person to "develop *and* employ" such technological means may suggest that the exemption is limited to only those means developed by the person desiring to circumvent, as opposed to commercially available circumvention means. The legislative history suggests otherwise, however, for it contemplates that the rights under Section 1201(f)(2) may be exercised through either generally available tools or specially developed tools:

---

[764] Section 1201(e) defines "information security" to mean activities carried out to identify and address the vulnerabilities of a government computer, computer system, or computer network.

[765] Jonathan Band & Taro Issihiki, "The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step," *Cyberspace Lawyer*, Feb. 1999, at 2, 4. Section 1201(f) may also represent the first Congressional recognition of the legitimacy of software reverse engineering. Id.

> [Section 1201(f)(2)] recognizes that to accomplish the acts permitted under [Section 1201(f)(1)] a person may, in some instances, have to make and use certain tools. In most instances these will be generally available tools that programmers use in developing computer programs, such as compilers, trace analyzers and disassemblers, which are not prohibited by this section. In certain instances, it is possible that a person may have to develop special tools to achieve the permitted purpose of interoperability. Thus this provision creates an exception to the prohibition on making circumvention tools contained in subsections 1201(a)(2) and (b). These tools can be either software or hardware.[766]

From this legislative history, it is apparent that the phrase "develop and employ" in Section 1201(f)(2) was probably intended to mean "develop and/or employ."

A second ambiguity is whether the "technological means" of Section 1201(f)(2) were intended to be limited to the kinds of reverse engineering "tools" cited in the legislative history (compilers, trace analyzers, disassemblers and the like), or whether they could be read more broadly to encompass computer programs, such as application programs, that in their ordinary operation are designed to circumvent technological measures protecting another computer program so as to interoperate with it. For example, consider the fact pattern at issue in the case of Lexmark International, Inc. v. Static Control Components, Inc.,[767] discussed in Section II.G.1(o)(1) below. In that case, the district court ruled on a motion for a preliminary injunction that Static Control violated Section 1201(a)(2) by distributing microchips that were used to replace the microchip found in the plaintiff Lexmark's toner cartridges. Static Control's microchip contained a computer program that circumvented Lexmark's authentication sequence that prevented the printer engine software on the Lexmark printer from allowing the printer to operate with a refilled toner cartridge.

The district court in that case ruled that the exemptions of Section 1201(f) did not apply because Static Control's microchips could not be considered to contain independently created computer programs, since the toner loading program on those microchips was an exact copy of the toner loading program contained on Lexmark's microchips.[768] However, suppose Static Control had independently developed the computer program contained on its microchips.[769]

---

766 S. Rep. No. 105-190, at 33 (1998).

767 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003), rev'd, 387 F.3d 522 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27,422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

768 As discussed further in Section II.G.1(a)(13)(i) below, the Sixth Circuit on appeal reversed the district court's grant of a preliminary injunction and remanded. Among other things, the Sixth Circuit questioned whether Lexmark's toner loading program was even copyrightable, ruling that on the preliminary injunction record Lexmark had made inadequate showings with respect to originality of its toner loading program and whether that program functioned as a "lock-out code" that had to be copied for functional purposes. Lexmark Int'l v. Static Control Components, 387 F.3d 522, 536-41 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27,422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

769 The Sixth Circuit also ruled that, whether or not the toner loading program on Static Control's microchips was independently created, the record established that there were other programs on Static Control's microchips that were independently created, and those computer programs also interoperated with Lexmark's printer engine program on Lexmark's microchips. Id. at 550.

Would the exemption of Section 1201(f)(2) apply? Static Control could argue yes, on the ground that Section 1201(f)(2) permits it to "employ technological means [the computer program on its microchip] to circumvent a technological measure [the authentication sequence implemented by the Lexmark printer engine software] … for the purpose of enabling interoperability of an independently created computer program [again, the computer program on Static Control's microchip] with other programs [the Lexmark printer engine program]."

On the other hand, Lexmark could argue no, on the ground that the legislative history indicates that the "technological means" referenced in Section 1201(f)(2) were meant to be limited to reverse engineering "tools," and the program on the Static Control microchip is not a reverse engineering tool, but rather an application program. In sum, the issue is whether the "independently created computer program" referenced in Section 1201(f)(2) can also constitute the "technological means" of circumvention, or whether the "technological means" is limited to the reverse engineering tool used to develop the independently created computer program in the first place. Stated differently, the issue is whether Section 1201(f)(2) was meant to be narrow to cover only the development and employment of special tools used to aid the reverse engineering permitted by Section 1201(f)(1), or whether it was intended to permit more generalized circumvention of technological measures by one computer program in order to interoperate with another computer program whose technological protection measures are being circumvented by the first program. A similar ambiguity is embedded in Section 1201(f)(2)'s reference to "other" programs – can a program whose technological measure is circumvented by an independently created computer program, both in the ordinary operation of the independently created computer program and in the reverse engineering that was done to create such program, qualify as an "other" program? The legislative history contains no guidance on the interpretation of "other" in the exemption.

It appears that the Copyright Office agrees with an expansive reading of the Section 1201(f) exemption. After the district court's decision in the Lexmark case came down, Static Control submitted a proposed exemption to the Copyright Office in its 2003 rulemaking proceeding under Section 1201(a)(1) to determine classes of works exempt from the anti-circumvention prohibitions. In particular, Static Control asked for an exemption for the following classes of works:

1. Computer programs embedded in computer printers and toner cartridges and that control the interoperation and functions of the printer and toner cartridge.

2. Computer programs embedded in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product.

3. Computer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance.[770]

[770] Memorandum from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress, "Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition

The Copyright Office set forth its analysis of Static Control's requested exemptions, among many other requested exemptions, in a lengthy memorandum issued on Oct. 27, 2003 by the Register of Copyrights to the Librarian of Congress. Although it is not clear from the memorandum whether the Copyright Office took a position with request to Static Control's second and third proposed exemptions, the Copyright Office determined that no exemption was warranted for the first proposed exemption because "Static Control's purpose of achieving interoperability of remanufactured printer cartridges with Lexmark's … printers could have been lawfully achieved by taking advantage of the defense found in §1201(f), the reverse engineering exemption."[771]

The Copyright Office read the purpose behind Section 1201(f) broadly: "Not only did Congress intend that 'interoperability' include the exchange of information between computer programs; it also intended 'for such programs mutually to use the information which has been exchanged.' Interoperability necessarily includes, therefore, concerns for functionality and use, and not only of individual use, but for enabling competitive choices in the marketplace."[772] The Copyright Office elaborated that the statutory exemptions of Section 1201(f) afford broader exemptions than even the Copyright Office itself could grant by virtue of rulemaking. In particular, the Copyright Office's exemptions are limited to individual acts of exemption prohibited by Section 1201(a)(1), whereas the statutory exemptions of Section 1201(f) include the distribution of the means of circumvention into the marketplace:

> [T]he statutory exemption found in §1201(f) not only permits circumvention of technological measures to analyze and identify interoperable elements of a protected computer program, but also provides exemptions to the trafficking provisions in §1201(a)(2) and 1201(b). Even if the Register had found a factual basis for an exemption, it would only exempt the act of circumvention. It would not exempt the creation and distribution of the means to circumvent or the distribution of interoperable computer programs embedded in devices. Since it is clear that Static Control's goal was not merely to privately circumvent, but rather to facilitate the distribution of competitive toner cartridges to others, a recommendation for an exemption in this rulemaking would have little effect on the intended use.[773]

Accordingly, the Copyright Office concluded that "Congress has comprehensively addressed the important concern of interoperability for competition and functionality within its own statutory exemption" and that an exemption through rulemaking was not necessary.[774]

---

on Circumvention of Copyright Protection Systems for Access Control Technologies," Oct. 27, 2003, p. 172, available as of Jan. 10, 2004 at www.copyright.gov/1201/docs/registers-recommendation.pdf.

771 Id. at 176.

772 Id. at 178 (quoting the House Manager's Report at 14).

773 Id. at 180-81 (emphasis in original).

774 Id. at 183.

Providing Information or Means for Interoperability to Others. Section 1201(f)(3) provides that the "information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section."

Section 1201(f)(3) contains ambiguities with respect to its scope that are similar to those noted with respect to Section 1201(f)(2). The legislative history for Section 1201(f)(3) states the following:

> [Section 1201(f)(3)] recognizes that developing complex computer programs often involves the efforts of many persons. For example, some of these persons may be hired to develop a specific portion of the final product. For that person to perform these tasks, some of the information acquired through the permitted analysis, and the tools to accomplish it, may have to be made available to that person. This subsection allows developers of independently created software to rely on third parties either to develop the necessary circumvention tools or to identify the necessary information to achieve interoperability. The ability to rely on third parties is particularly important for small software developers who do not have the capability of performing these functions in-house. This provision permits such sharing of information and tools.[775]

Although Section 1201(f)(3) clearly contemplates an exemption for distribution to third parties of the "technological means" referenced in Section 1201(f)(2), as well as the "information" gleaned from reverse engineering under Section 1201(f)(1), the same issues of the scope of "technological means" intended to be within the exemption arise as in Section 1201(f)(2). As noted, the Copyright Office seems to read Section 1201(f)(3) broadly to permit the distribution of independently developed computer programs that circumvent the technological protection measures of other programs in order to interoperate with such other programs. The legislative history quoted above, however, seems to read Section 1201(f)(3) more narrowly as directed to distribution of reverse engineering "tools" or information to third party developers who may be hired to assist in the development of an independent computer program, as opposed to a distribution of a competitive product into the marketplace.

These ambiguities in the scope of the Section 1201(f) exemptions will need to be resolved over time through litigation. In addition, it is worth observing that, although Section 1201(f) provides useful exemptions, it leaves open the issue of whether circumvention of access restrictions in order to perform reverse engineering for purposes other than interoperability, such as error correction, is prohibited. The Copyright Office's exemption rulemaking procedures may afford a mechanism to further flesh out or clarify the Section 1201(f) exemptions.

---

[775] S. Rep. No. 105-190, at 33 (1998).

Several cases have adjudicated the scope of the Section 1201(f) exemption:

(i) Universal City Studios Inc. v. Reimerdes

In Universal City Studios, Inc. v. Reimerdes,[776] discussed in further detail in Section II.G.1(m)(4) below, the court rejected the applicability of Section 1201(f) to the defendants' posting on their Web site of, and posting links to, a descrambling computer program known as "DeCSS," which circumvented the encryption of movies stored in digital form on a digital versatile disk ("DVD") encoded with the industry standard Content Scramble System ("CSS"). The defendants argued that DeCSS had been created to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux-compatible players on the market at the time.[777] They further contended that DeCSS was necessary to achieve interoperability between computers running the Linux operating system and DVDs, and that the exception of Section 1201(f) therefore applied.[778]

The court rejected this argument for several reasons. First, Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information, and the defendants did not themselves do any reverse engineering (DeCSS had been created by a third party). Even if the defendants had authored DeCSS, the court ruled that Section 1201(f)(3) would allow the dissemination only of information gleaned from the reverse engineering and solely for the purpose of achieving interoperability as defined in the statute (which was not the reason the defendants posted DeCSS), and not dissemination of the means of circumvention itself.[779] Second, the defendants could not claim that the sole purpose of DeCSS was to create a Linux DVD player, because DeCSS was developed on and ran under the Windows operating system, and could therefore decrypt and play DVD movies on Windows as well as Linux machines.[780] In addition, in an earlier opinion, the court ruled that Section 1201(f) was inapplicable because the legislative history of the DMCA makes clear that Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works, such as movies.[781]

---

[776] 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

[777] Id. at 319.

[778] Id. at 320.

[779] Id.

[780] Id.

[781] Universal City Studios Inc. v. Reimerdes, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000) (citing S. Rep. No. 105-190 (1998) and H.R. Rep. 105-551 (II) (1998)). Section 1201(f) would seem applicable to the original reverse engineering that the developers of DeCSS engaged in, but the trickier issue dealt with by the court is whether it should apply to subsequent use of the DeCSS to gain access to copyrighted works stored on a DVD in order to play such works under the Linux operating system. Such access is for use of the work stored on the DVD (albeit in an interoperable way), whereas the exception speaks in terms of "identifying and analyzing" the copyrighted work to achieve interoperability. In addition, Section 1201(f) appears to be a defense only to the conduct of circumvention prohibited by Section 1201(a)(1), and not to the distribution of devices prohibited

(ii) Storage Technology Corporation v. Custom Hardware Engineering & Consulting

This case rejected an assertion of a Section 1201(f) defense because the defendant's circumvention resulted in an infringing copy of the plaintiff's copyrighted program being made in RAM, and the Section 1201(f) defense exempts circumvention only if it does not result in copyright infringement. For a discussion of the details of the case, see Section II.G.1(o)(4) below.

(iii) Chamberlain Group, Inc. v. Skylink Technologies, Inc.

The facts of this case are set forth in Section II.G.1(o)(2) below. Although this case did not directly adjudicate the scope of the Section 1201(f) exemptions, the court made a few statements in dicta suggesting that Section 1201(f) acts to immunize interoperability from anti-circumvention liability. In that case, the Federal Circuit ruled that the anti-circumvention provisions of Section 1201 do not apply to all forms of circumvention to gain access to a work, but rather only to circumventions that facilitate some form of copyright infringement.[782] The court reached this conclusion in part on the rationale that a broad interpretation of the anti-circumvention provisions to prohibit all forms of unauthorized access, whether or not protected copyright rights were thereby implicated, would be tantamount to "ignoring the explicit immunization of interoperability from anticircumvention liability under § 1201(f)."[783] This language, although dicta, characterizes the Section 1201(f) exemption very broadly.[784]

Another dictum by the court in connection with articulating its rationale for rejecting such a broad interpretation of anti-circumvention liability makes clear the court's belief that the anti-circumvention provisions should not be construed to prevent interoperability of computer programs:

> Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA

---

under Sections 1201(a)(2) and 1201(b). Because the court found that DeCSS is a device within the prohibition of Section 1201(a)(2), it was not subject to the exception of Section 1201(f).

782 Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1195, 1203 (Fed. Cir. 2004), cert. denied, 161 L. Ed. 2d 481 (2005).

783 Id. at 1200.

784 The court noted that it had no occasion to reach the argument, raised by an amicus, that Section 1201(f) should cover the defendant's actions in distributing a product that circumvented technological measures restricting access to the plaintiff's computer program so as to interoperate with it. Because Section 1201(f) is an affirmative defense, the court noted that it would become relevant only if the plaintiff could prove a prima facie case of anti-circumvention liability to shift the burden to the defendant, which the court ruled the plaintiff had ultimately failed to do. Id. at 1200 n.15.

would allow virtually any company to attempt to leverage its sales into aftermarket monopolies – a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit.[785]

(iv) Lexmark International, Inc. v. Static Control Components, Inc.

For a discussion of the applicability of the reverse engineering exception of Section 1201(f) in this case, see Section II.G.1(o)(1) below.

(v) Davidson Assocs. v. Internet Gateway

In this case, the plaintiff Davidson & Assocs., doing business as Blizzard Entertainment, owned the copyrights in several computer games. The games could be played in either a single-player mode or in an online multi-player mode called "Battle.net mode."[786] Blizzard operated a 24-hour online gaming service known as the Battle.net service that allowed owners of certain Blizzard games to play those games against each other in Battle.net mode by linking together over the Internet through Battle.net servers. In addition to multi-player game play, Battle.net mode allowed users to chat with other potential players, to record wins and losses and save advancements in a password protected individual game account, and to set up private games on the Battle.net service to allow players to determine whom they wished to interact with on the Battle.net service.[787] The court noted that these Battle.net mode features were "accessed from within the games themselves," which seems to mean that there was particular code within the Blizzard games that allowed them to operate in Battle.net mode and communicate with the Battle.net servers.[788]

The Battle.net service was designed to prohibit access and use of Battle.net mode by unauthorized or pirated copies of Blizzard games. In particular, in order to log on to the Battle.net service and access Battle.net mode, the Blizzard games were designed to initiate an authentication sequence or "secret handshake" between the game and the Battle.net server based on the "CD Key" of the game, a unique sequence of alphanumeric characters that was printed on a sticker attached to the case in which each game was packaged. The game would pass the CD Key to the Battle.net server, which would verify its validity and determine whether the same CD Key was already being used by another game that was currently logged on to the server. If the CD Key was determined to be valid by the server and not already in use, the server would send a signal to the game allowing it to enter the Battle.net mode and to use the Battle.net gaming services.[789]

---

[785] Id. at 1201 (citations omitted).

[786] Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1168 (E.D. Mo. 2004).

[787] Id.

[788] Id.

[789] Id. at 1169.

In order to install a copy of a Blizzard game, the user was required to click acceptance of a clickwrap license agreement that prohibited reverse engineering of the software and that required the user to agree to the Terms of Use of the Battle.net service, which prohibited emulation or redirection of the communication protocols used by Blizzard as part of Battle.net service for any purpose.[790]

The defendants developed a server, known as the bnetd server, that was designed to emulate the Battle.net service so as to allow players to play their Blizzard games in an online multi-player mode through the bnetd server.[791] In order to develop the bnetd server, the defendants had to reverse engineer the Blizzard games to learn the Battle.net protocol. In addition, because Blizzard games were designed to connect only to Battle.net servers, the defendants had to modify a computer file in the Blizzard games containing the Internet address of the Battle.net servers so as to cause the games to connect to a bnetd server instead. The defendants distributed a utility known as "BNS" that modified such file and caused Blizzard games to connect to the bnetd server rather than the Battle.net server. Once connected to the bnetd server through the modified Internet address file, a Blizzard game would send its CD Key to the bnetd server. When the bnetd server received the CD Key, unlike Battle.net, it did not determine whether the CD Key was valid or currently in use by another player. Instead, the bnetd server would always send the game an "okay" reply. Thus, both authorized as well as unauthorized or pirated copies of Blizzard games could be played in online mode through the bnetd server.[792]

The plaintiffs alleged two violations of the anti-circumvention provisions of the DMCA. First, they alleged that the defendants had violated Section 1201(a)(1)(A) in the course of development of the bnetd emulator by circumventing Blizzard's technological measures (the secret handshake) to gain access to Battle.net mode in the course of their reverse engineering.[793] Although not clear from the court's opinion, the copyrighted work that the defendant's gained access to via their circumvention was apparently the code in the Blizzard games that allowed them to operate in Battle.net mode and to communicate with the Battle.net service.

The defendants argued that their circumvention in the course of reverse engineering was permitted by Section 1201(f)(1) because it was done for the sole purpose of creating and distributing interoperable computer programs such as the bnetd server. They also argued that they had authority to access the Battle.net mode because they lawfully purchased the Blizzard software they reverse engineered.

The district court rejected these defenses. First, it ruled that it was "undisputed that defendants circumvented Blizzard's technological measure, the 'secret handshake,' between Blizzard games and Battle.net, that effectively control access to Battle.net mode."[794] By its

---

[790] Id. at 1169-71.

[791] Id. at 1172.

[792] Id. at *1172-73.

[793] Id. at 1183.

[794] Id. at 1184-85.

reference to "Battle.net mode," the court was again presumably referring to the code in the Blizzard games that allowed them to operate in Battle.net mode. The court rejected the defendants' reliance on Section 1201(f)(1), because the defendants had not developed an independently created computer program. The court noted that the defendants' actions in developing the bnetd server "extended into the realm of copyright infringement" because once game play started, "there are no differences between Battle.net and the bnetd emulator from the standpoint of a user who is actually playing the game."[795] It is unclear from this language precisely what the basis was on which the court found copyright infringement. Perhaps the court believed that the defendants had copied code from the Battle.net server into the bnetd server, for earlier in the opinion the court noted that the plaintiffs contended "that the defendants not only copied code that would achieve interoperability, but also copied elements that would preserve player account information, display of icons, and presentation of ad banners."[796] However, the opinion on appeal suggests that there was no copying of battle.net server code into the bnetd server.[797]

The court also rejected the Section 1201(f)(1) defense because it found that the defendants' actions constituted more than enabling interoperability, since the emulator did not check the validity of the CD Key code passed from the game to the emulator, thereby allowing unauthorized copies of the Blizzard games to play on bnetd servers.[798]

The plaintiffs also asserted that by distributing the bnetd software, the defendants had violated Section 1201(a)(2) by trafficking in devices whose only purpose was to circumvent their secret handshake and allow access to Battle.net mode. The defendants did not dispute the plaintiffs' factual assertions, but instead asserted the defense of Sections 1201(f)(2)-(3) on the ground that those sections entitled them to distribute software to others for the purpose of enabling interoperability with the Blizzard games.[799] The court rejected the defenses on two grounds. First, the court ruled that the defendants' purpose in distributing their software was not solely to enable interoperability, but rather to "avoid the restricted access to Battle.net."[800] In addition, the court reiterated its conclusion that the development and distribution of the bnetd software was infringing, and "persons who commit copyright infringement cannot benefit from the exemptions of § 1201(f)."[801] Accordingly, the court granted the plaintiffs' motion for

---

795 Id. at 1185.

796 Id. at 1184.

797 Davidson & Assocs. v. Jung, 422 F.3d 630, 636 (8th Cir. 2005) ("By necessity, Appellants used reverse engineering to learn Blizzard's protocol language and to ensure that bnetd.org worked with Blizzard games. Combs used reverse engineering to develop the bnetd.org server, including a program called 'tcpdump' to log communications between Blizzard games and the Battle.net server.").

798 334 F. Supp. 2d at 1185.

799 Id. at 1185-86.

800 Id. at 1186.

801 Id. at 1187.

summary judgment on their anti-circumvention and trafficking in anti-circumvention technology claims.[802]

On appeal, the Eight Circuit affirmed in an opinion that is even more terse and difficult to understand than the district court's opinion. The court found a violation of Section 1201(a)(1) merely because unauthorized copies of Blizzard games were allowed to play through the bnetd server, even though the circumvention of the secret handshake did not cause the illegal copy of the Blizzard games to be made in the first place:

> Blizzard games, through Battle.net, employed a technological measure, a software "secret handshake" (CD key), to control access to its copyrighted games. The bnetd.org emulator developed by Appellants allowed the Blizzard game to access Battle.net mode features without a valid or unique CD key. As a result, unauthorized copies of the Blizzard games were played on bnetd.org servers.[803]

The court also ruled that the anti-trafficking provisions of Section 1201(a)(2) had been violated because the bnetd.org emulator had as its sole purpose "to avoid the limitations of Battle.net."[804]

With respect to the Section 1201(f) defense asserted by the defendants, the Eighth Circuit generalized all subsections of Section 1201(f) into one set of requirements as follows:

> To successfully provide the interoperability defense under § 1201(f), Appellants must show: (1) they lawfully obtained the right to use a copy of a computer program; (2) the information gathered as a result of the reverse engineering was not previously readily available to the person engaging in the circumvention; (3) the sole purpose of the reverse engineering was to identify and analyze those elements of the program that were necessary to achieve interoperability of an independently created computer program with other programs; and (4) the alleged circumvention did not constitute infringement.[805]

---

[802] Id.

[803] Davidson & Assocs. v. Jung, 422 F.3d 630, 640 (8th Cir. 2005). The Eighth Circuit distinguished the Lexmark decision by noting that in Lexmark, the Sixth Circuit had found Lexmark's authentication sequence did not effectively control access to the Toner Loading Program and Printer Engine Program at issue, because it was not Lexmark's authentication sequence that controlled access to such programs, but rather the purchase of a Lexmark printer that allowed access to the programs. "Here, Battle.net's control measure was not freely available. Appellants could not have obtained a copy of Battle.net or made use of the literal elements of Battle.net mode without acts of reverse engineering, which allowed for a circumvention of Battle.net and Battle.net mode. Unlike in *Lexmark Int'l, Inc.*, Battle.net mode codes were not accessible by simply purchasing a Blizzard game or logging onto Battle.net, nor could data from the program be translated into readable source code after which copies were freely available without some type of circumvention." Id. at 641. Although the preceding passage is confusing, it seems to imply (by the reference to "literal elements of Battle.net mode") that the secret handshake controlled access to some Battle.net code within the Blizzard game itself. The Court's reference to "Battle.net" seems to be referring to the Battle.net server software.

[804] Id.

[805] Id. at 641-42.

In a very confusing portion of its opinion, the court then ruled that the exemption of Section 1201(f) was not available to the defendants because their circumvention constituted infringement. Precisely what that "infringement" was is unclear, although the court seems to base its holding on the fact that infringement by *third parties* was encouraged because pirated copies of Blizzard games could be played in multi-player mode through the bnetd server (even though the circumvention at issue did not cause or allow the pirated copies of the Blizzard games to be made in the first instance):

> As detailed earlier, Blizzard's secret handshake between Blizzard games and Battle.net effectively controlled access to Battle.net mode within its games. The purpose of the bnetd.org project was to provide matchmaking services for users of Blizzard games who wanted to play in a multi-player environment without using Battle.net. The bnetd.org emulator enabled users of Blizzard games to access Battle.net mode features without a valid or unique CD key to enter Battle.net. The bnetd.org emulator did not determine whether the CD key was valid or currently in use by another player. As a result, unauthorized copies of the Blizzard games were freely played on bnetd.org servers. Appellants failed to establish a genuine issue of material fact as to the applicability of the interoperability exception.[806]

Based on these terse and confusing rulings, the court affirmed summary judgment in favor of the plaintiffs.[807]

(vi) Sony Computer Entertainment America v. Divineo

In Sony Computer Entertainment America, Inc. v. Divineo,[808] the court ruled that downstream lawful or fair uses of a circumvention device, including use to exercise Section 1201(f) rights, did not relieve the defendant from liability for trafficking in such devices under the DMCA. For a discussion of the details of the facts and rulings of the court, see Section II.G.1(b)(3) above.

(8) Encryption Research

Section 1201(g) provides that it is not a violation of the regulations prohibiting circumventing a technological measure if such circumvention is done as an act of good faith "encryption research." "Encryption research" is defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." "Encryption technology" is defined as "the scrambling and descrambling of information using mathematical formulas or algorithms." Sections 1201(g)(2)(C) and (D) require, however, that the person have made a

---

[806] Id. at 642.

[807] Id.

[808] 547 F. Supp. 2d 957 (N.D. Cal. 2006).

good faith effort to obtain authorization before the circumvention, and that such acts not otherwise constitute a copyright infringement or violate other applicable law. Section 1201(g)(5) required that a report be generated to Congress on encryption technologies, with legislative recommendations (if any), not later than one year after enactment of the bill.

(9) Protection of Minors

Section 1201(h) provides that a court, in applying the prohibitions of Section 1201(a) against the manufacture or trafficking in a component or part designed to circumvent technological measures, may consider the necessity of such component or part for its intended and actual incorporation into a product whose sole purpose is to prevent the access of minors to material on the Internet.[809]

(10) Protection of Personally Identifying Information

Section 1201(i) provides that it is not a violation of the Section 1201(a)(1)(A) prohibition on circumventing a technological measure if such measure, or the work it protects, is capable of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected, or if the measure in the normal course of its operation or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work, without providing conspicuous notice of such collection or dissemination to such person and the capability to prevent or restrict the same, and the circumvention is carried out solely to prevent such collection or dissemination. If a technological measure is disclosed to a user as not being capable of collecting or disseminating personally identifying information, then the exception of Section 1201(i) does not apply.

(11) Security Testing

Section 1201(j) provides that it is not a violation of the prohibitions of Sections 1201(a)(1)(A) and 1201(a)(2) if a person is engaged in "security testing," which is defined to mean accessing a computer, computer system, or computer network solely for the purpose of good faith testing, investigating or correcting a security flaw or vulnerability with the authorization of the owner or operator, provided that such act does not otherwise constitute a violation of applicable law (including the Computer Fraud and Abuse Act of 1986).

(12) Copy Restrictions To Be Built Into VCRs and Camcorders

Section 1201(k) dictates that certain technological capabilities be built into consumer analog video cassette recorders (VCRs) and camcorders (professional analog video cassette recorders are exempted) to protect certain analog television programming and prerecorded

---

[809] An earlier version of H.R. 2281 would have expanded this exception to also allow a parent to circumvent a technological measure controlling access to a test or evaluation of that parent's minor child's abilities by a nonprofit educational institution if the parent attempted to obtain authorization before the circumvention and the circumvention was necessary to obtain a copy of the test or evaluation.

movies. Specifically, effective 18 months after enactment of the DMCA, most formats of consumer analog[810] VCRs and camcorders must contain one of two forms of copy control technology in wide use in the market today – either the "automatic gain control technology" (which causes distortion in the images upon playback) or the "colorstripe copy control technology" (which causes distracting visible color stripes to appear through portions of the viewable picture in normal viewing mode). Effective immediately, Section 1201(k) also prohibits tampering with these analog copy control technologies to render them ineffective. The Conference Report accompanying H.R. 2281[811] states that Congress intended this Section to prohibit the manufacture and sale of "black box" devices and software "hacking" that defeat these copy control technologies.

Section 1201(k) defines certain specific encoding rules that such devices must implement in order to preserve the capability to perform long-standing consumer home taping practices. Specifically, such devices cannot limit the copying of traditional broadcasts of programming through basic or extended basic tiers of programming services, although they may limit the copying of pay-per-view, near video-on-demand or video-on-demand transmission, or content stored on prerecorded media, as well the making of second generation copies where the original transmission was through a pay television service (such as HBO, Showtime or the like).

(13) Other Cases Filed Under the Anti-Circumvention Provisions

Several other anti-circumvention cases have been filed under the DMCA:

(i) Sony Computer Entertainment, Inc. v. Connectix, Inc.

On Jan. 27, 1999, Sony Computer Entertainment, Inc. and its U.S. subsidiary Sony Computer Entertainment America, manufacturers and distributors of the Sony PlayStation, filed suit against Connectix, Inc., a company that had developed a software emulator called the "Virtual Game Station" that would enable video games written for the PlayStation to run on Apple computers. In order to create the emulator, Connectix disassembled and reverse engineered the PlayStation's operating system. The plaintiff's complaint included claims for copyright infringement, trademark dilution, and circumvention of technological protection measures.[812]

The circumvention claim was based on the fact that the PlayStation and its video games each contain embedded technological measures to prevent counterfeit games from running on the PlayStation, and the alleged fact that Connectix's emulator software did not contain such

---

[810] Page 68 of the Conference Report states, "The conferees also acknowledge that numerous other activities are underway in the private sector to develop, test, and apply copy control technologies, particularly in the digital environment. Subject to the other requirements of this section, circumvention of these technologies may be prohibited under this Act."

[811] H.R. Rep. No. 105-796, at 78 (1998).

[812] See Band & Issihiki, supra note 765, at 8.

technological measures, thus enabling counterfeit games to run on it. The plaintiffs contended that omission of the PlayStation's technological measures constituted an unlawful circumvention of those measures. In its opposition to the plaintiffs' motion for a temporary restraining order, Connectix asserted that its emulator did in fact implement the PlayStation's technological measures and could not run counterfeit games. Thus, the alleged factual predicate on which the plaintiffs based their circumvention claim was apparently missing. On Feb. 4, 1999, the district court judge denied the plaintiffs' motion for a temporary restraining order.[813]

Even if Connectix's emulator software did not contain the technological measures of the PlayStation, the plaintiffs' circumvention claim appears to be flawed for several reasons. First, the DMCA's prohibition under Section 1201(a)(1) on circumvention of technological measures controlling access was not yet in effect at the time the complaint was filed, and the DMCA contains no prohibition on the act of circumventing copy controls. Second, Connectix's emulator did not actively "circumvent" anything in the games it could run. At most, it simply allegedly operated regardless of whether the video games contained the authentication signals required by the PlayStation (i.e., it allegedly ignored the authentication signal of the PlayStation). But Section 1201(c)(3) provides that Section 1201 does not require a computing product to "provide for a response to any particular technological measure," so long as the product is not primarily designed or produced for the purpose of circumventing a technological measure or has only limited commercially significant purposes or uses other than the same. Because the Connectix emulator was not primarily designed to circumvent technological measures, but rather to run legitimate PlayStation games, it should probably fall within the savings clause of Section 1201(c)(3).[814]

(ii) RealNetworks, Inc. v. Streambox Inc.

On Dec. 20, 1999, RealNetworks, Inc., the developer and distributor of various versions of the "RealPlayer," which embodied "streaming" technology that allowed Internet users to obtain real-time delivery and instant playback of audio and video content over the Internet, brought suit against Streambox, Inc.[815] RealNetworks' products embodied anti-piracy technology. Specifically, RealNetworks supplied copyright holders with a product known as "RealProducer," which converted ordinary audio and video files into digitized "RealAudio" and "RealVideo" files. RealNetworks also offered a "RealServer" product to copyright holders that allowed them to distribute their copyrighted material in a secure format designed to interact only with RealPlayers to further prevent unauthorized access to copyrighted content.[816]

---

[813] Id. at 8-9. On appeal, the Ninth Circuit ultimately held that Connectix's reverse engineering of the Sony Playstation fell within the fair use doctrine. See Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000). The Ninth Circuit's opinion did not address the DMCA issues.

[814] Band & Issihiki, supra note 765, at 8-9.

[815] Complaint for Violation of The Digital Millennium Copyright Act, Contributory, Vicarious and Direct Copyright Infringement, Tortious Interference with Contract, and Lanham Act Violations, RealNetworks, Inc. v. Streambox Inc., No. C99-2070Z (W.D. Wa. Dec. 20, 1999), available as of Dec. 30, 1999 at www.realnetworks.com/company/pressroom/pr/99/rnwk_complaint.html.

[816] Id. ¶ 6.

RealNetworks based its complaint on the following three products developed and distributed by Streambox:

> "Streambox Ripper," which converted any RealAudio file to a file in the format of Windows Media Audio (WMA), MPEG-Layer 3 (MP3), or Microsoft Windows Wave Format (WAV). Once in any of these three formats, an audio file could be copied, stored, or freely distributed, thereby circumventing RealNetworks' security measures.[817]
>
> "Streambox VCR," which mimicked a RealPlayer, tricking RealServers into interacting with it and distributing both RealAudio and RealMedia files to it, thereby also circumventing the RealNetworks' security measures.[818]
>
> "Streambox Ferret," which was supposedly designed to work with and enhance the functionality of RealPlayers. RealNetworks alleged, however, that Streambox Ferret replaced the "snap.com" search engine on the RealPlayer's search bar with a "Streambox" logo that diverted those using the RealPlayer's search function from Snap's search services (with whom RealNetworks had an exclusive arrangement) to a competing service operated by Streambox. In addition, RealNetworks alleged that Streambox Ferret corrupted completely the search functionality of the more recent versions of the RealPlayer.[819]

RealNetworks alleged, among other things, that (i) by circumventing RealNetworks' technological measures that protect the rights of copyright owners to control whether an end-user can copy and distribute copyright owners' works, both Streambox Ripper and Streambox VCR violated Section 1201(b) of the DMCA,[820] and (ii) because the installation of Streambox Ferret modified the graphical user interface and computer code of RealPlayer, thereby creating an unauthorized derivative work, Streambox's distribution of Streambox Ferret made it contributorily liable for copyright infringement, as well as vicariously liable, since Streambox allegedly controlled and profited from the infringement.[821]

In a decision issued Jan. 18, 2000, the court entered a preliminary injunction against Streambox, enjoining the manufacturing and distribution of Streambox VCR and Streambox Ferret, but not of Streambox Ripper.[822] This case raised three important procedural issues with respect to the DMCA. First, the case raised the interesting issue of who has standing to invoke the remedies of the DMCA – specifically, whether RealNetworks should be considered a proper party to bring the lawsuit, since the material that Streambox Ripper and Streambox VCR placed

---

817 Id. ¶¶ 12-13.

818 Id. ¶¶ 17-19.

819 Id. ¶¶ 22-24.

820 Id. ¶¶ 33-35 & 41-43.

821 Id. ¶¶ 48-49.

822 RealNetworks, Inc. v. Streambox Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wa. 2000).

into a different file format (i.e., allegedly circumvented a protection measure for) was copyrighted, not by RealNetworks, but by its customers. As discussed further below, Section 1203 of the DMCA provides: "Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation." Significantly, the reference to "any person" suggests that Section 1203 does not limit its scope to the copyright owner of the material with respect to which a technological protection measure has been circumvented, and the court so held. Specifically, the court ruled that RealNetworks had standing to pursue DMCA claims under Section 1203 based on the fact that it affords standing to "any person" allegedly injured by a violation of Section 1201 and 1202 of the DMCA.[823]

Second, the case raised the issue of what type of "injury" a plaintiff must show under Section 1203. Neither Section 1203 itself nor the legislative history illuminate this issue. In the instant case, RealNetworks was apparently relying on the argument that, because its customers were potentially injured by Streambox's violation of Section 1201(b), RealNetworks itself was also injured. Although the court did not explicitly address this issue, by issuing a preliminary injunction, it implicitly accepted that RealNetworks was exposed to injury cognizable by the DMCA.

Third, the case raised the issue of whether a plaintiff who demonstrates a likelihood of success on the merits of claims under Section 1201 of the DMCA is entitled to a presumption of irreparable harm for purposes of a preliminary injunction, as would be the case in a showing of likely success on a claim for copyright infringement. The court noted that this must be considered an open issue: "Because the DMCA is a recently-enacted statute, there appears to be no authority holding that a plaintiff seeking a preliminary injunction who shows a reasonable likelihood of success on a claim arising under section 1201 of the DMCA is entitled to a presumption of irreparable harm."[824] Accordingly, the court considered in each instance whether Streambox's violations of the DMCA were likely to cause irreparable harm.

Turning to the plaintiff's claims under the anti-circumvention provisions of the DMCA, the court noted that RealNetworks' products embodied two technological measures to control against unauthorized access or copying of content. First, a "Secret Handshake" – an authentication sequence that only RealServers and RealPlayers knew – ensured that files hosted on a RealServer could be sent only to a RealPlayer. Second, a "Copy Switch" was used, which was a piece of data in all RealMedia files that contained the content owner's preference regarding whether or not the stream could be copied by end users.[825] RealPlayers were designed to read the Copy Switch and obey the content owner's wishes.

---

[823] Id. at *15-16. This holding is consistent with CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000). In that case the plaintiff was a cable provider bringing suit against defendants under the DMCA for selling and distributing pirate cable descrambling equipment. The court held that the plaintiff was authorized to bring suit under Section 1203(a), as it was a person injured by a violation of the DMCA.

[824] RealNetworks, 2000 U.S. Dist. LEXIS 1889 at *17.

[825] Id. at *6.

The court ruled that the Secret Handshake constituted a technological measure that effectively controlled access to copyrighted works within the meaning of Section 1201(a)(3)(B), and that the Copy Switch constituted a technological measure that effectively protected the right of a copyright owner to control the unauthorized copying of its work within the meaning of Section 1201(b)(2)(B). The court concluded that, because Streambox VCR was primarily designed to bypass the Secret Handshake and circumvent the Copy Switch (and had only limited commercially significant purposes beyond the same), Streambox VCR violated Sections 1201(a)(2) and 1201(b) of the DMCA.[826]

The court rejected Streambox's defense that Streambox VCR allowed consumers to make "fair use" copies of RealMedia files under the Supreme Court's decision in Sony Corp. v. Universal City Studios, Inc.[827] The court distinguished the Sony case on the ground that, in Sony, the Supreme Court based its holding on the fact that video cassette recorders were mostly used by consumers for "time shift" viewing of programs, rather than the redistribution of perfect digital copies of audio and video files, and that substantial numbers of copyright holders who broadcast their works either had authorized or would not object to having their works time-shifted by private viewers. In the instant case, the court noted, copyright owners had specifically chosen to prevent the copying enabled by the Streambox VCR by putting their content on RealServers and leaving the Copy Switch off.[828]

In addition, the court, citing Nimmer's copyright treatise, ruled that, by passage of the DMCA, Congress had decided that "those who manufacture equipment and products generally can no longer gauge their conduct as permitted or forbidden by reference to the *Sony* doctrine. For a given piece of machinery might qualify as a stable item of commerce, with a substantial noninfringing use, and hence be immune from attack under *Sony's* construction of the Copyright Act – but nonetheless still be subject to suppression under Section 1201."[829] The court also rejected Streambox's asserted defense under Section 1201(c)(3) of the DMCA, which it cited for the proposition that the Streambox VCR was not required to respond to the Copy Switch. The court noted that this argument failed to address Streambox VCR's circumvention of the Secret Handshake, which was enough by itself to create liability under Section 1201(a)(2).[830]

Turning to the Streambox Ripper product, the court ruled that the plaintiff had not established a reasonable likelihood of success on its DMCA claim. RealNetworks maintained that the primary purpose and only commercially significant use for the Ripper was to enable consumers to prepare unauthorized derivative works of copyrighted audio or video content. The court rejected this argument, noting that the Ripper has legitimate and commercially significant uses to enable content owners, including copyright holders and those acquiring content with the content owner's permission, to convert their content from the RealMedia format to other formats.

---

826 Id. at *19-21.

827 464 U.S. 417 (1984).

828 RealNetworks, 2000 U.S. Dist. LEXIS at *21-22.

829 Id. at *23 (quoting 1 M. Nimmer & D. Nimmer, *Nimmer on Copyright* (1999 Supp.) § 12A.18[B]).

830 RealNetworks, 2000 U.S. Dist. LEXIS at *23.

Moreover, there was little evidence that content owners use the RealMedia format as a "technological measure" to prevent end users from making derivative works. In any case, the court found that RealNetworks had not introduced evidence that a substantial number of content owners would object to having end users convert RealMedia files that they legitimately obtained into other formats, or that Ripper would cause injury to RealNetworks.[831]

Finally, the court ruled that the plaintiff was entitled to a preliminary injunction with respect to Streambox Ferret. RealNetworks claimed that Streambox committed contributory or vicarious copyright infringement by distributing the Ferret to the public, because consumers who used the Ferret as a plug-in were making an unauthorized derivative work of the RealPlayer by changing the RealPlayer user interface to add a clickable button that permitted the user to access the Streambox search engine, rather than the Snap search engine. Although the court stated that it was not persuaded that RealNetworks had demonstrated that it was likely to succeed on its contributory/vicarious infringement claims on this basis, the court concluded that RealNetworks had raised serious questions going to the merits of its claims, and the balance of hardships clearly favored RealNetworks, because the addition of the alternative search engine afforded by the Ferret jeopardized RealNetworks' exclusive relationship with Snap.[832]

In September of 2000, the parties settled the lawsuit pursuant to an agreement in which Streambox agreed to modify Streambox Ripper so that it no longer transformed RealMedia streams into other formats, to modify Streambox VCR so that it respected RealNetworks' copy protection features, to license RealNetworks' software development kit (which would allow Streambox to create versions of its products that worked with RealNetworks' copy protection technology), to stop distributing Streambox Ferret, and to pay an undisclosed sum of money.[833]

(iii) Universal City Studios, Inc. v. Reimerdes

In this case, the plaintiffs were copyright holders who distributed motion pictures encoded in a proprietary system for the encryption and decryption of data contained on digital versatile disks (DVDs) known as the Content Scramble System (CSS). The CSS technology was licensed to manufacturers of DVDs, who used it to encrypt the content of copyrighted motion pictures distributed in the DVD format. The plaintiffs filed suit under the DMCA against various defendants whom the plaintiffs alleged violated the anti-circumvention provisions of the DMCA by posting on their websites the source code of a program named "DeCSS," which was able to defeat DVD encryption using the CSS technology and enable viewing of DVD movies on unlicensed players and the making of digital copies of DVD movies.[834] The plaintiffs sought a

---

831 Id. at *27-28.

832 Id. at *30-33.

833 "Early DMCA Lawsuit Settled, Streambox Will Modify Products to Prevent Digital Copying," *BNA's Electronic Commerce & Law Report* (Oct. 11, 2000) at 1019.

834 Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

preliminary and permanent injunction to prevent the defendants from posting DeCSS on their Web site and from linking their site to others that posted DeCSS.[835]

On Jan. 20, 2000, the court entered a preliminary injunction against the defendants, restraining them from posting on any website or otherwise making available DeCSS or any other technology, product or service primary designed or produced for the purpose of, or having only limited commercially significant purposes or use other than, circumventing CSS, or marketed by defendants or others acting in concert with them for use in circumventing CSS.[836] In an opinion issued Feb. 2, 2000, the court set forth its findings of fact and conclusions of law supporting the preliminary injunction.[837]

On Aug. 17, 2000, after a bench trial, the court issued a permanent injunction against the defendants.[838] The court ruled that DeCSS was clearly a means of circumventing CSS, a technological access control measure, that it was undisputed that DeCSS was designed primarily to circumvent CSS, and therefore that DeCSS constituted a prima facie violation of Section 1201(a)(2).[839] The court rejected the defendants' argument that CSS did not "effectively control" access to the plaintiffs' copyrighted works because it was based on a 40-bit encryption key, which the defendants argued was a weak cipher. The court noted that Section 1201(a)(3)(B) provides that a technological measure "effectively controls access to a work" if it requires the application of information or a process with the authority of the copyright owner to gain access to a work. Because one cannot gain access to a CSS-protected work on a DVD without the application of three keys that are required by the player software and are made available only under license, CSS satisfied this definition. The court refused to import into the statute any requirement for a technologically "strong means" of protection.[840]

The court also rejected the defendants' argument that DeCSS was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux-compatible players on the market at the time. The court ruled that, even if there were so, it would be immaterial to whether the defendants had violated Section 1201(a)(2) by trafficking in DeCSS.[841] "The offering or provision of the program is the prohibited conduct – and it is prohibited irrespective of why the program was written, except to

---

835 Id. at 303.

836 Preliminary Injunction, Universal City Studios, Inc. v. Reimerdes, No. 00 Civ. 0277 (LAK) (S.D.N.Y. Jan. 20, 2000) ¶ 2.

837 Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

838 Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). An amended final judgment was entered by the court on Aug. 23, 2001, enjoining the defendants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS was posted. Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

839 111 F. Supp. 2d at 317-19.

840 Id. at 318. The court cited legislative history to the effect that a technological measure "effectively controls access" to a copyrighted work merely if its *function* is to control access. Id. at 317-18.

841 Id. at 319.

whatever extent motive may be germane to determining whether [the defendants'] conduct falls within one of the statutory exceptions."[842]

The court rejected a number of other defenses under the DMCA asserted by the defendants. First, for the reasons set forth in Section II.G.1(g) above in the discussion of Section 1201(f), the court rejected the defendants' argument that the reverse engineering exception of Section 1201(f) was applicable.

Second, the defendants asserted the encryption research defense under Section 1201(g), which requires a showing that the person asserting the defense lawfully obtained the encrypted copy of the work being studied, the circumvention act at issue is necessary to conduct encryption research, the person made a good faith effort to obtain authorization before the circumvention, and the act does not constitute copyright infringement. The court held that the defendants had failed to prove that any of them were engaged in good faith encryption research, nor was there any evidence that the defendants made any effort to provide the results of the DeCSS effort to the copyright owners (which Section 1201(g)(3) instructs the court to take into account in assessing whether one is engaged in good faith encryption research), nor any evidence that any of them made a good faith effort to obtain authorization from the copyright owners.[843]

Third, the defendants asserted the security testing defense under Section 1201(j). The court rejected this defense, which is limited to "assessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorization of the owner or operator," because the record did not establish that DeCSS has anything to do with testing computers, computer systems, or computer networks, and the defendants had not sought authorization for their activities.[844]

Fourth, the defendants claimed that they were engaged in a fair use under Section 107 of the copyright statute. The court categorically rejected this defense, noting that the defendants were not being sued for copyright infringement, but rather for offering to the public technology primarily designed to circumvent technological measures that control access to copyrighted works.[845] The court held that fair use is not a defense to Section 1201(a)(2) of the DMCA: "If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate."[846] The court noted that Congress had provided a vehicle, in the form of rulemaking by the Register of Copyrights, by which particular classes of copyrighted works could be exempted from the prohibitions if noninfringing uses of those

---

[842] Id.

[843] Id. at 320-21.

[844] Id. at 321.

[845] Id. at 322.

[846] Id.

classes of works would be affected adversely by Section 1201(a)(1).[847] The court also rejected the defendants' assertion that, because DeCSS could be used for noninfringing purposes, its distribution should be permitted under Sony Corp. v. Universal City Studios, Inc.[848] The court elected to follow the holding in the RealNetworks case that a piece of technology might have a substantial noninfringing use, and therefore be immune from attack under Sony, yet nonetheless be subject to suppression under Section 1201.[849]

Finally, in one of the most novel aspects of the opinion, the court addressed the issue whether the mere linking by the defendants to other Web sites on which DeCSS could be obtained should be deemed to be offering to the public or providing or otherwise trafficking in DeCSS within the prohibitions of Section 1201(a)(2). The court, noting that the dictionary definitions of the words "offer," "provide," and "traffic" are broad, ruled that "the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it."[850] Accordingly, the court enjoined the defendants from providing three types of links:

> Links "to sites that automatically commence the process of downloading DeCSS upon a user being transferred by defendants' hyperlinks." The court ruled that this was the functional equivalent of the defendants transferring the DeCSS code themselves.[851]
>
> Links "to web pages that display nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS and no other content. The only distinction is that the entity extending to the user the option of downloading the program is the transferee site rather than defendants, a distinction without a difference."[852]
>
> Links "to pages that offer a good deal of content other than DeCSS but that offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS," based on the given facts, in which the defendants had intentionally used and touted the links to "mirror" sites to help others find copies of DeCSS, after encouraging sites to post DeCSS

---

[847] Id. at 323 The court, in a very lengthy analysis, also rejected various First Amendment challenges to the constitutionality of the anti-circumvention provisions of the DMCA. See id. at 325-341.

[848] 464 U.S. 417 (1984).

[849] Reimerdes, 111 F. Supp. 2d at 323. In the preliminary injunction proceeding, one of the defendants asserted a defense under Section 512(c) of the DMCA, discussed below, which limits liability of "service providers" for certain acts of infringement committed through systems or networks operated by them. The court rejected this defense on the ground that Section 512(c) provides protection only from liability for copyright infringement, and not for violations of the anti-circumvention provisions of Section 1201(a)(2). The court also ruled that the defendant had offered no proof that he was a "service provider" within the meaning of Section 512(c). 82 F. Supp. 2d at 217.

[850] Reimerdes, 111 F. Supp. 2d at 325.

[851] Id.

[852] Id.

and checking to ensure that the mirror sites in fact were posting DeCSS or something that looked like it, and proclaimed on their own site that DeCSS could be had by clicking on the links.[853]

On appeal, the defendants renewed their attack on the constitutionality of the DMCA. In Universal City Studios Inc. v. Corley,[854] the Second Circuit rejected such challenges and upheld the constitutionality of the DMCA anti-circumvention provisions. The court first rejected the defendants' argument that Section 1201(c)(1) should be read narrowly to avoid ambiguity that could give rise to constitutional infirmities. The defendants contended that Section 1201(c)(1) could and should be read to allow the circumvention of encryption technology when the protected material would be put to fair uses. The court disagreed that Section 1201(c)(1) permitted such a reading. "Instead, it clearly and simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred."[855] The court held that, in any event, the defendants did not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibited them from making such fair use.[856] "Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique of in the format of the original."[857]

The court ruled that computer programs are not exempted from the category of First Amendment speech merely because their instructions require use of a computer. Rather, the ability to convey information renders the instructions of a computer program in source code form "speech" for purposes of the First Amendment.[858] However, the court held that the "realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, *i.e.*, functional and expressive elements."[859] Accordingly, the scope of First Amendment protection for the DeCSS code at issue was limited.[860]

With this background, the court turned to a First Amendment analysis of the specific prohibitions of the injunction. With respect to the prohibition against posting of the DeCSS code, the court held that the prohibition was content neutral and was directed only toward the nonspeech component of DeCSS – "[t]he DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional

---

[853] Id.

[854] 273 F.3d 429 (2d Cir. 2001).

[855] Id. at 443 (emphasis in original).

[856] Id. at 459.

[857] Id.

[858] Id. at 447.

[859] Id. at 451.

[860] Id. at 453.

capability is not speech within the meaning of the First Amendment."[861] Therefore, the content-neutral posting prohibition, which had only an incidental effect on a speech component, would pass muster if it served a substantial governmental interest unrelated to the suppression of free expression, which the court found that it did.[862]

With respect to the prohibition against linking to other web sites posting DeCSS, the court again noted that a link has both a speech and a nonspeech component. "It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user's computer screen."[863] And again, the court ruled that the prohibition on linking was content neutral. "The linking prohibition applies whether or not the hyperlink contains any information, comprehensible to a human being, as to the Internet address of the web page being accessed. The linking prohibition is justified solely by the functional capability of the hyperlink."[864] The court rejected the defendants' argument that the prohibition burdened substantially more speech than necessary to further the government's legitimate interest because it did not require an intent to cause harm by the linking, and that linking could be enjoined only under circumstances applicable to a print medium. The court found that the defendants' arguments ignored the reality of the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Accordingly, "the fundamental choice between impairing some communication and tolerating decryption cannot be entirely avoided."[865]

Having rejected all constitutional challenges to the district court's injunction, the Second Circuit affirmed the district court's final judgment.[866] The defendants decided not to appeal the case further to the Supreme Court.[867]

(iv) A Related DVD Case Involving Trade Secret Claims – DVD Copy Control Association, Inc. v. McLaughlin (the Bunner case)

This case,[868] although initially filed in state court alleging only misappropriation of trade secrets, presented another fact pattern amenable to a claim under the anti-circumvention provisions of the DMCA. The plaintiff in that case, DVD Copy Control Association, Inc. (DVD

---

[861] Id. at 454.

[862] Id. at 454-55. The court noted that it had considered the opinion of the California Court of Appeal in the Bunner case, discussed in subsection e. below and that to "the extent that *DVD Copy Control* disagrees with our First Amendment analysis, we decline to follow it." Id. at 455 n.29. As noted in subsection e. below, the Supreme Court of California subsequently reversed the California Court of Appeal decision.

[863] Id. at 456.

[864] Id.

[865] Id. at 458.

[866] Id.

[867] Lisa Bowman, "Copyright Fight Comes to an End" (July 3, 2002), available as of July 8, 2002 at http://news.com.com/2102-1023-941685.html.

[868] No. CV786804 (Santa Clara Superior Court, Dec. 27, 1999).

CCA), was the sole licensor of CSS.[869] The plaintiff alleged that various defendants had misappropriated trade secrets in CSS by posting on their websites proprietary information relating to how the CSS technology functions, the source code of DeCSS, and/or providing links to other websites containing CSS proprietary information and/or the DeCSS program.[870]

On Dec. 29, 1999, the court denied an application by the plaintiff for a temporary restraining order that would have required the defendants to remove the DeCSS program and proprietary information from their websites, as well as links to other sites containing the same.[871] However, on Jan. 21, 2000 (the day after the court in Reimerdes issued its preliminary injunction under the DMCA), the judge reversed course and issued a preliminary injunction prohibiting the defendants from "[p]osting or otherwise disclosing or distributing, on their websites or elsewhere, the DeCSS program, the master keys or algorithms of the Content Scrambling System ('CSS'), or any other information derived from this proprietary information."[872]

In its order, the court stated that the evidence was fairly clear that the trade secret was obtained through reverse engineering, and acknowledged that reverse engineering is not considered "improper means" of obtaining a trade secret under the Uniform Trade Secrets Act. "The only way in which the reverse engineering could be considered 'improper means' herein would be if whoever did the reverse engineering was subject to the click license agreement which preconditioned installation of DVD software or hardware, and prohibited reverse engineering. Plaintiff's case is problematic at this pre-discovery state. Clearly they have no direct evidence at this point that [defendant] Jon Johansen did the reverse engineering, and that he did so after clicking on any licence [sic] agreement."[873] Nevertheless, without elaboration, the court found that the "circumstantial evidence, mostly due to the various defendants' inclination to boast about their disrespect for the law, is quite compelling on both the issue of Mr. Johansen's improper means [and] th[e] Defendants' knowledge of impropriety."[874] The court found that the harm to the defendants of the injunction would be minimal, while without the injunction, "the Plaintiff's right to protect this information as secret will surely be lost, given the current power of the Internet to disseminate information and the Defendants' stated determination to do so."[875]

The court rejected the defendants' argument "that trade secret status should be deemed destroyed at this stage merely by the posting of the trade secret to the Internet. To hold otherwise would do nothing less than encourage misappropriators of trade secrets to post the

---

869 Id. ¶ 4.

870 Id. ¶¶ 1, 27-29, 45-50, 60-61.

871 Deborah Kong, "DVD Movie Fight Loses," *San Jose Mercury News* (Dec. 30, 1999) at 1C.

872 Order Granting Preliminary Injunction, DVD Copy Control Assoc. v. McLaughlin (Sup. Ct., County of Santa Clara, Jan. 21, 2000), available as of Jan. 19, 2002 at www.eff.org/pub/Intellectual_property/Video/DVDCCA_case/20000120-pi-order.html.

873 Id. at 2.

874 Id. at 2-3.

875 Id. at 3.

fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible, thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet."[876] The court refused, however, to extend the injunction to links to other websites where DeCSS was posted. The court warned that a ban on Internet links would be "overbroad and burdensome," calling links "the mainstay of the Internet and indispensable to its convenient access to the vast world of information. A website owner cannot be held responsible for all of the content of the sites to which it provides links."[877]

In November 2001, a California Court of Appeal reversed the injunction on First Amendment grounds. In DVD Copy Control Assoc. v. Bunner,[878] the court acknowledged that, if the trial court correctly concluded that the plaintiffs had established a reasonable probability of success, a preliminary injunction would be justified in the absence of any free speech concerns. Nevertheless, the court found that the preliminary injunction could not withstand First Amendment scrutiny. The court ruled that DeCSS was "speech" within the scope of the First Amendment because "[r]egardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS."[879] The court then held that republication of DeCSS by defendant Bunner[880] was "pure speech within the ambit of the First Amendment" and that the preliminary injunction therefore constituted an unlawful prior restraint.[881] "[A] person who exposes the trade secret may be liable for damages if he or she was bound by a contractual obligation to safeguard the secret. And anyone who infringes a copyright held by [the plaintiff] of by an DVD content provider may be subject to an action under the Copyright Act. We hold only that a preliminary injunction cannot be used to restrict Bunner from disclosing DeCSS."[882]

On appeal, the California Supreme Court reversed the California Court of Appeal's decision, ruling that the trial court's preliminary injunction did not violate the First Amendment.[883] Although the Court held that restrictions on the dissemination of computer code were subject to scrutiny under the First Amendment because the code was a means of expressing ideas,[884] it found that the preliminary injunction passed scrutiny, assuming the trial court properly issued the injunction under California's trade secret law, because it was content neutral (and therefore not subject to strict scrutiny) and achieved the requisite balance of interests by

---

[876] Id.

[877] Id. at 4.

[878] 60 U.S.P.Q.2d 1803 (Cal. Ct. App. 2001).

[879] Id. at 1809.

[880] According to Bunner, defendant Jon Johansen actually reverse engineered the CSS software and Bunner merely republished it. He argued that he had no reason to know that DeCSS had been created by improper use of any proprietary information since the reverse engineering of CSS performed by Johansen was not illegal under Norwegian law. Id. at 1805-06.

[881] Id. at 1811.

[882] Id. at 1812.

[883] DVD Copy Control Ass'n v. Bunner, 31 Cal.4th 864 (2003).

[884] Id. at 876.

burdening no more speech than necessary to serve the government interests at stake.[885] The Court emphasized that its holding was "quite limited," and that its ruling that the preliminary injunction did not violate the free speech clauses of the United States and California Constitutions was based on the assumption that the trial court properly issued the injunction under California's trade secret law. "On remand, the Court of Appeal should determine the validity of this assumption."[886]

On remand, the California Court of Appeal held that the preliminary injunction was not warranted under California trade secret law because DeCSS had been so widely distributed on the Internet that it was no longer a trade secret.[887] At the time of the hearing in the trial court for a preliminary injunction, the evidence showed that DeCSS had been displayed on or linked to at least 118 Web pages in 11 states and 11 countries throughout the world and that approximately 93 Web pages continued to publish information about DeCSS. Subsequent to the filing of the law suit, a campaign of civil disobedience began among the programming community to spread the DeCSS code as widely as possible. Persons distributed the code at the courthouse, portions of it appeared on tee shirts, and contests were held encouraging people to submit ideas about how to disseminate the information as widely as possible.[888]

The court stated, "Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value."[889] However, in the instant case, the court held that the evidence in the case demonstrated that DeCSS had been published to "a worldwide audience of millions" and "the initial publication was quickly and widely republished to an eager audience so that DeCSS and the trade secrets it contained rapidly became available to anyone interested in obtaining them."[890] Accordingly, the plaintiff had not established a likelihood of success on its trade secret claim because DeCSS had been so widely published that the CSS technology "may have lost its trade secret status."[891]

In a related DeCSS case involving jurisdictional issues, defendant Matthew Pavlovich, a Texas resident who posted DeCSS on the web, was sued by the movie industry in California. A state judge granted an injunction against his posting of DeCSS on trade secret grounds. The California Supreme Court ruled that Pavlovich could not be sued in California because he did not have substantial ties to the state. In January of 2004, the U.S. Supreme Court reversed an

---

885 Id. at 877-85.

886 Id. at 889.

887 DVD Copy Control Ass'n Inc. v. Bunner, 116 Cal. App. 4th 241 (6th Dist. 2004).

888 Id. at 248-49.

889 Id. at 251.

890 Id. at 252-53.

891 Id. at 255.

emergency stay of the California Supreme Court's decision and lifted the injunction. Justice O'Connor noted in the order that there was no need to keep DeCSS a secret.[892]

(v) A Related DVD Case – Norwegian Prosecution of Jon Johansen

In January 2002, Norwegian prosecutors brought criminal charges against Jon Johansen, one of the original three authors of the DeCSS program, for violating Norwegian hacking laws.[893] On Jan. 11, 2002, the civil rights organization Electronic Frontier Norway (EFN) issued a press release calling for Johansen's acquittal and full redress.[894] After a trial, a three-judge court in Oslo acquitted Johansen, ruling that consumers have rights to view legally obtained DVD films "even if the films are played in a different way than the makers had foreseen." On appeal, Johansen was again acquitted.[895]

(vi) Another Challenge to the DMCA – The Felten Case.

During 2000, the Secure Digital Music Initiative (SDMI) offered a cash prize to anyone who could break its watermark encryption scheme for the protection of digital content. A team of scientists, led by Prof. Edward Felten of Princeton University, was able to crack the scheme and desired to publish a paper on how they were able to do it. The RIAA threatened Prof. Felten, contending that publication of the paper would violate the anti-circumvention provisions of the DMCA. As a result of the threats, Prof. Felten withdrew publication of his paper from an April 2001 conference. In June 2001, he and seven other researchers, together with the Usenix Association (a professional organization that had accepted Felten's paper for a security symposium to be held during August 2001), filed a lawsuit against the RIAA, seeking a declaration that publication of their work would not violate the DMCA, and against the Justice Department to block it from prosecuting the symposium organizers for allowing the paper to be presented.[896] On Nov. 28, 2001, a district judge in New Jersey dismissed the lawsuit, apparently concluding that neither the RIAA nor the Justice Department had imminent plans to seek to stop Prof. Felten from publishing his findings.[897] Citing assurances from the government, the RIAA,

---

892 Samantha Chang, "Supreme Court Unscrambles DVD Decision" (Jan. 17, 2004), available as of Jan. 19, 2004 at www.reuters.com/newsArticle.jhtml?type=musicNews&storyID=4152687.

893 Declan McCullagh, "Norway Cracks Down on DVD Hacker" (Jan. 10, 2002), available as of Jan. 19, 2002 at www.wired.com/news/politics/0,1283,49638,00.html.

894 The press release was available as of Jan. 19, 2002 at www.efn.no/freejon01-2002.html.

895 "Court Surprised DVD-Jon's Lawyer" (Dec. 22, 2003), available as of Dec. 22, 2003 at www.aftenposten.no/english/local/article.jhtml?articleID=696470.

896 Declan McCullagh, "Code-Breakers Go to Court" (June 6, 2001), available as of Jan. 19, 2002 at www.wired.com/news/mp3/0,1285,44344,00.html.

897 Robert Lemos, "Court Dismisses Free-Speech Lawsuit" (Nov. 28, 2001), available as of Jan. 19, 2002 at http://news.cnet.com/news/0-1005-200-8010671.html.

and the findings of the district judge, in Feb. of 2002, Prof. Felten and his research team decided not to appeal the dismissal of their case.[898]

(vii) Pearl Investments, LLC v. Standard I/O, Inc.

In this case, Pearl hired Standard to perform software programming services to develop an automated stock-trading system (ATS). After completion of ATS, an employee of Standard named Chunn who had helped develop ATS, working on his own time, created software for his own experimental automated trading system, which he maintained on a server separate from the server that Pearl's ATS system was operating on, although Chunn's server was hosted by the same service provider as Pearl's ATS system.[899] Pearl's ATS system operated on a virtual private network (VPN) that contained access restrictions implemented through a special router to the VPN.[900] At one point, Pearl requested the service provider to install Linux on its ATS server. The service provider mistakenly installed Linux on Chunn's server, which was plugged into Pearl's router. Pearl alleged that a "tunnel" (a secure connection) was configured in the router that provided a connection between Chunn's server and Pearl's server, thereby allowing Chunn to circumvent Pearl's password-protected VPN and gain unauthorized access to its ATS system running on the VPN, which included Pearl's copyrighted software.[901]

Pearl brought claims against Standard and Chunn for, among other things, violation of Section 1201(a)(1)(A) of the DMCA based on the alleged creation of the tunnel. Both the plaintiff and the defendants sought summary judgment on the claim. The court ruled that Standard was entitled to summary judgment because the evidence was undisputed that Chunn, in developing and operating his automated trading system, was acting solely on his own and not as an employee of Standard. Standard could therefore not be held liable for his actions.[902]

The court, however, denied summary judgment to Chunn. First, the court ruled that Pearl's VPN was the "electronic equivalent" of a locked door that fit the definition of a technological protection measure put in place by the copyright owner to control access to Pearl's copyrighted ATS software.[903] The court rejected the argument that the VPN did not effectively control Chunn's access to the ATS system in view of the fact that he had written the ATS system himself and maintained a backup file of it for Pearl. "The question of whether a technological measure 'effectively controls access' is analyzed solely with reference to how that measure works 'in the ordinary course of its operation.' 17 U.S.C. § 1201(a)(3)(B). The fact that Chunn had alternative means of access to the works is irrelevant to whether the VPN effectively

---

898 Electronic Frontier Foundation press release, "Security Researchers Drop Scientific Censorship Case" (Feb. 6, 2002), available as of Feb. 10, 2002 at www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html. The government stated in documents filed with the court in Nov. 2001 that "scientists attempting to study access control technologies" are not subject to the DMCA. Id.

899 Pearl Investments, LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 339-40 (D. Me. 2003).

900 Id. at 342, 349.

901 Id. at 341-42 & n.36, 349.

902 Id. at 346-47, 349-50.

903 Id. at 350.

controlled access to them."[904] Finally, the court ruled that because there was a factual dispute about whether only employees of the service provider, rather than Chunn, had configured the tunnel from Chunn's server to the Pearl VPN, or whether Chunn had configured his server and router to tunnel into Pearl's network, Chunn was not entitled to summary judgment on the DMCA claim.[905]

In a subsequent jury trial, the jury found for Chunn on Pearl's DMCA claim.[906]

(viii) 321 Studios v. Metro Goldwyn Mayer Studios, Inc.

In this case, 321 Studios marketed and sold software called DVD Copy Plus, which was capable of copying the video contents of a DVD, both encrypted and unencrypted with the DeCSS encryption scheme, onto a recordable CD. 321 Studios sought a ruling that its software did not violate the anti-circumvention provisions of the DMCA.[907] The court ruled that the software's capability to decrypt DVDs encoded with CSS did violate the anti-circumvention provisions. The court first rejected 321 Studios' argument that CSS was not an effective technological measure because the CSS access keys were widely available on the Internet. The court held that "this is equivalent to a claim that, since it is easy to find skeleton keys on the black market, a deadbolt is not an effective lock to a door."[908]

With respect to the specific prohibition of Section 1201(a)(2), 321 Studios argued that it had the authority of the copyright holder to decrypt DVDs protected by CSS because its product worked only on original DVDs, and the purchaser of a DVD has the authority of the copyright holder to bypass CSS to play the DVD. The court rejected this argument, citing Universal City Studios, Inc. v. Corley[909] for the proposition that purchase of a DVD does not authorize the purchaser to decrypt CSS, but rather only to view the content on the DVD. Only a licensed DVD player has the authority of the copyright holder to decrypt CSS and 321 Studios did not hold a CSS license.[910]

With respect to the specific prohibition of Section 1201(b)(1), 321 Studios argued that CSS was not a copy control measure because it controlled only access to content and did not control or prevent copying of DVDs. The court rejected this argument, noting that while it was technically correct that CSS controlled access to DVDs, "the purpose of this access control is to control copying of those DVDs, since encrypted DVDs cannot be copied unless they are

---

[904] Id.

[905] Id.

[906] See Pearl Investments v. Standard I/O, Inc., 324 F. Supp. 2d 43 (2004) (rejecting Pearl's claim that the jury's verdict in favor of Chunn on the DMCA claim was inconsistent with its conclusion that Chunn's physical hookup to the Pearl system caused damage to Pearl).

[907] 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1089-90 (N.D. Cal. 2004).

[908] Id. at 1095.

[909] 273 F.3d 429 (2d Cir. 2001).

[910] 321 Studios, 307 F. Supp. 2d at 1096.

accessed."[911] The court also rejected 321 Studios' argument that the primary purpose of DVD Copy Plus was not to violate rights of a copyright holder since the software could be used for many purposes that did not involve accessing CSS or that involved making copies of material in the public domain or under fair use principles. In a potentially very broad holding, the court held that the downstream uses of DVD Copy Plus, whether legal or illegal, were irrelevant to determining whether 321 Studios itself was violating the DMCA.[912] "It is the technology itself at issue, not the uses to which the copyrighted material may be put. This Court finds, as did both the Corley and Elcom courts, that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer's violation of the provisions of § 1201(b)(1)."[913]

321 Studios also argued that its software did not violate Section 1201(b)(2) because it used authorized keys to decrypt CSS. The court ruled that, "while 321's software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses CSS."[914]

Finally, 321 Studios argued that, under the common requirement of both Sections 1201(a)(2) and 1201(b)(1), its DVD Copy Plus software was not primarily designed and produced to circumvent CSS, but rather was designed and produced to allow users to make copies of all or part of a DVD, and that the ability to unlock CSS was just one of the features of its software. The court rejected this argument, noting that Sections 1201(a)(2) and 1201(b)(1) both prohibit any technology or product "or part thereof" that is primarily designed or produced for circumvention. Because it was undisputed that a portion of 321 Studios' software was solely for the purpose of circumventing CSS, that portion of the software violated the DMCA.[915] Accordingly, the court enjoined 321 Studios from manufacturing, distributing, or otherwise trafficking in any type of DVD circumvention software.[916]

(ix) I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.

This case reached the opposite result from the 321 Studios v. Metro Goldwyn Mayer case, and held that the unauthorized use of an otherwise legitimate, owner-issued password does

---

911 Id. at 1097.

912 Id.

913 Id. at 1097-98.

914 Id. at 1098. This holding is contrary to that reached by the court in I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004), discussed in the next subsection.

915 321 Studios, 307 F. Supp. 2d at 1098. The court ruled that it could not determine on summary judgment whether the software had only limited commercially significant purposes other than circumvention, and that would be an issue a jury would have to decide. Id. The court also rejected 321 Studios' challenge to the constitutionality of the anti-circumvention provisions on the ground that is unconstitutionally restricted 321 Studios' right to tell others how to make fair use of a copyrighted work, impermissibly burdened the fair use rights of others, and exceeded the scope of Congressional powers. Id. at 1098-1105.

916 Id. at 1105.

not constitute a "circumvention" of a technological measure under the DMCA.[917] The plaintiff owned a web-based service that provided information on tracking magazine advertising exclusively to its clients through proprietary passwords. The defendant obtained a user identification and password issued to a third party and made unauthorized use of the same to gain access to the plaintiff's web site, from which the defendant downloaded approximately 85% of the report formats and copied those formats into its competing service.[918] The court ruled there was no DMCA violation because "what defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure's author. … Defendant did not surmount or puncture or evade any technological measure to do so; instead, it used a password intentionally issued by plaintiff to another entity."[919]

(x) Paramount Pictures Corp. v. 321 Studios.

The court in this case, in a very short opinion citing the Corley and Reimerdes cases and for the reasons stated therein, held that 321 Studios violated the anti-circumvention provisions of the DMCA by manufacturing and selling its software product that permitted the possessor of a DVD encoded with CSS to decode CSS and thereby make identical copies of the DVD. The court enjoined 321 Studios from manufacturing, distributing, linking to, or otherwise trafficking in any of its software products that were capable of decrypting CSS.[920]

(xi) Macrovision Corp. v. 321 Studios

In this case, the same judge as in the Paramount Pictures case, in a one paragraph opinion that simply cited his earlier decision in the Paramount Pictures case, issued a preliminary injunction against 321 Studios barring it from selling the various versions of its DVD copying software.[921] In August of 2004, 321 Studios reached a settlement with the motion picture industry, which included a financial payment and an agreement to stop distributing its DVD copying software worldwide, and ceased operations.[922]

(xii) Comcast of Illinois X v. Hightech Electronics, Inc.

In this case, the defendant Hightech set up a website named 1-satellite-dish.com that contained links to over thirty other websites selling illegal cable pirating devices. Comcast brought claims under Sections 1201(a)(2) and (b)(1) against the website as well as against Net

---

[917] I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004).

[918] Id. at 523.

[919] Id. at 532-33.

[920] Paramount Pictures Corp. v. 321 Studios, 69 U.S.P.Q.2d 2023, 2023-24 (S.D.N.Y. 2004).

[921] Macrovision Corp. v. 321 Studios, 2004 U.S. Dist. LEXIS 8345 (S.D.N.Y. May 12, 2004).

[922] "Maker of DVD-Copying Products Reaches Settlement Over Suits" (Aug. 10, 2004), available as of Aug. 11, 2004 at www.siliconvalley.com/mld/siliconvalley/news/editorial/9364923.htm.

Results, the named domain server for the 1-satellite-dish.com website.[923] The defendants argued that only copyright holders can bring suit under the anti-circumvention provisions and that Comcast, in regard to the cable signals at issue, was not the copyright owner. The court rejected this argument, citing CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000), which held that the plaintiff cable provider had standing to bring suit under Section 1203(a) against the defendants for selling and distributing pirate cable descrambling equipment, as it was a person injured by a violation of the DMCA Accordingly, the Comcast court concluded that Comcast could bring its claim under the DMCA.[924]

With respect to the merits of the DMCA claims, the court ruled that Comcast controlled through technological measures access to copyrighted programs it provided to its subscribers by scrambling those programs, and that such measures also protected the rights of the copyright owners in those programs, as required by Sections 1201(a)(2) and (b)(1). Citing the Reimerdes case, the court noted that there can be a violation of the DMCA for maintaining links to other websites that contain access to or information regarding circumvention technology. The court noted that the Intellectual Reserve case had refused to find contributory liability for posting links to infringing websites because there was no direct relationship between the defendant and the people who operated the websites containing the infringing material, and the defendants did not receive any kind of compensation from the linked websites.[925]

By contrast, in the instant case, the court noted that Comcast had alleged that Hightech received compensation from the website operators that linked to 1-satellite-dish.com. In addition, the court found that Net Results, as the domain server of websites selling illegal cable equipment, could possibly be engaging in trafficking under the DMCA because it was allegedly assisting sellers of illegal cable equipment in distributing such equipment. The court therefore concluded that Comcast had sufficiently stated a claim against the defendants under the DMCA in trafficking or acting in concert with a person who had manufactured or distributed illicit circumvention equipment, and denied the defendants' motion to dismiss the DMCA claims.[926]

(xiii) Davidson & Assocs. v. Internet Gateway

For a discussion of this case, which found violations of both the anti-circumvention and trafficking prohibitions of Section 1201, see Section II.G.1(g)(5) above.

(xiv) Agfa Monotype Corp. v. Adobe Sys.

This case addressed the issue of whether a passive bit or flag indicating the copyright owner's preference with respect to copying or distribution constitutes an effective technological access control measure or measure protecting copyright rights, and held that it does not. The

---

[923] Comcast of Illinois X v. Hightech Electronics, Inc., 2004 Copyr. L. Dec. ¶ 28,840 at pp. 37,299 & 37,232-33 (N.D. Ill. 2004).

[924] Id. at 37,233.

[925] Id.

[926] Id. at 37,233-34.

plaintiffs were the copyright owners in about 3,300 copyrighted TrueType fonts. The plaintiffs alleged that Version 5 of Adobe's Acrobat product violated the anti-circumvention provisions of the DMCA because it ignored the "embedding bits" in certain of the plaintiffs' fonts that indicated whether the fonts were licensed for editing.[927]

Adobe Acrobat 5.0 was capable of embedding fonts into portable electronic documents stored in Adobe's Portable Document Format (PDF). The court described the technology of font embedding as follows:

> A font is copied when it is embedded. Fonts are embedded through embedding bits. Embedding bits indicate to other programs capable of reading them, such as Adobe Acrobat, the font embedding licensing rights that the font vendor granted with respect to the particular font. The software application decides whether or not to embed the font based upon the embedding bit. An embedding bit cannot be read by a computer program until that program has already accessed the font data file. TrueType Fonts are not encrypted, scrambled, or authenticated. A TrueType Font data file can be accessed regardless of the font's embedding permissions. A program seeking to access a TrueType font need not submit a password or complete an authorization sequence to access, use or copy TrueType Fonts.[928]

The Microsoft TrueType Font specification defined four levels of embedding bit restrictions: Restricted (font cannot be embedded); Print & Preview (font can be embedded but the document must be opened as read-only and no edits may be applied to the document), Editable (font can be embedded and the document may be opened for reading and editing), and Installable.[929] Acrobat 5.0 made it possible for the first time to embed in the "form field" or "free text annotation" of a PDF document[930] any TrueType Font whose embedding bit was not set to "Restricted," including fonts whose embedding bit was set to "Print and Preview." This capability of Acrobat 5.0 was referred to as the "Any Font Feature."[931]

The plaintiffs contended that the Any Font Feature resulted in "editable embedding," because a recipient of a PDF file with embedded fonts could use the fonts to change the contents of a form field or free text annotation. The plaintiffs further contended that such editable embedding was possible only because Acrobat 5.0 allowed the embedding bits set by the plaintiffs to be "circumvented" in violation of the DMCA.[932]

---

[927] Agfa Monotype Corp. v. Adobe Sys., 404 F. Supp. 2d 1030, 1031-32 (N.D. Ill. 2005).

[928] Id. at 1031.

[929] Id. at 1031-32.

[930] A PDF form field was designed to allow a recipient to complete an electronic form and electronically return the information inputted on the form to the creator. A PDF free text annotation was designed to allow recipient to insert comments into the PDF document that could be viewed by the creator when electronically returned. Id. at 1033.

[931] Id. at 1032.

[932] Id. at 1034.

The court rejected the plaintiffs' claims under both Sections 1201(a)(2) and 1201(b)(1) of the DMCA. With respect to Section 1201(a)(2), the court ruled that the plaintiffs' embedding bits did not effectively control access to the TrueType fonts. The court found that an embedding bit was a passive entity that did nothing by itself. Embedding bits were not encrypted, scrambled or authenticated, and software applications such as Acrobat 5.0 did not need to enter a password or authorization sequence to obtain access to the embedding bits or the specification for the TrueType font (which was publicly available for free download from the Internet). The embedding bits therefore did not, in their ordinary course of operation, require the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the plaintiffs' TrueType fonts, as required by Section 1201(a)(3)(B) in order for a technological measure to effectively protect access to a copyrighted work.[933]

In addition, the court ruled that Acrobat 5.0 did not contain technology, components or parts that were *primarily* designed to circumvent TrueType embedding bits. The court found that Acrobat 5.0 had many commercially significant purposes other than to circumvent embedding bits, even if it did circumvent them. The purpose of the embedded font capability in Acrobat 5.0 was so that electronic documents could look exactly the same when printed and viewed by a recipient as sent by the creator. The primary purpose of the forms feature was to allow recipients to complete electronic forms they receive and electronically return the information inputted on the form to the creator. Similarly, the commercial purpose of the free text annotation feature was to allow recipients to insert comments into the PDF that could be viewed by the creator when electronically returned. Nor was Acrobat 5.0 marketed for the primary purpose of circumventing the embedding bits – Adobe had made no mention of embedding bits, circumvention of embedding bits, or the Any Font Feature in any of its marketing materials for Acrobat 5.0.[934]

With respect to the plaintiffs' Section 1201(b)(1) claim, Adobe argued, and the court agreed, that the embedding bits did not constitute a technological measure that prevented, restricted, or otherwise limited the exercise of a right of copyright. The plaintiffs had already authorized the copy and distribution of their TrueType fonts for embedding in PDF documents for "Print and Preview" purposes. Acrobat 5.0 did not make an additional copy or distribution of a font to embed the font in free text annotations or form fields, and the plaintiffs' copyright did not give them the right to control subsequent use of lawfully made copies of the fonts.[935]

In addition, for the same reasons noted in connection with the plaintiffs' Section 1201(a)(2) claim, the court ruled that Acrobat 5.0 as a whole and the parts thereof were not primarily designed or promoted for font embedding purposes and had many other commercially significant purposes other than circumventing the embedding bits associates with the plaintiffs'

---

[933] Id. at 1036-37.

[934] Id. at 1032-33.

[935] Id. at 1038-40.

TrueType fonts. Accordingly, the court granted Adobe's motion for summary judgment with respect to the plaintiffs' anti-circumvention claims.[936]

(xv) Egilman v. Keller & Heckman

This case agreed with the I.M.S. case and held that access to a computer through the unauthorized use of a valid password does not constitute an unlawful circumvention.[937] The plaintiff Egilman was a medical doctor and testifying expert witness in a case in which the court had issued an order prohibiting anyone involved in the litigation from publishing any statements on Internet websites over which they had control concerning the litigation. Egilman was sanctioned for violating the order by publishing certain inflammatory statements on his website. Egilman claimed that one of the defendant's law firms had obtained the user name and password to his website without authorization and disclosed that information to another defendant's law firm, which then used the user name and password to gain access to his website, from which the firm obtained information showing that Egilman had violated the court order. Egilman asserted a claim under the anti-circumvention provisions against the law firm.[938]

The court rejected the claim. It reviewed the facts and holding of the I.M.S. case discussed in subsection j. above, and found that the case was correctly decided.[939] The court therefore ruled that "using a username/password combination as intended – by entering a valid username and password, albeit without authorization – does not constitute circumvention under the DMCA." The "technological measure" employed by Egilman had not been "circumvented," but rather merely utilized.[940]

(xvi) Macrovision v. Sima Products Corp.

In Macrovision v. Sima Products Corp.,[941] the court held that the defendant's products, which eliminated Macrovision's Analog Copy Protection (ACP) signals imprinted on DVDs containing copyrighted works to prevent the copying of the DVDs, violated the anti-circumvention provisions. The ACP system inserted additional information in the non-visible portion of the analog signal, the practical effect of which was to render videotaped copies of the analog signal so visually degraded as to be unwatchable. The defendant's devices eliminated Macrovision's ACP from an analog signal. The removal function was effectuated by a single chip, usually the SA7114 chip from Philips. Macrovision contended, and Sima did not dispute,

---

936 Id. at 1040.

937 Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105 (D.D.C. 2005).

938 Id. at 107-09.

939 Id. at 112-14.

940 Id. at 114.

941 2006 U.S. Dist. LEXIS 22106 (S.D.N.Y. Apr. 20, 2006).

that Sima's devices could be fitted with an alternate chip manufactured by Philips that, under license from Macrovision, would recognize the ACP and not allow for its circumvention.[942]

Sima contended that its devices were intended primarily to allow the consumer to make "fair use" backup copies of a DVD collection. The court noted, however, that although the DMCA provides for a limited "fair use" exception for certain *users* of copyrighted works under Section 1201 (a)(2)(B), the exception does not apply to *manufacturers* or *traffickers* of the devices prohibited by Section 1201(a)(2).[943]

Sima argued that the "primary purpose" of its devices was not circumvention. The court rejected this argument, noting that, although some of the devices had some auxiliary functions, Sima did not argue that it was necessary for the device to be able to circumvent ACP in order to perform those functions. Nor did Sima argue that using the Macrovision-licensed Philips chips would prevent the devices from performing the auxiliary functions or facilitating the copying of non-protected works, such as home videos. Accordingly, the devices had only limited commercially significant purposes or uses other than circumvention.[944] The court also noted that Sima had touted on its web site the devices' capability of circumventing copy protection on copyrighted works. And the DMCA does not provide an exception to the anti-circumvention provisions for manufacturers of devices designed to enable the exercise of fair use rights. Finally, the court noted that in any event Sima had cited no authority, and the court was aware of none, for the proposition that fair use includes the making of a backup copy.[945] Accordingly, the court preliminarily enjoined Sima from selling its devices and any other products that circumvented Macrovision's copyright protection technologies in violation of the DMCA.[946]

(xvii) Nordstrom Consulting, Inc. v. M&S Technologies, Inc.

In Nordstrom Consulting, Inc. v. M&S Technologies, Inc.,[947] Nordstrom, acting as a consultant, developed software for a visual eye chart to be distributed as part of M&S's visual acuity systems. Nordstrom retained ownership of the copyrights in the software and, after a falling out with M&S, assigned the copyrights to a separate corporation. After leaving M&S, the plaintiffs alleged that M&S violated the DMCA by circumventing the password protection on a computer used by Nordstrom in order to gain access to the software.[948] The court rejected this claim. Citing the Chamberlin v. Skylink case, the court noted that there must be a showing that the access resulting from the circumvention led to infringement, or the facilitation of infringement, of a copyrighted work, and the plaintiffs had failed to make such a showing. The

---

942 Id. at *2-3.

943 Id. at *2-3, 6.

944 Id. at *6-7.

945 Id. at *7-8.

946 Id. at *11-12.

947 2008 U.S. Dist. LEXIS 17259 (N.D. Ill. Mar. 4, 2008).

948 Id. at *3-8.

court noted it was undisputed that the defendant had accessed the software in order to repair or replace the software of a client of M&S and a valid licensee of the software, so the circumvention of the password did not result in an infringement or the facilitation of infringement.[949]

M&S, in turn, alleged that Nordstrom had violated the DMCA by circumventing the digital security of M&S's computer network. M&S's network was divided into two parts, one dealing with visual acuity systems and one with hotel/hospitality businesses. M&S asserted that, while Nordstrom had a password to access the acuity side of the system, he did not have a password to access the hotel side, yet Nordstrom claimed to have accessed the hotel side. The court denied summary judgment on M&S's claim because of factual disputes. Nordstrom asserted that he did not access the hotel side of the system and that any materials on the hotel side were not registered copyrights. By contrast, M&S had offered evidence that Nordstrom accessed the hotel side of the system, and alleged that the hotel side contained copyrighted works.[950]

(xviii) R.C. Olmstead v. CU Interface

This case agreed with the I.M.S. case and held that access to a computer through the unauthorized use of a valid username and password does not constitute an unlawful circumvention.[951] The plaintiff was the owner of data processing software for credit unions called RCO-1 that it licensed to the defendant. The defendant CUI hired some developers to develop a replacement program for RCO-1 and, to aid development, allowed the developers to gain access to RCO-1 using valid usernames and passwords issued to CUI. The plaintiff claimed that such unauthorized access violated the DMCA. The court rejected this claim, finding the case indistinguishable from I.M.S. and the reasoning of I.M.S. persuasive. The court also noted that the license agreement between the plaintiff and CUI did not set any restrictions regarding issuance of usernames and passwords, so that the plaintiff could not even show that CUI's use of its usernames and passwords was unauthorized.[952] "Simply put, CUI did not circumvent or bypass any technological measures of the RCO software – it merely used a username and password – the approved methodology – to access the software."[953]

(xix) Avaya v. Telecom Labs

In this case, the court refused to decide on a motion for summary judgment the issue addressed in the I.M.S. case of whether unauthorized use of a valid password to gain access to software constitutes a violation of the DMCA.[954] The plaintiff Avaya sold PBX systems with

---

[949] Id. at *23-24/

[950] Id. at *30-31.

[951] R.C. Olmstead, Inc. v. CU Interface, LLC, 2009 U.S. Dist. LEXIS 87705 (N.D. Ohio Mar. 27, 2009).

[952] Id. at *21-24.

[953] Id. at *24.

[954] Avaya, Inc. v. Telecom Labs, Inc., 2009 U.S. Dist. LEXIS 82609 (D.N.J. Sept. 9, 2009).

maintenance software embedded in them. When selling a new system, Avaya supplied the customer with a set of default passwords that the customer used to first log in to the system. Avaya alleged that the passwords were used without authorization by the defendants to log in and gain access to Avaya's maintenance software. Defendants moved for summary judgment that use of valid logins to gain access to software does not violate the DMCA. The court ruled that summary judgment was not appropriate because granting the motion would not result in dismissal of any portion of Avaya's DMCA claims from the case. All that would be resolved would be the abstract issue of whether use of valid logins does not violate the DMCA. Because Avaya had not identified a single, specific PBX to which the alleged illegal conduct was applied, ruling on the motion would have no effect until such time as the defendants could prove which of the PBXs at issue were accessed with the known, valid logins that they alleged were immune from DMCA liability.[955] "Avaya's DMCA claims may or may not have merit, but a summary judgment rendered on a discrete set of facts that have yet to be proven is not the proper vehicle for that determination."[956]

(xx) Actuate v. IBM

In Actuate Corp. v. International Business Machines Corp.,[957] Actuate alleged that IBM's unauthorized posting on an IBM web site of Actuate's copyrighted software for downloading, together with the license keys that allowed for unlimited use of such software by downloaders, whether they were authorized to use the software or not, constituted circumvention of technological measures on the software that restricted access to it and trafficking in circumvention devices. IBM filed a motion to dismiss the claim, relying on the I.M.S., Egilman, and R.C. Olmstead cases for the proposition that improper use of a legitimate password issued by the copyright holder does not constitute circumvention.[958]

The court denied the motion. It found the I.M.S., Egilman, and R.C. Olmstead cases in conflict with the 321 Studios and the Microsoft v. EEE Business cases from the Northern District of California with respect to the issue of whether the unauthorized use of an otherwise legitimate password can constitute circumvention. The court rejected IBM's argument that the two lines of cases were not inconsistent on the ground that, in the 321 Studios and Microsoft v. EEE Business cases, there was no allegation that the parties whose passwords were being used had issued those passwords to a third party. The court found no basis in 321 Studios for such a distinction, and noted that Egilman expressly rejected the distinction. Accordingly, the court concluded that the two lines of cases simply reached contradictory results, and declined to follow the reasoning of the I.M.S. line of cases. It instead followed the 321 Studios and the Microsoft v. EEE Business cases, and held that unauthorized distribution of passwords and user-names avoids and bypasses a technological measure in violation of Sections 1201(a)(2) and 1201(b)(1).[959]

---

955 Id. at *2 & *10-13.

956 Id. at *13.

957 2010 U.S. Dist. LEXIS 33095 (N.D. Cal. Apr. 5, 2010).

958 Id. at *9-10.

959 Id. at *24-25.

> The reasoning of the I.M.S. court – that a password somehow does not fall within [the analogy to the combination of a locked door used in the DeCSS cases], is not well-founded. Rather, a combination to a lock appears to be essentially the same as a password. Nor does the Court find support in the statute itself for drawing a distinction between passwords and other types of code that might be used for decryption. Therefore, the Court rejects Defendants' position. Unauthorized use of a password may constitute circumvention under the DMCA.[960]

(xxi) Navistar v. New Baltimore Garage

In this case, the plaintiff restricted access to its dealer communication network and copyrighted material stored therein through use of passwords. The license agreement for use of the network prohibited sharing with or otherwise distributing passwords to third parties and using a third party's password to gain access to the network. The defendant, a licensee of the plaintiff's network, violated these prohibitions and shared its passwords with a third party who used them to log in and gain unauthorized access to information on the plaintiff's network. The plaintiff claimed that the defendant's provision to the third party with access to the plaintiff's network through the unauthorized use of its passwords constituted circumvention of a technological measure or trafficking in technology designed to circumvent access or copy controls. The court, noting a split in authority on the issue, ruled that unauthorized use of a valid password does not violate the anti-circumvention provisions of the DMCA, and the unauthorized sharing of a valid password does not constitute prohibited trafficking. Accordingly, the court granted the defendant's motion to dismiss the plaintiff's DMCA claim with leave to amend.[961]

(xxii) Dice Corp. v. Bold Technologies

Both the plaintiff and the defendant provided software for companies in the alarm industry. The defendant wrote an extraction program to extract customer data from the plaintiff's software (written in Thoroughbred basic) and convert it into a format that could be read by the defendant's software (written in C++ and Visual Basic). The database files where the customer data was stored by the plaintiff's software were not subject to any access or security features and could be accessed by anyone who had a copy of Thoroughbred basic. No administrative password was required to run queries on the database.[962]

The plaintiff's complaint alleged that encryption of its software constituted a technological measure that effectively controlled access to its products and that the defendant's use of former employees of the plaintiff with knowledge of methods to

---

960 Id. at *26.

961 Navistar, Inc. v. New Baltimore Garage, Inc., 2012 U.S. Dist. LEXIS 134369 at *2-5, 13-15 & 29 (N.D. Ill. Sept. 20, 2012).

962 Dice Corp. v. Bold Technologies, 2012 U.S. Dist. LEXIS 153234 at *2, 11-13, &23 (E.D. Mich. Oct. 25, 2012).

circumvent such encryption permitted the defendant to access the plaintiff's software without permission, in violation of the anti-circumvention provisions of the DMCA. The court granted the defendant summary judgment on this claim, finding that the plaintiff had produced no evidence that the defendant accessed any source code (which one of the plaintiff's employees admitted during discovery was not in fact encrypted) or other copyrighted material of the plaintiff. Rather, the defendant had accessed through its extraction program only customer data that was owned by the user of the plaintiff's software, which data was neither encrypted nor protected against access by any password or other technological measure.[963]

(14) Criminal Prosecutions Under the DMCA

(i) The Sklyarov/Elcomsoft Case

Dmitry Sklyarov, a 27-year-old Russian programmer who worked for a Russian company called Elcomsoft, helped create the Advanced eBook Processor (AEBPR) software, which enabled eBook owners to translate from Adobe's secure eBook format into the more common Portable Document Format (PDF). The software worked only on legitimately purchased eBooks. Sklyarov was arrested at the behest of Adobe Systems, Inc. on July 17, 2001 in Las Vegas after he delivered a lecture at a technical convention, and charged by the Dept. of Justice with criminal violations of the DMCA for distributing a product designed to circumvent copyright protection measures. He was subsequently released on $50,000 bail and restricted to California.[964]

On Dec. 13, 2001, the U.S. government permitted Sklyarov to return home to Russia with his family, essentially dropping prosecution of him in return for his agreement to testify against his employer Elcomsoft in criminal proceedings the government brought against Elcomsoft. In early Feb. 2002, the Electronic Frontier Foundation, joined by The Computing Law and Technology and U.S. Public Policy Committees of the Association for Computing Machinery, the American Association of Law Libraries, the Electronic Privacy Information Center, the Consumer Project on Technology, Computer Professionals for Social Responsibility, and the Music Library Association, filed an amicus brief, along with a brief from 35 law professors, supporting a motion by Elcomsoft to dismiss the case. Elcomsoft's motion and the Electronic Frontier Foundation's brief argued that the DMCA should be found unconstitutional because it impinges on protected speech and stifles technological innovation.

Elcomsoft's motion to dismiss and its challenge on constitutional grounds were rejected by the court in an opinion issued on May 8, 2002.[965] The court concluded that Congress intended to ban all circumvention tools and rejected Elcomsoft's argument that Congress intended to ban only those circumvention devices that would facilitate copyright infringement.[966] The court also specifically concluded that "[n]othing within the express language [of the anti-

---

963 Id. at *43, 45-46 & 48-49.

964 This information is taken from the Free Dmitry Sklyarov! web site at www.freesklyarov.org.

965 United States v. Elcom Ltd., 62 U.S.P.Q.2d 1736 (N.D. Cal. 2002).

966 Id. at 1743.

circumvention provisions] would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use. Instead, all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement."[967] The court rejected the constitutional challenges on a rationale very similar to that of the Second Circuit's opinion in the Corley case,[968] discussed in Section II.G.1(m)(4) above. On Dec. 17, 2002, after a two week trial, a jury acquitted Elcomsoft of criminal charges under the DMCA. The jury foreman told the press that some jurors were concerned about the scope of the DMCA and whether it curtailed the fair use of material simply because it was in electronic format. "Under the eBook formats, you have no rights at all, and the jury had trouble with that concept," the foreman reported.[969]

(ii) Other Criminal Prosecutions Under the DMCA

In Feb. of 2003, the operator of a web site, iSoNews.com, pleaded guilty to criminal DMCA violations for sale of "mod" chips that allowed Microsoft Xbox and Sony Playstation owners to modify their devices so they could use them to play illegally copied games. As part of a plea bargain, the defendant turned over the site's domain name to the control of the U.S. Department of Justice, which then put a notice on the site stating that it had been surrendered to U.S. law enforcement.[970] In Sept. of 2003, a federal jury found a Florida hacker known as "JungleMike" guilty under the DMCA of selling hardware used to illegally receive DirecTV satellite broadcasts. This case marked the first-ever jury conviction under the DMCA. Several other defendants pleaded guilty to DMCA charges in the same operation.[971]

In July of 2005, a Maryland man, one of a group of employees and managers from the three-store Pandora's Cube chain in Maryland, pled guilty and was sentenced to four months in prison for conspiracy to commit felony copyright infringement and for violating the DMCA based on sales by Pandora's Cube of modified Xboxes that let players use pirated console games. Pandora's Cube was also selling modified Xboxes preloaded with pirated games.[972]

In United States v. Whitehead,[973] the Ninth Circuit affirmed the sentence for a man who was convicted of selling over $1 million worth of counterfeit access cards that allowed his customers to access DirecTV's digital satellite feed without paying for it. The court found no

---

[967] Id.

[968] Id. at 1744-57.

[969] Howard Mintz, "Russian Company is Acquitted by S.J. Jury" (Dec. 17, 2002), available as of Dec. 18, 2002 at www.bayarea.com/mld/mercurynews/4763575.htm.

[970] Declan McCullagh, "Feds Confiscate 'Illegal' Domain Names" (Feb. 26, 2003), available as of Feb. 27, 2003 at www.news.com.com/2102-1023-986225.html.

[971] "DirecTV Hacker Convicted Under DMCA," *BNA's Patent, Trademark & Copyright Journal* (Sept. 26, 2003) at 595.

[972] Daniel Terdiman, "Video Game Pirate Headed to Slammer" (July 27, 2005), available as of July 28, 2005 at http://news.com.com/2100-1043_3-5807547.html.

[973] 532 F.3d 991 (9th Cir. 2008).

abuse of discretion in the district court's conclusion that a substantial amount of community service (1000 hours), a hefty restitution order ($50,000) and five years of supervised release were more appropriate than prison, even though the punishment was below that of the federal sentencing guidelines, which called for a range of 41 to 51 months in prison.[974]

(15) Other Uses of the Anti-Circumvention Provisions as a Sword

The RealNetworks and Reimerdes cases suggest how the anti-circumvention provisions of the DMCA might be used as a "sword" in other ways. For example, the manufacturer of a database product that enables users to password protect data files might bring an action under the DMCA against the manufacturer of "cracking" software that enables third parties to bypass or deactivate the password protection on such data files. The manufacturer of the database product might, for example, allege "injury" from the "cracking" software in the form of damage to its reputation as the manufacturer of a "secure" product. Alternatively, if a claim were made against the database product manufacturer by a user alleging injury resulting from the user's data file being "cracked" by a third party, such claim would provide another basis for the database product manufacturer to allege its own injury from the "cracking" software.

Other recent examples of attempts at creative use of the anti-circumvention provisions as a sword are the following:

(i) Lexmark International, Inc. v. Static Control Components, Inc.

Lexmark sold toner cartridges for use with its laser printers. The cartridges were of two types: "regular" cartridges that could be refilled and remanufactured freely by third parties, and "prebate" cartridges that could be used only once, and for which the consumer agreed, in the form of a shrinkwrap agreement placed across the top of every prebate cartridge box, to return the used cartridge to Lexmark for remanufacturing and recycling. Lexmark's printers contained two computer programs – a Printer Engine Program that controlled various printer operations such as paper feed, paper movement, and motor control, and a Toner Loading Program of 37 to 55 bytes, which resided within microchips attached to the toner cartridges and enabled Lexmark printers to approximate the amount of toner remaining in the cartridge.[975]

To protect the Printer Engine Programs and Toner Loading Programs, and to prevent unauthorized toner cartridges from being used with Lexmark's printers, Lexmark's printers used an authentication sequence that ran each time a toner cartridge was inserted into a Lexmark printer, the printer was powered on, or whenever the printer was opened and closed. The authentication sequence required the printer and the microchip on the cartridge to calculate a Message Authentication Code (MAC) using a hashing algorithm, to communicate the MAC from the microchip to the printer, and the printer to compare the MAC it calculated with the MAC it

---

[974] Id. at 992.

[975] Lexmark International, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003).

received from the microchip. If the MAC calculated by the microchip matched that calculated by the printer, the cartridge was authenticated and authorized for use by the printer, which in turn enabled the Printer Engine Program to allow the printer to print and the Toner Loading Program to monitor the toner status of the authenticated cartridge.[976]

The defendant Static Control Components (SCC) manufactured and sold a "SMARTEK" microchip that was used to replace the microchip found in Lexmark's toner cartridges. SCC admitted that it copied verbatim Lexmark's Toner Loading Program into its SMARTEK microchips and that its SMARTEK microchips were designed to circumvent Lexmark's authentication sequence by mimicking the sequence performed by an original microchip on Lexmark's cartridges and the printer.[977] Lexmark sued SCC for violation of the anti-circumvention provisions of the DMCA as well as copyright infringement.

The District Court's Ruling. On a motion for a preliminary injunction, the district court ruled that SCC had violated the anti-circumvention provisions of the DMCA and committed copyright infringement. With respect to the issue of infringement, although SCC admitted copying the Toner Loading Program, SCC argued that the program was not copyrightable because it was a functional "lock-out code" whose exact content was required as part of the authentication sequence. The court rejected this argument, because the binary content of the Toner Loading Program was not used as an input to the hashing algorithm of the authentication sequence, and copying of the Toner Loading Program was therefore not necessary for a valid authentication sequence to occur.[978] The court also rejected SCC's arguments that its copying was a fair use, noting that "[w]here the accused infringer's copying is part of the ordinary operation of the accused product, fair use does not apply,"[979] and that the Toner Loading Program was an uncopyrightable formula or constant, noting that there were a number of ways the Toner Loading Program could have been written to approximate toner level.[980] Because SCC had engaged in verbatim copying of the Toner Loading Program, it had committed copyright infringement. The court also rejected a copyright misuse defense, ruling that "Lexmark's efforts to enforce the rights conferred to it under the DMCA cannot be considered an unlawful act undertaken to stifle competition."[981]

Turning to the DMCA claim, the court found that the SMARTEK microchips violated the anti-circumvention provision of Section 1201(a)(2) in that its primary purpose was to circumvent a technological measure that effectively controlled access to a copyrighted work. The court adopted a plain dictionary meaning of "access" as the "ability to enter, to obtain, or to make use

---

[976] Id. at 952-53.

[977] Id. at 955-56.

[978] Id. at 950, 958-59.

[979] Id. at 960.

[980] Id. at 962.

[981] Id. at 966. The court further noted that an "antitrust claim cannot succeed under an after-market antitrust theory when the accused party has not changed its policy and has been otherwise forthcoming about its policies." Id. at 966 n.3.

of."[982] The court held that the authentication sequence was an effective technological measure restricting access under this definition, because it required application of information and the application of a process to gain access to Lexmark's copyrighted Toner Loading Programs and Printer Engine Programs for use.[983] Accordingly, SCC's manufacture, distribution and sale of its SMARTEK microchips violated the DMCA.[984] The court held that the exemption under Section 1201(f) for circumvention for reverse engineering "solely for the purpose of enabling interoperability of an independently created computer program with other programs" was inapplicable. The court ruled that SCC's SMARTEK microchips could not be considered to contain independently created computer programs, since they were exact copies of Lexmark's Toner Loading Programs and the "SMARTEK microchips serve no legitimate purpose other than to circumvent Lexmark's authentication sequence."[985]

Finally, the court ruled, consistent with the Reimerdes case, that a plaintiff that demonstrates a likelihood of success on the merits of a claim for violation of the anti-circumvention provisions of the DMCA is entitled to a presumption of irreparable injury for purposes of a preliminary injunction. Accordingly, the court entered a preliminary injunction against the distribution of the SMARTEK microchips.[986]

The Sixth Circuit's Ruling. On appeal, the Sixth Circuit reversed and remanded.[987] Turning first to the issue of copyright infringement, the Sixth Circuit found the district court's ruling erroneous with respect to whether the Toner Loading Program constituted a "lock-out code." The court noted generally that "[t]o the extent compatibility requires that a particular code sequence be included in [a] component device to permit its use, the merger and scenes a faire doctrines generally preclude the code sequence from obtaining copyright protection."[988] The court noted that the Toner Loading Program served as input to a checksum operation performed each time the printer was powered on or the printer door was opened and closed for toner cartridge replacement. Specifically, after downloading a copy of the Toner Loading Program to calculate toner levels, the Printer Engine Program ran the checksum calculation using every data byte of the Toner Loading Program as input. The program then compared the result of the calculation with a checksum value located elsewhere on Lexmark's toner cartridge chip. If any single byte of the Toner Loading Program was altered, the checksum value would not match the checksum calculation result.[989]

---

[982] Id. at 967.

[983] Id. at 967-68.

[984] Id. at 969-70.

[985] Id. at 971

[986] Id. at 971, 974.

[987] Lexmark Int'l v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27,422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

[988] Id. at 536.

[989] Id. at 541.

In addition, the Sixth Circuit noted that, at least for purposes of a preliminary injunction, the expert testimony established that it would be "computationally impossible" to modify the checksum value without contextual information that the defendant did not have access to. Accordingly, the checksum operation imposed a compatibility constraint that "justified SCC's copying of the Toner Loading Program."[990] Accordingly, the court concluded that, on the preliminary injunction record, the Toner Loading Program was not copyrightable.[991]

With respect to the DMCA claims, the Sixth Circuit began its analysis by agreeing with the district court and the Reimerdes case that there should be a presumption of irreparable harm arising from demonstration of a likelihood of success on a DMCA claim.[992] The court then turned to separate analyses of Lexmark's anti-circumvention claims with respect to the Printer Engine Program and the Toner Loading Program.

Concerning the Printer Engine Program, the court held that Lexmark's authentication sequences did not "control access" to the Printer Engine program sufficiently to trigger the applicability of the anti-circumvention provisions because anyone could read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence.[993] "The authentication sequence, it is true, may well block one form of 'access' – the ability to … make use of' the Printer Engine Program by preventing the printer from functioning. But it does not block another relevant form of 'access' – the 'ability to [] obtain' a copy of the work or to 'make use of' the literal elements of the program (its code)."[994]

The court rejected Lexmark's argument that several cases had embraced a "to make use of" definition of "access" in applying the DMCA. The court noted that "[i]n the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution."[995] Those cases finding liability based on a technological measure that restricted

---

990 Id. at 542.

991 Id. at 544. Because the court found the Toner Loading Program not to be copyrightable, it noted that it need not decide whether copying of the same was a fair use. Nevertheless, the court noted its disagreement with the district court's fair use analysis, among other reasons because the copying was done for functional reasons. "In copying the Toner Loading Program into each of its SMARTEK chips, SCC was not seeking to exploit or unjustly benefit from any creative energy that Lexmark devoted to writing the program code. As in *Kelly*, SCC's chip uses the Toner Loading Program for a different purpose, one unrelated to copyright protection. Rather than using the Toner Loading Program to calculate toner levels, the SMARTEK chip uses the content of the Toner Loading Program's data bytes as input to the checksum operation and to permit printer functionality. Under these circumstances, it is far from clear that SCC copied the Toner Loading Program for its commercial value *as a copyrighted work* – at least on the preliminary-injunction record we have before us."Id.

992 Id. at 533.

993 Id. at 546.

994 Id. at 547 (quoting from *Merriam-Webster's Collegiate Dictionary*'s definitions of "access").

995 Id. at 548.

"use" of the work were ones in which consumers were restricted from making use of copyrightable expression in the work, such as a video game.[996]

> "The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, 'using' or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional. … Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply."[997]

The Sixth Circuit's holding that, to qualify for DMCA anti-circumvention protection, a technological measure for a computer program must block either the ability to copy the code or to read the literal code, at least where that code does not create any separately protectable expression such as a video game, is potentially very significant. Many computer programs perform only "invisible" functions and do not generate copyrightable expression as output to the user. The Sixth Circuit's ruling that technological measures which merely restrict use of such programs, and do not prohibit copying or reading of the code (such as passwords and handshaking or other authentication sequences), do not qualify for anti-circumvention protection under the DMCA, if adopted by other courts and applied widely, may significantly narrow the scope of protection the DMCA affords to computer programs. Under the Sixth Circuit's definition of "access control," it may be that only those measures that encrypt or otherwise protect a program against copying or the ability to read it will be sufficient to qualify purely "functional" programs for anti-circumvention protection under the DMCA.

Concerning the Toner Loading Program, the court ruled that the defendant's chip did not provide "access" to the Toner Loading Program, but rather replaced the program, and therefore did not circumvent any access control. In addition, to the extent the Toner Loading Program was not copyrightable, it would not constitute a "work protected under [the copyright statute]" to which the DMCA protections would apply.[998]

Finally, the court turned to the interoperability defenses asserted by the defendant. The Sixth Circuit rejected the district court's ruling against the defendant's argument that its microchip constituted a "technological means" that it could make available to others under § 1201(f)(3) solely for the purpose of enabling interoperability of an independently created computer program with other programs. The district court rejected the defense on the ground

---

[996] Id.

[997] Id.

[998] Id. at 549-50.

that the defendant had copied the Toner Loading Program and thus had not created an independently created computer program.[999]

The Sixth Circuit noted that, even if the Toner Loading Program had been copied, the defendant's microchips contained other independently developed computer programs that interoperated with the Printer Engine Program, and those other programs were sufficient to allow the defendant to benefit from the interoperability defense.[1000] The implication of this ruling is that every computer program on a device need not qualify for the interoperability defense in order for the device itself to be able to benefit from the defense.

The court also rejected Lexmark's argument that the independently created program must have existed prior to the reverse engineering – holding that they can be created simultaneously – and its argument that the circumvention means must be necessary or absolutely needed for interoperability – ruling that the statute is silent as to whether there is any necessity requirement at all, but there was necessity in this case because the Toner Loading Program was used in a checksum calculation. Finally, the defendant's copying of the Toner Loading Program did not destroy the interoperability defense (§ 1201(f)(3) conditions its defense on a requirement that the circumvention not violate other "applicable law") because the Sixth Circuit had concluded that the Toner Loading Program was not copyrightable on the preliminary injunction record.[1001] Accordingly, the Sixth Circuit vacated the district court's grant of a preliminary injunction and remanded the case.[1002]

The depth of the court's concern about the policy implications of Lexmark's proposed broad reading for the scope of the anti-circumvention provisions is further illustrated by comments made by two members of the panel in separate opinions. One judge, in a concurring opinion, noted that the main point of the DMCA is "to prohibit the pirating of copyright-protected works such as movies, music and computer programs. If we were to adopt Lexmark's reading of the statute, manufacturers could potentially create monopolies for replacement parts simply by using similar, but more creative, lock-out codes."[1003] He further stated that "Congress did not intend to allow the DMCA to be used offensively in this manner, but rather only sought to reach those who circumvented protective measures 'for the purpose' of pirating works protected by the copyright statute."[1004]

Another judge, in an opinion concurring in part and dissenting in part, stated, "We agree that the DMCA was not intended by Congress to be used to create a monopoly in the secondary

---

[999] Id. at 550.

[1000] Id.

[1001] Id. at 550-51.

[1002] Id. at 551.

[1003] Id. at 552.

[1004] Id.

markets for parts or components of products that consumers have already purchased."[1005] This judge also argued that fair use should be a defense to an anti-circumvention violation, because where fair use applies there would be no "right of a copyright owner" to be infringed by the circumvention.[1006]

By order entered Feb. 23, 2006, the parties stipulated to entry of summary judgment on all DMCA claims and counterclaims in favor of Static Control Components. The order preserved Lexmark's right to appeal the order, as well as the Sixth Circuit's interpretation of the DMCA, after entry of final judgment on all issues in the cases.[1007]

On remand from the Sixth Circuit, the district court found that neither party had submitted new evidence that would undermine the Sixth Circuit's applicability of facts to the law with respect to the issue of the copyrightability of the Toner Loader Program. Accordingly, the Sixth Circuit's decision controlled, and the court ruled that the Toner Loader Program was insufficiently original to be copyrightable.[1008] The court also held that, even if the Toner Loader Program were copyrightable, the defendant's use of it on its chip was a fair use, principally on the ground that the first fair use factor heavily weighed in the defendant's favor "because Lexmark does not even rebut that [the defendant's] purpose for copying the [Toner Loader Program] was solely for the purpose of enabling interoperability between remanufactured Lexmark cartridges and Lexmark printers, *not* for the allegedly-expressive, hypothetically-copyrightable content contained therein."[1009]

(ii) Chamberlain Group, Inc. v. Skylink Technologies, Inc.

In this case, the plaintiff Chamberlain was the manufacturer of a garage door opener (GDO) system which contained a feature known as "rolling code" designed to protect against burglars equipped with "code grabber" devices. A code grabber allows a burglar to capture and record the coded radio frequency (RF) signal sent by the transmitter device to the GDO, which can then be used to open the GDO at a later time to enter the house.[1010] Chamberlain's rolling code feature was designed to defeat code grabbers by changing the expected transmitted RF code each time the GDO was activated. The feature was implemented by two copyrighted computer

---

[1005] Id. at 553. The judge also noted a link in the legislative history between the anti-circumvention prohibitions and the facilitation of copyright infringement. He quoted a House Report to the DMCA stating that Section 1201(b)(1) sought to prohibit "making or selling the technological means to overcome these protections and *thereby facilitate copyright infringement*." Id. at 564 (emphasis by the court) (quoting H.R. Rep. 105-796 (Oct. 8, 1998)).

[1006] 387 F.3d at 562.

[1007] See "Lexmark Stipulates to Judgment on DMCA Claims," *BNA's Patent, Trademark & Copyright Journal* (Mar. 10, 2006) at 506.

[1008] Static Control Components, Inc. v. Lexmark Int'l, Inc., 2007 U.S. Dist. LEXIS 36017, at *36 (E.D. Ky. Apr. 18, 2007).

[1009] Id. at *38.

[1010] Chamberlain Group Inc. v. Skylink Technologies Inc., 292 F. Supp. 2d 1023, 1026-27 (N.D. Ill. 2003).

programs owned by Chamberlain – one in the transmitter of the GDO and the other in the receiver of the GDO that activated the motor to open the door. Each time the transmitter was activated to open the door, the computer program in the transmitter would cause the next rolling code in sequence to be sent to the receiver where it was stored, which code the receiver would require the next time the transmitter was activated, or the door would not open.[1011]

The defendant sold a universal transmitter device that was capable of opening Chamberlain's GDO, although the opener code transmitted by the defendant's door opener was not a rolling code. The defendant's door opener was able to bypass Chamberlain's rolling code feature by mimicking a certain "resynchronization" process of Chamberlain's rolling code software.[1012] Chamberlain characterized that portion of the computer program in the receiver that verified the rolling code as a protective measure that controlled access to Chamberlain's copyrighted computer program in the receiver, and argued that by circumventing the rolling code feature and gaining access to the receiver computer program to open the garage door, the defendant was in violation of the anti-circumvention provisions of Section 1201(a)(2).[1013]

Rulings by the District Court. The district court denied a motion by Chamberlain for summary judgment on the anti-circumvention claim, analyzing a number of defenses raised by the defendant. The first defense was that because the defendant's universal transmitter was capable of operating a number of different GDOs, it was not "primarily" designed to circumvent the access control measure of Chamberlain's GDO. The court rejected this argument, noting that the defendant's transmitter had one particular setting that served only one function – to operate the Chamberlain rolling code GDO. The fact that the transmitter was able to serve more than one purpose was insufficient to deny summary judgment to Chamberlain.[1014]

Next, the defendant argued that Chamberlain's computer programs were not in fact subject to copyright protection. The court ruled that this argument raised a disputed issue of material fact sufficient to deny summary judgment, particularly since Chamberlain had not supplied to the defendant the most recent version of the rolling code software until filing its reply brief (which differed from the version of the software that Chamberlain had registered), and the defendant had therefore not had a sufficient opportunity to review it.[1015]

Finally, the defendant argued that the consumers' use of the defendant's transmitter with Chamberlain's rolling code GDOs was authorized. In particular, Chamberlain argued that a consumer who purchases a Chamberlain GDO owns it and has a right to use it to access his or her own garage. Before the defendant's transmitter was capable of operating the rolling code GDO, the consumer was required to program the transmitter into the GDO. The defendant argued that this fact demonstrated that the consumer had thereby authorized the use of the

---

[1011] Id. at 1027-28.

[1012] Id. at 1029-32.

[1013] Id. at 1028, 1033.

[1014] Id. at 1037-38.

[1015] Id. at 1038.

defendant's transmitter with the GDO software. The defendant further noted that the packaging for Chamberlain's GDO did not include any restrictions on the consumer's ability to buy a replacement transmitter or additional transmitter.[1016] Thus, according to the defendant, "those Chamberlain GDO consumers who purchase a Skylink transmitter are not accessing the GDO without the authority of Chamberlain, but instead, have the tacit permission of Chamberlain to purchase any brand of transmitter that will open their GDO."[1017] The court ruled that these facts, together with the fact that there was a history in the GDO industry of universal transmitters being marketed and sold to allow homeowners an alternative means to access any brand of GDO, raised sufficient disputes of material fact about whether the owner of a Chamberlain rolling code GDO was authorized to use the defendant's universal transmitter to deny summary judgment to Chamberlain.[1018]

Following this opinion, and at the invitation of the court, the defendant moved for summary judgment on Chamberlain's DMCA claim, which the court granted.[1019] Although both parties had agreed for purposes of Chamberlain's original motion for summary judgment that Chamberlain did not place any restrictions on consumers regarding the type of transmitter they had to buy to operate a Chamberlain rolling code GDO, in opposing the defendant's motion for summary judgment, Chamberlain submitted an affidavit of its Vice President asserting that Chamberlain did not authorize the circumvention of its rolling code GDOs, and argued that it had not warned consumers against using unauthorized transmitters because it had no idea that other transmitters could be made to operate its rolling code GDOs.[1020] The court rejected these arguments, finding that the affidavit was conclusory and entitled to little weight, and that Chamberlain's failure to anticipate the defendant's technology did not "refute the fact that homeowners have a reasonable expectation of using the technology now that it is available."[1021]

Finally, Chamberlain argued that even if its customers were authorized to circumvent its security measures, that had no bearing on whether sellers had similar authorization. The court found this argument ignored the fact that (1) there was a history in the GDO industry of marketing and selling universal transmitters; (2) Chamberlain had not placed any restrictions on the use of competing transmitters to access its rolling code GDOs; and (3) in order for the

---

[1016] Id. at 1039.

[1017] Id.

[1018] Id. at 1040. An amicus brief submitted by the Computer and Communications Industry Association (CCIA) argued that the court should deny summary judgment because the defendant's activities fell within Section 1201(f) of the DMCA, which CCIA argued permits circumvention of a protective measure for the purpose of achieving interoperability. The court noted that, although it was not reaching this issue, the defendant might perhaps be entitled to summary judgment on that basis. Id.

[1019] Chamberlain Group, Inc. v. Skylink Technologies, Inc., 292 F. Supp. 2d 1040 (N.D. Ill. 2003). As a preliminary matter, Chamberlain asserted that the defendant bore the burden of proof to show that it was authorized to circumvent – not access – Chamberlain's software as an affirmative defense. The court disagreed, ruling that it was clearly Chamberlain's burden to demonstrate that the defendant circumvented a technological measure without the authority of the copyright owner. Id. at 1044.

[1020] Id.

[1021] Id.

defendant's transmitter to activate the Chamberlain garage door, the homeowner herself had to choose to store the defendant's transmitter signal into the Chamberlain GDO's memory, thereby demonstrating the homeowner's willingness to bypass Chamberlain's system and its protections.[1022]

Accordingly, the court granted the defendant's motion for partial summary judgment with respect to Chamberlain's DMCA claim.[1023] Since so much of the district court's opinion emphasized the fact that Chamberlain had not placed restrictions on the type of transmitters customers could use to operate Chamberlain's GDOs, one must wonder whether the court would have ruled differently had Chamberlain made clear to customers of its GDO products at the time of purchase that they were not authorized to use any transmitters to access the software in their GDOs other than Chamberlain's transmitters. If so, then under the district court's rationale, it seems that DMCA claims of the type Chamberlain made in this case could easily be strengthened by copyright holders in the future by making express statements of authorization with respect to use of their products. The Federal Circuit, in its decision on appeal, expressly declined to reach this issue.[1024]

The Federal Circuit's Decision. On appeal, the Federal Circuit affirmed in a detailed opinion that examined the legislative history and purpose of the anti-circumvention provisions of the DMCA, and placed some significant boundaries around the scope of those provisions.[1025] The Federal Circuit began its analysis by ruling that the plaintiff has the burden under an anti-circumvention claim to prove that the defendant's access to its copyrighted work was not authorized. The court derived this holding from the distinction between a copyright – which is a property right – and the anti-circumvention provisions – which do not establish a new property right, but rather only a new cause of action for liability. Under a copyright (a property right), the plaintiff need only establish copying, and the burden then shifts to the defendant to prove a defense. By contrast, under the anti-circumvention provisions, the language of the statute defines the cause of action in terms of a circumvention or trafficking without authority of the copyright owner. The plaintiff therefore has the burden to prove that the defendant's access was unauthorized.[1026]

In a very significant ruling, the Federal Circuit held that the anti-circumvention provisions of Section 1201 do not apply to all forms of circumvention to gain access to a work, but rather only to circumventions that accomplish "forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners"[1027] –

[1022] Id. at 1946.

[1023] Id.

[1024] The Federal Circuit did, however, make some statements suggesting that such restrictions might constitute copyright misuse, as discussed below.

[1025] The Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004)), cert. denied, 161 L. Ed. 2d 481 (2005).

[1026] Id. at 1193.

[1027] Id. at 1202.

in other words, circumventions that facilitate some form of copyright infringement.[1028] Conversely, "defendants whose circumvention devices do not facilitate infringement are not subject to § 1201 liability."[1029]

The court reached this conclusion based on three rationales. First, the court noted that in the statutory language itself, "virtually every clause of § 1201 that mentions 'access' links 'access' to 'protection.'"[1030] Second, the court found that every decision cited by the plaintiff finding anti-circumvention liability involved a circumvention that facilitated or was coupled with copyright infringement. In the Reimerdes case, the DeCSS program allowed the user to circumvent the CSS protective system and to view or to copy a motion picture from a DVD, whether or not the user had a DVD player with the licensed technology. In the Lexmark case, the court ruled that the defendant's conduct in copying the Toner Loading Program constituted copyright infringement. In the Gamemasters case, the defendant conceded that its product made temporary modifications to the plaintiff's copyrighted computer program. In the Real Networks case, the defendant's product allegedly disabled Real Networks' copy switch, which defeated the copyright owner's ability to control copying upon streaming of the work.[1031] "In short, the access alleged in all [these] cases was intertwined with a protected right."[1032]

Third, the court believed that a broad reading of the anti-circumvention provisions to prohibit all forms of unauthorized access, whether or not protected copyright rights were thereby implicated, as urged by Chamberlain, would risk too much potential harm to competition. "Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would allow virtually any company to attempt to leverage its sales into aftermarket monopolies – a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit."[1033]

The court noted that such a broad reading would also contradict other statutory provisions of the DMCA. In particular, Section 1201(c)(1) provides that nothing in Section 1201 shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use. The court noted that a reading of Section 1201 that prohibited access without regard to the rest of the copyright statute would clearly affect rights and limitations, if not remedies and defenses,[1034]

[1028] Id. at 1195, 1203.

[1029] Id. at 1195.

[1030] Id. at 1197.

[1031] Id. at 1198-99 (citations omitted).

[1032] Id. at 1199.

[1033] Id. at 1201 (citations omitted).

[1034] Id. at 1200.

and might also be tantamount to "ignoring the explicit immunization of interoperability from anticircumvention liability under § 1201(f)."[1035]

The court's statements might imply that circumvention for fair uses is privileged. Indeed, the court stated, "Chamberlain's proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would therefore allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work – or even selected copies of that copyrighted work. Again, this implication contradicts § 1201(c)(1) directly."[1036] Despite these pregnant statements, however, the court stated in a footnote, "We leave open the question as to when § 107 might serve as an affirmative defense to a prima facie violation of § 1201. For the moment we note only that though the traditional fair use doctrine of § 107 remains unchanged as a defense to copyright infringement under § 1201(c)(1), circumvention is not infringement."[1037]

Turning to Chamberlain's specific claims under Section 1201(a)(2), the court summarized the requirements for liability as follows:

> A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[1038]

The court ruled that Chamberlain had failed to satisfy both the fourth and fifth elements of the test. With respect to the fifth element, Chamberlain had neither alleged copyright infringement nor explained how the access provided by the defendant's transmitter facilitated third party infringement of any of its copyright rights. Instead, the defendant's transmitter merely enabled the end user to make legitimate use of the computer program in the GDO.[1039]

Nor had Chamberlain established the fourth element. The record established that Chamberlain had placed no explicit restrictions on the types of transmitter that the homeowner

---

[1035] Id. Although amicus Computer and Communications Industry Association urged the court to consider the import of Section 1201(f) on the case, the court did not reach the issue since it held there had been no anti-circumvention violation by the defendant in the first place under its reading of the scope of the DMCA. Id. at 1191 n.8.

[1036] Id. at 1202.

[1037] Id. at 1200 n.14.

[1038] Id. at 1203.

[1039] Id. at 1198, 1204.

could use with its system at the time of purchase.[1040] "Copyright law itself authorizes the public to make certain uses of copyrighted materials. Consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software. What the law authorizes, Chamberlain cannot revoke."[1041] Although this statement suggests that a plaintiff could not even use contractual prohibitions to eliminate authorization to circumvent controls to gain access to the software in a way that did not facilitate infringement, the court backed away from any such absolute principle in a footnote: "It is not clear whether a consumer who circumvents a technological measure controlling access to a technological measure controlling access to a copyrighted work in a manner that enables uses permitted under the Copyright Act but prohibited by contract can be subject to liability under the DMCA. Because Chamberlain did not attempt to limit its customers' use of its product by contract, however, we do not reach that issue."[1042]

In conclusion, then, the court held, "The Copyright Act authorized Chamberlain's customers to use the copy of Chamberlain's copyrighted software embedded in the GDOs that they purchased. Chamberlain's customers are therefore immune from § 1201(a)(1) circumvention liability. In the absence of allegations of either copyright infringement or § 1201(a)(1) circumvention, Skylink cannot be liable for § 1201(a)(2) trafficking."[1043] The court therefore affirmed the district court's grant of summary judgment in favor of Skylink.[1044]

(iii) In re Certain Universal Transmitters for Garage Door Openers

In addition to its lawsuit against Skylink, Chamberlain also filed an action in the International Trade Commission to bar the importation of Skylink's GDOs. That investigation established a second ground beyond that of the district court's ruling as to why Skylink had not committed a violation of the DMCA. Specifically, in an Initial Determination concerning temporary relief in the investigation that preceded the district court's ruling, an administrative law judge denied temporary relief on the ground that Skylink's transmitters did not violate the DMCA because they "do not circumvent Chamberlain's copyrighted rolling code software program, but instead send fixed identification code signals to Chamberlain's GDOs that fall outside of the copyrighted software. … The fact that [Skylink's] transmitters send a fixed identification code that does not circumvent Chamberlain's copyrighted software program removes those products entirely from the purview of the DMCA, regardless of whether Chamberlain warns its customers and Skylink that non-rolling code transmitters are unauthorized."[1045]

[1040] Id. at 1183.

[1041] Id. at 1202.

[1042] Id. at 1202 n.17.

[1043] Id. at 1204.

[1044] Id.

[1045] In re Certain Universal Transmitters for Garage Door Openers, 70 U.S.P.Q.2d 1906, 1909 (I.T.C. 2004).

After the district court's ruling, Skylink moved to dismiss the ITC investigation on the ground that Chamberlain's claim was barred under res judicata by that ruling. Chamberlain opposed the dismissal on the ground that there were new facts not before the district court – namely, that Chamberlain had since changed its GDO users' manuals to expressly warn customers that use of non-rolling code transmitters would circumvent Chamberlain's rolling code security measure, and to make clear that customers were not authorized to access Chamberlain's operating software using non-rolling code transmitters.[1046] The administrative law judge ruled that this fact was insufficient to avoid res judicata, because the fact could have been asserted before the district court, since the administrative ruling on the request for temporary relief issued before the district court acted.[1047] In addition, the administrative law judge ruled that Chamberlain's new owners' manuals "impose no enforceable restrictions on consumers even if they do 'warn' them that non-rolling code transmitters are 'unauthorized.' There are no negative consequences for a consumer who ignores the statement in Chamberlain's new manuals."[1048] Accordingly, the administrative law judge determined that the investigation should be terminated in its entirety and certified that determination to the Commission.[1049]

(iv) Storage Technology Corporation v. Custom Hardware Engineering & Consulting

In this case, the plaintiff Storage Technology Corporation ("StorageTek") sold systems for storing and retrieving very large amounts of computer data. StorageTek also serviced its customers' installations by means of diagnostic software, called the "Maintenance Code," that it used to identify malfunctions and problems in its customers' storage systems. In order to protect its service market, StorageTek restricted access to the Maintenance Code with a proprietary algorithm called GetKey.[1050]

When activated, the Maintenance Code ran a series of diagnostic tests and provided information concerning the nature of existing or potential problems. It was programmed to be set at different levels between 0 and 9. At the 0 level (the usual setting), the Maintenance Code was disabled. Above 0 the Maintenance Code activated specific diagnostic functions at different levels. To enable the Maintenance Code for a particular system, a technician was required to contact StorageTek's technical support staff, provide the serial number of the equipment being serviced and identify the desired level of the Maintenance Code. The technician would then be given a GetKey password specific to the request that the technician was required to enter in order to reset the maintenance level. During the process of accessing the Maintenance Code and

---

[1046] Id. at 1907-08.

[1047] Id. at 1909-10.

[1048] Id. at 1910.

[1049] Id.

[1050] Storage Technology Corp. v. Custom Hardware Engineering & Consulting, 2004 U.S. Dist. LEXIS 12391 (D. Mass. July 2, 2004) at *3-4.

changing the level, a complete copy of the code was made in the RAM memory of the system.[1051]

The defendants competed with StorageTek for servicing StorageTek systems. They figured out how to circumvent the GetKey algorithm to gain access to the Maintenance Code and to reset its maintenance level in order to run diagnostics that would generate information needed to service a particular system. StorageTek sued for both copyright infringement and violation of the anti-circumvention provisions.[1052]

The district court held that the defendants had infringed StorageTek's copyright in the Maintenance Code by virtue of the copy thereof made in RAM each time the GetKey process was circumvented and the maintenance level reset.[1053] The court held that such copying was not permitted under Section 117(c) of the copyright statute, which provides that it is not an infringement for the owner or lessee of a machine to authorize the making of a copy of a computer program if the program is copied solely by turning on the machine for the purpose only of maintenance and repair and the copy is used in no other manner and is destroyed immediately after the maintenance and repair is completed. The court ruled that Section 117(c) was not available because, although the defendants copied the Maintenance Code by turning on the machine, they did not do so just for repair, but also for the express purpose of circumventing StorageTek's security measures, modifying the maintenance level, and intercepting the diagnostic messages, and they did not destroy the copies they made immediately after completion of repairs.[1054]

The court also found a violation of the anti-circumvention provisions of the DMCA, ruling that GetKey was unquestionably a qualifying access control measure and there was no question that the defendants bypassed GetKey. The court also rejected the defendants' reliance on Section 1201(f), because that defense exempts circumvention only if it does not constitute infringement, and the defendants' bypassing of GetKey resulted in an infringing copy of the program being made in RAM.[1055] Accordingly, the court issued a preliminary injunction against the defendants.

On appeal, the Federal Circuit reversed, principally on the ground that the district court's analysis of Section 117(c) was incorrect. The court found that the district court had erred by focusing on the term "repair" in Section 117(c), while ignoring the term "maintenance," which the court noted from the legislative history was meant to encompass monitoring systems for problems, not simply fixing a single, isolated malfunction.[1056] The defendant had created

---

[1051] Id. at *7-8.

[1052] Id. at *9-11.

[1053] Id. at *11-12.

[1054] Id. at *12-13.

[1055] Id. at 14-15.

[1056] Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1312 (Fed. Cir. 2005), reh'g denied, 431 F.3d 1374 (Fed. Cir. 2005).

software, known as the Library Event Manager (LEM) and the Enhanced Library Event Manager (ELEM) to intercept and interpret fault symptom codes produced by the plaintiff's Maintenance Code.[1057] The plaintiff's expert testified that a copy of the Maintenance Code remained in RAM on an ongoing basis as the system operated with the LEM and ELEM attached. Because that description did not comport with the notion of "repair," the district court had ruled Section 117(c) inapplicable. However, in describing the defendants' process, the expert noted that the LEM and ELEM stayed in place so that when problems occurred, the defendants could detect and fix the malfunction. The Federal Circuit ruled that this ongoing presence to detect and repair malfunctions fell within the definition of "maintenance" in Section 117(c). Moreover, when the defendants' maintenance contract was over, the storage library was rebooted, which destroyed the Maintenance Code. The court noted that the protection of Section 117 does not cease simply by virtue of the passage of time, but rather ceases only when maintenance ends.[1058]

With respect to whether the Maintenance Code was necessary for the machine to be activated, the Federal Circuit relied heavily on the fact that both parties agreed the Maintenance Code was "so entangled with the functional code that the entire code must be loaded into RAM for the machine to function at all."[1059] The fact that the Maintenance Code had other functions, such as diagnosing malfunctions in the equipment, was irrelevant. Accordingly, the defendants were likely to prevail on their argument that Section 117(c) protected their act of copying of the plaintiff's Maintenance Code into RAM.[1060]

Turning to the anti-circumvention claim based on the defendants' circumvention of the GetKey protocol, the court cited its earlier opinion in the Chamberlain case for the proposition that a "copyright owner alleging a violation of section 1201(a) … must prove that the circumvention of the technological measure either 'infringes or facilitates infringing a right protected by the Copyright Act.'"[1061] Thus, to the extent that the defendants' activities did not constitute copyright infringement or facilitate copyright infringement, the plaintiff was foreclosed from maintaining an action under the DMCA.[1062] Citing the Lexmark and RealNetworks v. Streambox cases, the court observed that "courts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by

---

[1057] Id. at 1310.

[1058] Id. at 1313.

[1059] Id. at 1314.

[1060] Id. In the alternative, the court ruled that the defendants' copying of the software into RAM was within the software license rights of their customers because the defendants were acting as their customers' agents in turning on the machines. Id. at 1315. "Because the whole purpose of the license is to allow the tape library owners to activate their machines without being liable for copyright infringement, such activity by the licensee and its agents is implicitly authorized by the license agreement unless the agreement explicitly prohibits third parties from powering up the machines." Id. at 1317.

[1061] Id. at 1318 (quoting Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004)).

[1062] Storage Technology, 421 F.3d at 1318.

the Copyright Act. … To the extent that StorageTek's rights under copyright law are not at risk, the DMCA does not create a new source of liability."[1063]

Even if the plaintiff were able to prove that the automatic copying of the Maintenance Code into RAM constituted copyright infringement, it would still have to show that the LEM or ELEM (which bypassed GetKey) facilitated that infringement. With respect to that issue, the court noted the problem that the copying of the Maintenance Code into RAM took place regardless of whether the LEM or ELEM was used. Thus, there was no nexus between any possible infringement and the use of the LEM and ELEM circumvention devices. Rather, the circumvention of GetKey only allowed the defendants to *use* portions of the copyrighted software that the plaintiff wished to restrict technologically, but that had already been loaded into RAM. "The activation of the maintenance code may violate StorageTek's contractual rights vis-à-vis its customers, but those rights are not the rights protected by copyright law. There is simply not a sufficient nexus between the rights protected by copyright law and the circumvention of the GetKey system."[1064] Accordingly, it was unlikely that the plaintiff would prevail on its anti-circumvention claim.[1065] The court therefore vacated the preliminary injunction and remanded for further proceedings.[1066]

Two significant aspects of the Storage Tech case are worth noting:

– First, the court read the Section 117(c) rights very broadly. Section 117(c) was clearly designed to absolve maintenance providers from copyright liability based merely on the making of a copy of a computer program by virtue of its getting loaded into RAM upon starting a computer for maintenance. However, the Federal Circuit went further, and ruled that the defendants were entitled to *use*, in aid of rendering maintenance, any software that got loaded into RAM upon activation of the machine. Such a result seems in tension with Section 117(c)(2), which provides that, "with respect to any computer program or part thereof that is not necessary for the machine to be activated, such program or part thereof is not accessed or used other than to make such new copy by virtue of the activation of the machine." The reference to "part thereof" seems to contemplate that some code might get loaded upon machine activation, but yet not be necessary for the machine to be activated (in the way, for example, that operating system software is necessary for a machine to be activated). In that event, Section 117(c)(1) absolves the maintenance provider from liability for the making of the copy of such code upon machine activation, but Section 117(c)(2) would seem to prevent the maintenance provider from accessing or *using* such code "other than to make such new copy by virtue of the activation of the machine."

Notwithstanding this, the Federal Circuit's decision gave the maintenance provider the right to access and use the Maintenance Code, just because it was loaded upon activation. The court did so on the articulated basis that the Maintenance Code was "so entangled with the

---

[1063] Id.

[1064] Id. at 1319.

[1065] Id.

[1066] Id. at 1321.

functional code that the entire code must be loaded into RAM for the machine to function at all."[1067] However, this factual assertion seems belied by the fact that, as noted by the district court, the default setting for the Maintenance Code was level 0 (disabled), and it was designed to require intervention by Storage Tech engineers through the GetKey process to activate it to higher levels. Thus, although the Maintenance Code was loaded upon machine activation, it would not seem necessary for the machine to activate (function), because it was by default set to be disabled.

– Second, the court's interpretation of the anti-circumvention provisions gives them a narrower scope than the literal language of the copyright statute seems to read. Specifically, the court ruled that those provisions do not create a new source of liability beyond copyright infringement. If a circumvention does not lead to a copyright infringement, the circumvention is not illegal. In other words, the act of circumvention is not a *malum in se*.[1068] This holding, whatever merit it might be argued to have as a policy matter, seems contrary to the literal language of Section 1201(a)(1)(A), which states "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." The Federal Circuit's decision seems to add a clause at the end of this provision reading "and which circumvention results in copyright infringement." As discussed in Section II.G.1(n)(1) above, the separate opinions of two of the judges in the Lexmark case expressed similar views about what the proper scope of the anti-circumvention prohibitions should be interpreted to be.

On remand, StorageTek asserted an additional anti-circumvention claim against the defendants, based on the defendants alleged circumvention of GetKey in order to access and copy StorageTek's Run Time Diagnostics (RTD) code, which diagnosed troubles in the hardware. Unlike the rest of the Maintenance Code, the RTD code was not automatically loaded upon power-up, but instead was loaded only when utilized.[1069] The court rejected this claim on the ground that GetKey did not effectively protect or control access to the RTD code. The RTD code was contained on either the hard drive of the LMU or on floppy disks that StorageTek sometimes shipped with its products. Accordingly, any customer who owned a StorageTek system could access and copy the RTD code, regardless of the existence of GetKey protections. The court therefore concluded that GetKey did not effectively control access to the RTD code, and the court granted the defendants summary judgment on the anti-circumvention claim related to the RTD code.[1070]

[1067] Id. at 1314.

[1068] Latin for "wrong in itself."

[1069] Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Ltd., 2006 U.S. Dist. LEXIS 43690 at *15, 22 (D. Mass. June 28, 2006).

[1070] Id. at *25-26.

(b) Integrity of Copyright Management Information

(1) Definition of CMI

The DMCA contains provisions directed to maintaining the integrity of "copyright management information" (CMI), which Section 1202(c) of the DCMA defines to include the following items of information "conveyed" in connection with copies of a work or the performance or display of a work, including in digital form (but specifically excluding any personally identifying information about a user of a work):

– the title and other information identifying the work, including the information set forth on a copyright notice;

– the name and other identifying information about the author or the copyright owner of the work;

– the name and other identifying information about a performer, writer, or director associated with a work, other than a work performed publicly by radio and television broadcast stations;

– terms and conditions for use of the work;

– identifying numbers or symbols referring to such information or links to such information; and

– any other information that the Register of Copyrights may prescribe by regulation.

The statement of Rep. Coble accompanying the original introduction of the provision in S. 2037 corresponding to Section 1202 noted that the term "conveyed" was "used in its broadest sense and is not meant to require any type of transfer, physical or otherwise, of the information. It merely requires that the information be accessible in conjunction with, or appear with, the work being accessed." Under this definition, CMI could include information that is contained in a link whose address is conveyed with the copyrighted work. Such information could well be a shrinkwrap license, as such license would convey the "terms and conditions for use of the work," which is one of the express components of the definition of CMI.

(i) Cases Requiring CMI to be Part of a Technological System or Process

a. The IQ Group, Ltd. v. Wiesner Publishing, LLC

The case of The IQ Group, Ltd. v. Wiesner Publishing, LLC[1071] is one of the most thorough opinions to consider the scope of the definition of CMI, although it and the cases that follow its reasoning construe what qualifies as protectable CMI under the DMCA quite a bit

[1071] 409 F. Supp. 2d 587 (D.N.J. 2006).

more narrowly than the cases discussed in Section II.G.1(b)(1)(ii) below that reject its reasoning or result. There is thus a significant split in authority over the issue of what qualifies as protectable CMI.

The plaintiff IQ Group and the defendant Wiesner Publishing were business competitors who distributed ads by email to insurance agents on behalf of insurance companies. IQ distributed ads for two insurance companies that contained IQ's graphic logo. The logo functioned as a hyperlink in the ads such that, when clicked, it directed the user to a page of IQ's website which IQ claimed contained copyright notices. After IQ had distributed the ads for the two insurance companies, the companies hired Wiesner to distribute the same ads via email. Wiesner removed IQ's logo and hyperlink, added new information so that responses to the ads would go to the insurance companies, and then copied and distributed the ads by email. IQ sued the two insurance companies and Wiesner for, among other things, violation of the CMI provisions of the DMCA based on the removal of the logo from the ads. The parties cross moved for summary judgment.[1072]

The court ruled that the IQ's claim that the logo and hyperlink were within the scope of Section 1202 failed for two reasons. First, as to the logo, IQ's position impermissibly blurred the distinction between trademark law and copyright law. Second, properly interpreted, Section 1202 did not apply to either the logo or the hyperlink.[1073]

With respect to the first reason, the court ruled that protecting a logo, functioning as a service mark, under the CMI provisions would turn the DMCA "into a species of mutant trademark/copyright law, blurring the boundaries between the law of trademarks and that of copyright."[1074] Specifically, the court was concerned that if every removal or alteration of a logo attached to a copy of a work gave rise to a cause of action under the DMCA, the DMCA would become an extension of, and overlap with, trademark law. There was no evidence that Congress intended such an extreme outcome in enacting the DMCA.[1075]

The court then turned to the proper interpretation of the definition of CMI, noting that the interpretation of that definition was a matter of first impression. Although the court noted that the definition, read literally, seemed to apply wherever any author had affixed anything that might refer to his or her name, examination of the legislative history and other extrinsic sources convinced the court that the statute should be subject to a narrowing interpretation.[1076] Citing an article by law professor Julie Cohen[1077] and the legislative history of the WIPO Copyright Treaty that led to enactment of the DMCA to implement it, the court concluded that protected CMI should be limited to components of automated copyright protection or management systems.

[1072] Id. at 589-90.

[1073] Id. at 591-92.

[1074] Id. at 592.

[1075] Id.

[1076] Id. at 593.

[1077] Julie E. Cohen, "Copyright and The Jurisprudence of Self-Help," 13 Berkeley Tech. L.J. 1089 (1998).

Specifically, WIPO was intended to protect CMI as part of a double protection scheme for technical measures – to allow the protection of copyrighted works by the application of technical measures restricting access thereto and protecting copyright rights therein, and to protect the technical measures themselves against those who would crack them by other technologies or machines. Thus, the court found that in the framework of the WIPO treaties, technical measures such as CMI were viewed as components of automated copyright protection systems.[1078] This same understanding of CMI was embodied in the White Paper of the Information Infrastructure Task Force released in September of 1995, which presented a draft of Sections 1201 and 1202, and noted that systems for managing rights in works were being contemplated in the development of the national information infrastructure to serve the functions of tracking and monitoring uses of copyrighted works as well as licensing of rights and indicating attribution, creation and ownership interests. To implement these rights management functions, the White Paper noted that information would likely be included in an "electronic envelope" containing a digital version of a work to provide information regarding authorship, copyright ownership, date of creation or last modification, and terms and conditions of authorized uses.[1079]

From this the court concluded the White Paper demonstrated that the Working Group on Intellectual Property Rights, in drafting Section 1202, "understood this section to protect the integrity of automated copyright management systems functioning within a computer network environment," and that this interpretation was confirmed by contemporaneous commentary on the draft provision.[1080] Sections 1201 and 1202 underwent no significant revision between drafting in 1995 and enactment in 1998.[1081]

The court noted that this interpretation of Section 1202 made sense because it fit Section 1201 with Section 1202, and with chapter 12 of the DMCA as a whole. "Chapter 12, as a whole, appears to protect automated systems which protect and manage copyrights. The systems themselves are protected by § 1201 and the copyright information used in the functioning of the systems is protect in § 1202. … Section 1202 operates to protect copyright by protecting a key component of some of these technological measures. It should not be construed to cover copyright management performed by people, which is covered by the Copyright Act, as it preceded the DMCA; it should be construed to protect copyright management performed by the technological measures of automated systems."[1082]

In sum, the court ruled that "[t]o come within § 1202, the information removed must function as a component of an automated copyright protection or management system."[1083] The

---

[1078] 409 F. Supp. 2d at 593-95.

[1079] Id. at 594-95.

[1080] Id. at 595.

[1081] Id. Although the Senate Report stated that CMI need not be in digital form, the court noted that the Senate Report gave only a vague idea as to what CMI was intended to be, and there was nothing in it to suggest that the Senate Committee understood Section 1202 differently from the Working Group. Id. at 596.

[1082] Id. at 597.

[1083] Id.

court found no evidence that IQ intended that an automated system would use its logo or hyperlink to manage copyrights, nor that the logo or hyperlink performed such a function. Accordingly, the logo and hyperlink did not fall within the definition of CMI, and the court granted summary judgment for Wiesner on IQ's CMI claim.[1084]

b. Textile Secrets Int'l, Inc. v. Ya-Ya Brand Inc.

In this case, the plaintiff alleged that fabrics sold by the defendants infringed the plaintiff's copyright in its "FEATHERS" fabric design. The plaintiff also alleged that the defendants had violated the CMI provisions of the DMCA by removing the plaintiff's name and the copyright symbol from the selvage (the edge or border of fabric that is intended to be cut off and discarded) of its fabrics, as well as an attached tag stating that the design was a registered work of the plaintiff, and then making copies of the fabrics. The central issue in the case was whether the information on the selvage and the tag constituted CMI.[1085]

The defendants urged that, in view of the legislative history of the DMCA, the CMI provisions should be construed to apply only to transactions on the Internet or in the electronic marketplace. The plaintiff argued that a plain reading of the CMI provisions should lead to a conclusion that CMI can be protected on all types of works, in both digital and non-digital form.[1086] After an extensive survey of the history of the CMI provisions of the DMCA, including the White Paper of the National Information Infrastructure Task Force, congressional reports, and the WIPO treaties, the court ruled that the information on the selvage and the tag did not constitute CMI within the purview of the DMCA.[1087] The court found the IQ Group decision, discussed above, influential to its decision, although it chose not to define the scope of CMI as definitively as that case did.[1088] Nevertheless, the court was persuaded by that case that Section 1202 should be "subject to a narrowing interpretation" as follows:

> While the Court does not attempt in this decision to define the precise contours of the applicability of § 1202, the Court nevertheless cannot find that the provision was intended to apply to circumstances that have no relation to the Internet, electronic commerce, automated copyright protections or management systems, public registers, or other technological measures or processes as contemplated in

---

[1084] Id. at 597-98.

[1085] Textile Secrets Int'l, Inc. v. Ya-Ya Brand Inc., 524 F. Supp. 2d 1184, 1192-93 (C.D. Cal. 2007).

[1086] Id. at 1193-94.

[1087] Id. at 1194-99.

[1088] Id. at 1202 n.17 ("The Court is not attempting to define or specify what types of non-digital works are covered. Rather, under the particular facts of this case – that is, in the absence of any facts demonstrating that a technological process was utilized in connection with either applying the copyright information to the fabric or in removing such information or in subsequently distributing the design – the Court is not persuaded that the copyright information on the FEATHERS fabric warrants coverage by the DMCA.") (emphasis in original) & 1203 n.18 ("Although the Court is persuaded to some extent by the reasoning set forth in the IQ Group decision, the Court does not find it necessary to define the scope of § 1202 as definitively as the IQ Group court did (i.e., that the provision applies only to copyright management information that functions 'as a component of an automated copyright protection or management system').") (quoting IQ Group, 409 F. Supp. 2d at 598).

> the DMCA as a whole. In other words, although the parties do not dispute that the FEATHERS fabric contained [the plaintiff's] copyright information, there are no facts showing that any technological process as contemplated in the DMCA was utilized by plaintiff in placing the copyright information onto the FEATHERS fabric, or that defendants employed any technological process in either their removal of the copyright information from the design or in their alleged distribution of the design. In short, the Court finds that, in light of the legislative intent behind the DMCA to facilitate electronic and Internet commerce, the facts of this case do not trigger § 1202.[1089]

c. Jacobsen v. Katzer

In this case, the plaintiff was a leading member of the Java Model Railroad Interface (JMRI) Project, an online, open source community that developed model train software and distributed it under the open source Artistic License. The defendants also developed software for model railroad enthusiasts. The plaintiff brought a claim under Section 1201(b), alleging that the JMRI Project Decoder Definition Files distributed by the JMRI and used by the defendants constituted CMI and that by removing some of the information in the files and making copies of the files, the defendants had violated Section 1201(b). The defendants brought a motion to dismiss the claim.[1090]

The information in the files that the plaintiff claimed constituted CMI were the author's name, a title, a reference to the license and where to find the license, a copyright notice, and the copyright owner. The plaintiff alleged that he used a software script to automate adding copyright notices and information regarding the license and uploaded the files on the Internet through Source-Forge.net, and that the defendants downloaded the files and removed the names of the authors and copyright holder, title, reference to the license, where to find the license and the copyright notices, and instead, renamed the files and referred to their own copyright notice and named themselves as author and copyright owner. The court denied the motion to dismiss. It cited the IQ Group case's holding that the statute should be construed to protect CMI performed by the technology measures of automated systems, but found that the complaint alleged there had been some technological process engaged to protect the information inserted into the files. Thus, absent further discovery, the court found it inappropriate to dismiss the CMI claim.[1091]

In a subsequent opinion ruling on cross motions for summary judgement, the court, citing the IQ Group and McClatchey decisions, ruled that the DMCA protects only "CMI performed by the technological measures of automated systems."[1092] The court found, based on the allegations in the complaint, that there had been some technological process employed to protect the attribution information in the Decoder Definition Text Files. Further, there was no dispute that

---

[1089] Id. at 1201-02.

[1090] Jacobsen v. Katzer, 609 F. Supp. 2d 925, 928 & 934 (N.D. Cal. 2009).

[1091] Id. at 934.

[1092] Jacobsen v. Katzer, 2009 U.S. Dist. LEXIS 115204 at *20 (N.D. Cal. Dec. 10, 2009).

the defendants had employed a tool to translate the JMRI files to a format for their own use without copying this attribution information. Accordingly, the court granted summary judgment to the plaintiff that the attribution information constituted CMI protected by the DMCA. However because there remained disputed issues of fact regarding the defendants' knowledge and intent, the court denied the plaintiff's motion for summary judgment on liability under the CMI provisions of the DMCA.[1093]

d. Silver v. Lavadeira

The plaintiff published certain news reports on her web site and placed her name within the reports. The plaintiff alleged that the defendant copied certain information from her reports and violated Section 1202 by omitting her name from the copied material. The court ruled, based on IQ Group, that CMI is limited to components of technological measures functioning as automated systems, and that the plaintiff's name did not constitute CMI because she had not alleged that an automated technological system was responsible for the inclusion of her name in the news reports.[1094]

(ii) Cases Not Requiring CMI to be Part of a Technological System or Process

a. McClatchey v. The Associated Press

The court in McClatchey v. The Associated Press[1095] rejected the ruling of the IQ Group court that CMI must function as a component of an automated copyright protection management system in order to be protected by Section 1202 of the DMCA. In the McClatchey case, the plaintiff was the owner of a photograph she took on the morning of Sept. 11, 2001 as she observed United flight 93 crash into a field near her house. The photograph, which the plaintiff titled "End of Serenity," depicted a mushroom cloud caused by the crash, with a red barn and the rolling hills of Pennsylvania in the foreground. The plaintiff alleged that, in the course of an interview with her, a reporter from The Associated Press took a photograph of "End of Serenity" from a binder of materials she showed the reporter, then without authorization distributed the photo on the AP newswire together with an accompanying article written by the reporter.[1096]

The plaintiff brought a claim for violation of Section 1202 of the DMCA on the ground that she had included title and copyright information on "End of Serenity," which appeared in the photograph of it that the reporter took, but which was cropped out of the version of the photograph distributed by AP. Citing the IQ Group case, AP contended that Section 1202 was not applicable because the plaintiff's copyright notice on her photograph was not "digital." The

---

[1093] Id. at *21.

[1094] Report and Recommendation, Silver v. Lavandeira, No. 08 Civ. 6522 (JSR) (DF) at pp. 2-3 (S.D.N.Y. Jan. 7, 2009) (recommendation of magistrate judge), adopted in its entirety by the district court in Silver v. Lavandeira, 2009 U.S. Dist. LEXIS 15491 at *3 (S.D.N.Y. Feb. 26, 2009).

[1095] 2007 U.S. Dist. LEXIS 17768 (W.D. Pa. Mar. 9, 2007).

[1096] Id. at *3-4.

plaintiff testified in her deposition that she used a computer program called "Advanced Brochures" in a two-step process to print the title, her name, and the copyright notice on all printouts of her photograph. The court ruled that this technological process was sufficient to come within a digital "copyright management system" as defined in the statute. Moreover, the court noted that Section 1202(c) defines CMI to include "any" of the information set forth in the eight categories enumerated, "including in digital form." To avoid rendering those terms superfluous, the court held the statute must also protect non-digital information. Accordingly, the court concluded that the statute was applicable to the facts of the case.[1097]

AP sought summary judgment on the CMI claim on the ground that the metadata accompanying the photograph distributed by AP stated that the photograph was taken by the plaintiff. However, the court noted that the metadata also identified the plaintiff as a "stringer," from which recipients could have inferred that AP owned the copyright, and that there was no clear statement notifying recipients that the plaintiff owned the copyright to "End of Serenity." In addition, the court noted a factual dispute concerning whether the reporter had intentionally cropped the copyright notice out of the photograph, as the plaintiff alleged. Accordingly, the court denied AP's motion for summary judgment.[1098]

b. Associated Press v. All Headline News Corp.

In this case, the defendant gathered news stories on the Internet, including those of the Associated Press, and prepared them for republication by its customer sites under its own banner, either rewriting the text or copying the stories in full. It instructed its reporters to remove or alter the identification of the AP as author or copyright holder of the articles. AP brought a claim for common law "hot news" misappropriation and for violation of Section 1202. The defendant brought a motion to dismiss the claims, which the court denied. With respect to the CMI claim, the court rejected the IQ Group court's definition of CMI as limited to copyright management performed by the technological measures of automated systems. The court found that definition to be inconsistent with the text of the statutory definition, which makes no reference to "the technological measures of automated systems." Accordingly, the court denied the motion to dismiss the CMI claim.[1099]

c. Fox v. Hildebrand

In this case, the court rejected the Ya Ya Brand and IQ Group cases, ruling that CMI is not limited to notices that are digitally placed on a copyrighted work. The court found that the reference to "including in digital form" in the statutory definition of CMI in Section 1202(c) indicated that the definition was not limited to notices in digital form. Accordingly, the plaintiff's allegation that the defendant had copied the plaintiff's architectural drawings, on which the plaintiff had handwritten a copyright notice, and erroneously designated itself as the

---

[1097] Id. at *4-5, 15.

[1098] Id. at *15-17.

[1099] Associated Press v. All Headline News Corp., 608 F. Supp. 2d 454, 457 & 461-62 (S.D.N.Y. 2009).

copyright owner on the copied drawings, stated a claim under Section 1202(b) of the DMCA sufficient to survive the defendant's motion to dismiss.[1100]

d. Faulkner Press v. Class Notes

In this case, the court ruled that the plain language of the DMCA does not limit the definition of CMI to notices that are placed on works through technological processes. However, it granted summary judgment in favor of the defendant with respect to the plaintiff's claims for removal of CMI and addition of false CMI. The plaintiff owned the copyrights in electronic textbooks and film study questions created by a professor at the University of Florida for two wildlife issues courses. The textbooks had CMI printed on the boxes containing the electronic textbooks and within the textbooks' software. The film study questions were alleged to contain CMI by virtue of a watermark that appeared on the questions when viewed at a website maintained for the professor's course.[1101]

Class Notes hired students to take notes on the professor's class, and the plaintiff alleged that in the course of the note taking, the students viewed copyrighted material taken from the textbooks and film study questions presented by the professor and copied such material into the Class Notes note package. The plaintiff asserted a removal of CMI claim based on the fact that the Class Notes note package did not reproduce the CMI printed on the boxes of the electronic textbooks, and a false CMI claim based on the fact that the note package had the phrase "Einstein's Notes (c)" printed on it.[1102]

The court rejected both claims. With respect to the claim for removal of CMI, the court noted that Class Notes did not "remove" any CMI contained in the textbooks or on the film study questions. Its student note takers simply took notes from the professor's course and those notes were compiled into note packages. An action for removal of CMI requires the information to be removed from a plaintiff's product or work. Here, nothing was removed from the copyrighted works. Instead, information from the professor's courses was allegedly copied into a different form and then incorporated into the note packages. Hence, no CMI was removed from the plaintiff's product or work. With respect to the claim for false CMI, the court noted that the note packages were a different product from the professor's work even if they included materials from the professor's work. No alteration was made to the professor's product or work, so there was no violation of the DMCA by printing "Einstein's Notes (c)" on the note packages. Finally, even if there was illegal alteration of CMI, the court noted that the plaintiff had presented no evidence to show that Class Notes took any such action with intent to aid infringement. Accordingly, the court granted Class Notes summary judgment with respect to the CMI claims.[1103]

e. Agence France Presse v. Morel

[1100] Fox v. Hildebrand, 2009 U.S. Dist. LEXIS 60886 at *2, 5-8 (C.D. Cal. July 1, 2009).

[1101] Faulkner Press, LLC v. Class Notes, LLC, 2010 U.S. Dist. LEXIS 123935 at *2, 5 &13-14 (N.D. Fla. Nov. 23, 2010).

[1102] Id. at *2-4, 14-15.

[1103] Id. at *14-16.

In Agence France Presse v. Morel,[1104] photographer Daniel Morel took photos of Port au Prince, Haiti, shortly after an earthquake devastated the city and posted the photos on Twitpic. There were no copyright notices on the images themselves, but Morel's Twitpic page included the attributions "Morel" and "by photomorel" next to the images. A few minutes after Morel posted his photos, Lisandro Suero copied the photos, posted them on his Twitpic page, and tweeted that he had "exclusive photographs of the catastrophe for credit and copyright." Suero did not attribute the photos to Morel. Agence France Presse (AFP) downloaded 13 of Morel's photos from Suero's Twitpic page (not knowing that Suero had copied them from Morel), placed them on an image forum and transmitted them to Getty, an image licensing company. Morel's photos were labeled with the credit line "AFP/Getty/Lisandro Suero," designating AFP and Getty as the licensing agents and Suero as photographer. Getty then licensed Morel's photos to numerous third party news agencies, including CBS and CNN. After learning that the photos did not belong to Suero, AFP issued a wire instruction to change the photographer credit from Suero to Morel. However, Getty continued to sell licenses to charities, relief organizations, and new outlets that variously credited AFP, Suero, or Morel as the photographer.[1105]

Shortly thereafter, Corbis, which acted as Morel's worldwide licensing agent emailed Getty asserting exclusive rights to Morel's photos. That afternoon, AFP issued a "kill" for 8 images listing Morel as photographer, but the "kill" did not include identical images credited to Suero or images never credited to Morel. Morel and Corbis alleged that AFP and Getty failed to observe or enforce the credit change instruction or the "kill," continued to license and sell Morel's photos, and derived a direct financial benefit as a result. AFP filed a suit, seeking a declaratory judgment that AFP did not infringe Morel's copyrights in certain photos. Morel counterclaimed against AFP alleging copyright infringement and violation of the CMI provisions. AFP moved to dismiss Morel's counterclaims for failure to state a claim.[1106]

The court rejected the motion to dismiss the CMI claims. The court declined to adopt the definition of CMI in IQ Group as limited to a component of an automated copyright protection or management system. The court was persuaded by the reasoning of decisions rejecting IQ Group and held that the notations "Morel," "daniel morel," and "photomorel" used by Morel in connection with his photos fell within the scope of CMI under the plain language of the statute.[1107]

f. Murphy v. Millennium Radio

The case of Murphy v. Millennium Radio Group LLC[1108] was the first federal appellate court decision concerning whether CMI is limited to information that is a component of an automated copyright protection or management system. The plaintiff was the copyright owner of

---

[1104] 769 F. Supp. 2d 295 (S.D.N.Y. 2011).

[1105] Id. at 298-300.

[1106] Id. at 298, 300-301.

[1107] Id. at 305-06.

[1108] 650 F.3d 295 (3d Cir. 2011).

a photo. An unknown employee of the defendant scanned the photo from a magazine and posted the resulting electronic copy to the defendant's web site and to another web site. The resulting image, as scanned and posted to the Internet, eliminated the original photo's gutter credit (i.e., a credit placed in the inner margin, or "gutter," of a magazine page, ordinarily printed in a smaller type and running perpendicular to the relevant image on the page) identifying the plaintiff as the author. The plaintiff brought a claim for violation of the CMI provisions of the DMCA.[1109]

The district court had agreed with the reasoning of the IQ Group case and held that the photo credits were in no way a component of an automated copyright protection or management systems and therefore did not qualify as CMI protected under the DMCA.[1110] On appeal, the Third Circuit reversed. The Third Circuit noted that the statute imposes no explicit requirement that CMI be part of an automated copyright protection or management system, and rejected the defendants' argument that Section 1202's prohibition on removal of CMI must be interpreted in conjunction with Section 1201's focus on technological measures:

> [T]o all appearances, § 1201 and § 1202 establish independent causes of action which arise from different conduct on the part of defendants, albeit with similar civil remedies and criminal penalties. It may strike some as more intellectually harmonious to interpret the prohibition of removal of CMI in § 1202 as restricted to the context of § 1201, but nothing in the text of § 1201 actually dictates that it should be taken to limit the meaning of "copyright management information."[1111]

Turning to the legislative history of the DMCA, the court found that, while it is possible to read the legislative history to support an interpretation of CMI as limited to a component of an automated copyright protection or management system, that history did not provide an extraordinary showing of contrary intentions on the part of Congress that would justify rejecting a straightforward reading of the statutory language. The court there ruled that CMI is not restricted to the context of automated copyright protection or management systems.[1112] "Rather, a cause of action under § 1202 of the DMCA potentially lies whenever the types of information listed in § 1202(c)(1)-(8) and 'conveyed in connection with copies .. of a work … including in digital form' is falsified or removed, regardless of the form in which that information is conveyed."[1113] Accordingly, the Third Circuit vacated the district court's grant of summary judgment in favor of the defendants on the CMI claim.[1114]

g. William Wade Waller Co. v. Nexstar Broadcasting

[1109] Id. at 299.

[1110] Murphy v. Millennium Radio Group LLC, 2010 U.S. Dist. LEXIS 32631 at *2-3, *8-9 (D.N.J. Mar. 31, 2010).

[1111] 650 F.3d at 303.

[1112] Id. at 305.

[1113] Id.

[1114] Id. at 310.

This case involved the question whether a watermark logo in the bottom right hand corner of a photo identifying the copyright owner's web site constituted CMI. The court ruled that, although it was inclined to agree with a broad reading of what may constitute CMI, it did not need to decide the issue because there was no evidence that the defendants had removed the watermark when they posted the plaintiff's photos on their web site.[1115]

(2) Prohibitions on False CMI and Removal/Alteration of CMI

Section 1202(a) prohibits any person from knowingly providing CMI that is false or distributing or importing for public distribution CMI that is false, with the intent to induce, enable, facilitate, or conceal infringement. Section 1202(b) prohibits any person from intentionally removing or altering any CMI, distributing or importing for distribution CMI knowing that it has been altered or removed, or distributing, importing for distribution, or publicly performing works in which CMI has been removed or altered, in all cases knowing, or, with respect to civil remedies under Section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement.

(i) Cases re Removal or Alteration of CMI

a. Kelly v. Arriba Soft Corp.

The first case under the CMI provisions was Kelly v. Arriba Soft Corp.[1116] In that case, the defendant was the operator of a "visual search engine" on the Internet that allowed users to search for and retrieve images. In response to a search query, the search engine produced a list of reduced, "thumbnail" pictures. By clicking on the desired thumbnail, a user could view an "image attributes" window displaying the full-size version of the image, a description of its dimensions, and an address for the website where it originated. By clicking on the address, the user could link to the originating website for the image.[1117]

The search engine maintained an indexed database of approximately two million thumbnail images obtained through the operation of a web crawler that traveled the Web in search of images to be converted into thumbnails and added to the index. The defendant's employees conducted a final screening to rank the most relevant thumbnails and eliminate inappropriate images. The plaintiff was the owner of the copyright in about 35 photographs that were indexed by the crawler and put in the defendant's database. The plaintiff sued the defendant for copyright infringement, alleging that storage of the images in the database constituted a direct infringement, as well as a violation of the CMI provisions of the DMCA.[1118]

[1115] William Wade Waller Co. v. Nexstar Broadcasting, Inc., 2011 U.S. Dist. LEXIS 72803 at *2, *10-11 (E.D. Ark. July 6, 2011).

[1116] 53 U.S.P.Q.2d 1361 (C.D. Cal. 1999), aff'd in part and rev'd in part on other grounds, 336 F.3d 811 (9th Cir. 2003).

[1117] Id. at 1362.

[1118] Id.

The court ruled that the defendant's use of the images in thumbnail form constituted a fair use, and that there was no violation of the CMI provisions of the DMCA.[1119]

The plaintiff argued that the defendant violated the CMI provisions of the DMCA by displaying thumbnails of the plaintiff's images without displaying the corresponding CMI consisting of standard copyright notices in the surrounding text accompanying the photographs on the plaintiff's website from which the crawler obtained the photographs. Because these notices did not appear in the images themselves, the crawler did not include them when it indexed the images. As a result, the images appeared in the defendant's index without the CMI, and any users retrieving the images through the search engine would not see the CMI.[1120]

The court rejected this claim, holding that Section 1202(b)(1) (which prohibits intentionally removing or altering CMI) "applies only to the removal of copyright management information on a plaintiff's product or original work."[1121] The court also ruled that even if Section 1202(b)(1) did apply, the plaintiff had not offered any evidence showing that the defendant's actions were intentional, rather than merely an unintended side effect of the crawler's operation.[1122] The court found that the more applicable provision was that of Section 1202(b)(3), which prohibits distribution of copies of works knowing that CMI has been removed or altered without authority of the copyright owner or the law, knowing or having reason to know that it will induce, enable, facilitate, or conceal an infringement. The court also found no violation of this section, however, because users who clicked on the thumbnail version of the images were given a full-sized version, together with the name of the website from which the image was obtained (and an opportunity to link there), where any associated CMI would be available.[1123] "Users were also informed on Defendant's Web site that use restrictions and copyright limitations may apply to images retrieved by Defendant's search engine."[1124] Based on these facts, the court concluded that the defendant did not have "reasonable grounds to know" under Section 1202(b)(3) that it would cause its users to infringe the plaintiff's copyrights:

> Plaintiff's images are vulnerable to copyright infringement because they are displayed on Web sites. Plaintiff has not shown users of Defendant's site were any more likely to infringe his copyrights, any of these users did infringe, or Defendant should reasonably have expected infringement.[1125]

Accordingly, the court concluded that there had been no violation of the DMCA.

b. Thron v. Harper Collins Publishers

[1119] Id. at 1363-67.

[1120] Id. at 1366.

[1121] Id.

[1122] Id.

[1123] Id.

[1124] Id.

[1125] Id. at 1367.

In Thron v. Harper Collins Publishers,[1126] the plaintiff alleged that the defendant misappropriated two of his allegedly copyrighted photographs for use in a book published by the defendant. The plaintiff further contended that the defendant's subsequent efforts to publicize the book through the Internet violated the CMI provisions of the DMCA because the plaintiff had provided Amazon.com with a digital image of one of the photographs that was allegedly impermissibly altered to remove certain unspecified information related to the plaintiff's copyright registration. The court rejected this claim because the plaintiff's copyright registration was itself invalid and because the plaintiff had submitted no competent, admissible evidence to support any finding that the defendant removed or altered the information intentionally, as required by the statute.

c. Gordon v. Nextel Communications

In Gordon v. Nextel Communications,[1127] the plaintiff brought suit against Nextel and its advertising agency for copyright infringement for the unauthorized use of several of his dental illustrations in a television commercial for Nextel's two-way text message. The plaintiff also claimed a violation of the CMI provisions of the DMCA based on alleged removal of the copyright notice from the illustrations. The district court granted summary judgment on the CMI claims on the ground that the plaintiff failed to present any evidence that the defendants intentionally removed or altered the copyright information or that the defendants knew that the copyright information had been removed.[1128]

On appeal, the Sixth Circuit affirmed. The decision is important because the Sixth Circuit ruled for the first time that vicarious liability may apply with respect to violations of the CMI provisions (the rationale of the holding would presumably also apply to the anti-circumvention provisions of the DMCA). In particular, the court held that, regardless of the defendants' actual knowledge of the removal or alteration of the copyright information, they could be held vicariously liable if, just as in the case of ordinary infringement, they had the right and ability to supervise the conduct constituting the violation and they had an obvious and direct financial interest in the conduct.[1129]

The court noted that, although the record was not clear in this regard, it was reasonable to infer that the advertising agency retained the ability to supervise the development of the commercial. And both defendants had direct financial interests in the exploitation of the copyrighted materials. As a result, the court ruled that, even though the CMI provisions require the intentional removal of CMI or the distribution of copies of works "knowing" that CMI has been removed or altered, "it is inappropriate to permit summary judgment to be granted based on the defendants' lack of actual knowledge of the removal of the copyright management information when they may be vicariously liable for its removal."[1130] Thus, although the

---

[1126] 64 U.S.P.Q.2d 1221 (S.D.N.Y. 2002).

[1127] 68 U.S.P.Q.2d 1369 (6th Cir. 2003).

[1128] Id. at 1370.

[1129] Id. at 1371.

[1130] Id. at 1372.

plaintiff had to prove that the direct violators of the CMI provisions possessed actual knowledge of the unauthorized change to the CMI, the plaintiff need not prove that Nextel and its advertising agency, as vicarious infringers, had such knowledge.

Ultimately, however, the Sixth Circuit affirmed the district court's grant of summary judgment to the defendants on the ground that, even if the persons from whom the advertising agency had obtained the material containing the illustrations upon which the commercial was based had removed the copyright information from the illustrations, those persons testified without contradiction that they believed the materials had been authorized for use in television commercials. Accordingly, such removal was not done with reasonable grounds to know that it would "induce, enable, facilitate, or conceal an infringement," as required by Section 1202(b).[1131]

d. Monotype Imaging, Inc. v. Bitstream Inc.

In Monotype Imaging, Inc. v. Bitstream Inc.,[1132] the court adopted a rather broad reading of the scope of the CMI provisions. The plaintiff Monotype developed and distributed fonts and font software. The defendant Bitstream competed with Monotype, and developed a product called TrueDoc, a computer program that facilitated the display of typeface designs on computer screens and other output devices. Bitstream openly promoted the fact that TrueDoc replicated the original typefaces of other vendors. TrueDoc included a Character Shape Recorder (CSR) component that created a compact file format called a Portable Font Resource (PFR) based on an underlying font software program. The CSR obtained data that described the shape of the typeface characters of the underlying font program from the computer's operating system. When accessing information from the operating system about the font software, TrueDoc did not request the copyright notice from the Windows operating system.[1133] Monotype brought a claim for copyright infringement, apparently based on alleged copying of Monotype's font software in the course of creating PFR's that would work with TrueDoc, as well as a claim for violation of the CMI provisions. Bitstream moved for summary judgment.

Monotype claimed that TrueDoc's failure to copy the copyright notice from its font software programs violated the CMI provisions of the DMCA because it was virtually identical to removing the copyright notice. The court agreed with Monotype that the plain language of the DMCA does not require that TrueDoc, itself, physically remove the copyright notices from the Monotype font software in creating the PFR files. Thus, the court ruled that the mere fact that TrueDoc did not "remove" the copyright notices, but instead made copies of the font software without including the copyright notice, did not preclude liability under the DMCA.[1134]

Bitstream argued that there should be no finding of a CMI violation because when TrueDoc retrieved information from the operating system about a font software program, the

---

[1131] Id. at 1373.

[1132] 2005 U.S. Dist. LEXIS 7410 (N.D. Ill. Apr. 21, 2005).

[1133] Id. at *2-3.

[1134] Id. at *26-27.

operating system did not provide the copyright strings. Monotype countered by pointing to the fact that the copyright information is accessible through the operating system, and Bitstream simply chose not to include the copyright notice. Monotype's expert had examined Bitstream's TrueDoc source code and opined that Bitstream was capable of engineering TrueDoc to retrieve the copyright notice along with the font software information. The court ruled that, viewing this evidence in the light most favorable to Monotype, the expert testimony created a triable issue of fact whether Bitstream copied Monotype's fonts without the copyright notices in violation of the DMCA. Accordingly, the court denied Bitstream's motion for summary judgment on the CMI claim.[1135]

Three months later, after a bench trial, the court issued a second opinion ruling that Bitstream was not liable for either copyright infringement or CMI violations.[1136] With respect to CMI, because the court found the plaintiffs had failed to prove that Bitstream's licensees had used the CSR with any of the plaintiff's fonts, they had therefore failed to show that Bitstream intentionally removed CMI, or distributed copies of works knowing that CMI had been removed, with knowledge or having reasonable grounds to know that it would induce, enable, facilitate or conceal infringement, as required by Sections 1202(b)(1) and 1201(b)(3) of the DMCA.[1137]

The court also found no liability for contributory infringement, again because the plaintiffs failed to prove any direct infringement by Bitstream's licensees – in particular, that a Bitstream licensee had ever used the CSR to copy the plaintiffs' fonts.[1138] The court also found the plaintiffs did not present any evidence that Bitstream ever knew that its licensees were using TrueDoc's CSR with the plaintiffs' fonts.[1139] Citing the Supreme Court's Grokster case, however, the court noted that "a court may impute culpable intent as a matter of law from the characteristics or uses of an accused product."[1140] In determining whether the alleged contributory infringer acted with such culpable intent, the court, apparently not believing that the Grokster case repudiated any of the Aimster case's holding or rationale, noted that the Seventh Circuit considers the following factors under the Aimster case: "(1) the respective magnitudes of infringing and noninfringing uses; (2) whether the defendant encouraged the infringing uses; and (3) efforts made by the defendant to eliminate or reduce infringing uses."[1141]

The court found that the plaintiffs had not satisfied any of the factors. The plaintiffs had not submitted any evidence to tie the ratio of Bitstream fonts to non-Bitstream fonts available in the marketplace to the proportion of such fonts that Bitstream's customers actually used with the CSR. Nor had they presented any evidence that Bitstream knew of or encouraged the allegedly infringing uses of TrueDoc. With respect to the third factor, the court noted that Bitstream had

---

[1135] Id. at *27-28.

[1136] Monotype Imaging, Inc. v. Bitstream Inc., 376 F. Supp. 2d 877 (N.D. Ill. 2005).

[1137] Id. at 893.

[1138] Id. at 884.

[1139] Id. at 887.

[1140] Id.

[1141] Id.

made at least some efforts to reduce the risk of infringement of third parties' intellectual property through the use of TrueDoc, in the form of a "doc-lock" feature with the capability of preventing a third party from using a PFR that it had received for any purpose other than viewing the document with which the PFR came. Bitstream also engineered TrueDoc to honor the embedding flags that font foundries include in their font data, which prohibit a third party from embedding that font into another technology.[1142] Finally, the court found no liability under the inducement doctrine of the Grokster case, because there was no evidence that Bitstream had knowledge of its customers' alleged infringements, much less that it acted with the "purposeful, culpable expression and conduct" required under the Grokster decision.[1143]

e. Keogh v. Big Lots Corp.

In Keogh v. Big Lots Corp.,[1144] the court ruled that the prohibition of Section 1202(b)(3) of the DMCA against distributing works knowing that CMI has been removed or altered without authority of the copyright owner requires actual knowledge that CMI has been removed. Constructive knowledge of removal of CMI is not sufficient. Once CMI is removed from a work, however, the defendant is required to have only "reasonable grounds to know" (a constructive knowledge standard) that its actions would induce, enable, facilitate, or conceal an infringement of any right under the DMCA. Because the plaintiff had not alleged that the defendant had actual knowledge that CMI had been removed from imported birdhouses having designs that allegedly infringed the plaintiff's birdhouses, the court granted the defendant's motion to dismiss the CMI claim under Rule 12(b)(6).[1145]

f. Goldman v. Healthcare Management Systems

In Goldman v. Healthcare Management Systems,[1146] the plaintiff alleged that the defendant had been infringing upon the its copyright in a computer program since the plaintiff downloaded the program onto the defendant's computer, and that the defendant had violated the CMI provisions of the DMCA by knowingly removing the plaintiff's CMI (apparently in the form of a copyright notice). The court denied the plaintiff's motion for summary judgment, finding numerous disputed facts, including whether the appropriate copyright notices were on the original materials given to the defendant.[1147]

g. Thomas M Gilbert Architects v. Accent Builders

[1142] Id. at 887-88.

[1143] Id. at 888-89.

[1144] 2006 WL 1129375 (M. D. Tenn. Apr. 27, 2006).

[1145] Id. at *2.

[1146] 2006 U.S. Dist. LEXIS 89009 (W.D. Mich. Dec. 8, 2006).

[1147] Id. at *3-4.

In Thomas M. Gilbert Architects, P.C. v. Accent Builders & Developers, LLC,[1148] the court granted summary judgment in favor of the defendant on a claim under Section 1202(b) for removal of a copyright notice from the plaintiff's architectural plans. The court found no evidence to show that the defendant intentionally removed the notice, or that he had reason to know that its removal would induce, enable, facilitate, or conceal infringement. The defendant testified that he was unfamiliar with copyright law and did not recall seeing the copyright notice when he modified the plaintiff's plans. Accordingly, because the plaintiff had made no showing of the required intent, the court granted summary judgment in the defendant's favor.[1149]

h. Banxcorp v. Costco

In Banxcorp v. Costco Wholesale Corp.,[1150] the plaintiff published market research performance indices based on selected banking, mortgage and loan data that were used as benchmarks to measure the rates and performance of the U.S. banking and mortgage markets. Costco entered into an agreement with the defendant Capital One Financial Corp. to provide a co-branded direct banking service. The plaintiff and Capital One entered into a license agreement permitting Capital One to access and use the indices and the data contained therein. The plaintiff alleged that Capital One breached the license agreement by redistributing the indices to Costco in order to benefit the co-branded banking services. The plaintiff asserted a DMCA claim based on allegations that when the defendants copied the indices they altered or removed the CMI that the plaintiff had associated with the data.[1151] Specifically, the plaintiff had associated MCI with the indices that read: "(C) [year of publication] BanxCorp. All Rights Reserved." The plaintiff included in its complaint an example of an ad the defendants ran in conjunction with the indices that included the following differing CMI: "National Average of [Annual Percentage Yields] for money market accounts as published by BanxQuote.com as of 5/22/07."[1152]

The court held that these allegations were sufficient to survive a motion to dismiss the plaintiff's CMI claim. "At summary judgment, Defendants will have an opportunity to present evidence that the placement of the CMI either indicated that it did not refer to the BanxQuote Indices, or was sufficiently removed to demonstrate that Defendants lacked the intent required to show a violation of the DMCA. However, the Court declines to hold that, as a matter of law, CMI must be placed on the actual information on a website in order to state a claim under the DMCA."[1153]

i. Agence France Presse v. Morel

[1148] 629 F. Supp. 2d 526 (E.D. Va. 2008).

[1149] Id. at 537.

[1150] 723 F. Supp. 2d 596 (S.D.N.Y. 2010).

[1151] Id. at 599-600.

[1152] Id. at 610.

[1153] Id. at 610-11.

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. In ruling on the motion of Agence France Presse (AFP) to dismiss the claim against it for removal of CMI, AFP argued that CMI must be removed from the photograph itself to state a claim for removal or alteration of CMI. The court rejected this argument, noting that the DMCA defines CMI as information "conveyed in connection with copies" and so does not require the CMI to appear on the work itself. The court found it implausible that a viewer of Morel's photos would not understand the designations "Morel" and "by photomorel" appearing next to the images to refer to his authorship. While the location of CMI could go to AFP's intent, that face issue could not be resolve on a motion to dismiss. As to intent and knowledge of infringement, Morel had alleged that AFP, CNN, and CBS representatives contacted him about his photos, copied them without his permission, and distributed them with altered CMI. He also alleged that, in disregard of the credit change instruction, Getty continued to distribute photos crediting Suero or AFP as photographer. The court concluded that these allegations were sufficient to survive a motion to dismiss.[1154]

j. Scholz Design v. Custom Homes

In this case the plaintiff brought a claim under Section 1202 for removal of CMI based on the defendant's posting on a web site of copies of images depicting designs of homes that the plaintiff claimed a copyright in. The plaintiff claimed that the defendant had removed the plaintiff's name from the designs before posting them. The court ruled that the designs were not copyrightable as architectural drawings because they did not contain the necessary level of detail to allow construction of a home from them. The court then dismissed the plaintiff's CMI claim, ruling that it must have a valid copyright infringement claim in order for its Section 1202 claim to survive.[1155]

k. Personal Keepsakes v. PersonalizationMall.com

In this case the plaintiff, operator of a web site selling personalized gifts and knickknacks, brought a claim against the defendants who also operated a site selling personalized gifts on the Internet for allegedly taking the plaintiff's copyrighted poems and incorporating them into the defendants' own products. Among other things, the plaintiff brought a claim under Section 1201 for removal of CMI from the poems when they were copied into the defendants' products. The plaintiff identified three pieces of purported CMI that the defendants removed when copying the poems: the poetrygift.com name affiliated with the poems on the plaintiff's site, the titles of the works (specifically, "Baptism Gifts"/"On Your Baptism Day" and "Ring Bearer Gift"/"To Our Ring Bearer"), and the copyright notice on every page of the plaintiff's web site.[1156]

[1154] Agence France Presse v. Morel, 769 F. Supp. 2d 295, 305-06 (S.D.N.Y. 2011).

[1155] Scholz Design, Inc. v. Sard Custom Homes, LLC, 2011 U.S. Dist. LEXIS 76663 at *2-3, *9-10 & *14 (D. Conn. July 15, 2011).

[1156] Personal Keepsakes, Inc. v. PersonalizationMall.com, 2012 U.S. Dist. LEXIS 15280 at *1-2, 17-18 (N.D. Ill. Feb. 8, 2012).

The court rejected all bases for the CMI claim. The court held that the poetrygift.com name could not be CMI because the copyright registrations attached to the complaint showed Personal Keepsakes, Inc., not poetrygift.com, as the owner of the copyright. Thus, poetrygift.com was at best an indicator of the seller of the product, not of the copyright owner. The titles could not be CMI because the copyright registrations did not list the titles of the works as they appeared on the plaintiff's web site, but rather referred to them as "Personal Keepsakes VI" and "Personal Keepsakes X." One could therefore not search the copyright titles as used on the web site to see if they were registered. The court concluded that allowing a plaintiff to make a DMCA claim based on alleged CMI that does not link up in any way to the copyright registration would be an invitation to unfair litigation against parties who had tried to tread carefully to avoid copyright infringement.[1157]

In addition, the copyright notice that appeared on every page of the plaintiff's web site was not CMI with respect to the allegedly copied poems. The web site notice read "Web Site and Original Verses -- © (1991-2012)." The court found that, although it was plausible that the copyright notice referred to the poems at issue, the complaint did not suggest the poems at issue were "original verses" as referenced in the notice.[1158]

Finally, the court ruled that the plaintiff had stated a case of false CMI against one of the defendants when it put a copyright notice in the name of its "Walk with Jesus Baptism Keepsake" that incorporated the same or a very similar poem as the plaintiff's product, and that copyright notice followed a line in the poem that formed the title "Walk with Jesus." Consequently, the court held that it was plausible that the notice could refer to the poem, and not the product as a whole. The court also rejected the plaintiff's argument that statements in the defendants' web site Terms of Use referencing that the content or intellectual property on the web site was owned by the defendants constituted false CMI in connection with the poems, because the Terms of Use statements were not close to the poems.[1159] The court cited another district court decision requiring that a defendant must remove the CMI from the body or the area around the work to violate the DMCA, and concluded that "as a matter of law, if a general copyright notice appears on an entirely different webpage than the work at issue, then that CMI is not 'conveyed' with the work and no claim will lie under the DMCA. [The plaintiff] cannot base a DMCA claim on Defendants' general copyright notices placed elsewhere on the site."[1160]

(ii) Cases re False CMI

a. Schiffer Publishing, Ltd. v. Chronicle Books, LLC

[1157] Id. at *18-19.

[1158] Id. at *19-20.

[1159] Id. at *20-22.

[1160] Id. at *23. The court gave the plaintiff an opportunity to amend its DMCA claims if it could do so in good faith based on the guidance in the opinion. Id.

In Schiffer Publishing, Ltd. v. Chronicle Books, LLC,[1161] the plaintiffs owned copyrights in various photographs of fabrics, which the defendants allegedly infringed by scanning into digital form for inclusion into a book published by the defendants titled *1000 Fabrics*. The plaintiffs also alleged that the defendants had violated Sections 1202(a) and (b) by falsely naming themselves as the copyright holders of the pictures published in *1000 Patterns* and by "removing" the plaintiffs' copyright notices from those pictures.[1162]

The court found no violation of the CMI provisions of the DMCA. The court noted that to recover for a violation of Section 1202(a), a plaintiff must prove that the defendant knew the CMI on a distributed work was false and distributed the false CMI with the intent to aid infringement. The court ruled that the plaintiffs had not shown that the defendants possessed the requisite knowledge or intent to violate the relevant copyrights. Although there was evidence at trial that the defendants instructed its employees to avoid using too many series of page images from any single book containing the plaintiffs' photographs, the court found the evidence indicated only that the defendants knew the plaintiffs had copyrights in their books as compilations, not that they knew the individual photographs contained therein were copyright protected. Other evidence at trial suggested that the defendants erroneously believed the plaintiffs had no copyright in their individual photographs because they contained insufficient creativity. Accordingly, the intent requirement of Section 1202(a) was not met.[1163]

The court also found no violation of Section 1201(b) because the only CMI the plaintiffs included with their work were notices of copyright that appeared on the inside covers of their books. The individual photographs that were the subject of the action did not contain any CMI whatsoever, either on or near the images themselves. The court ruled that to establish a violation of Section 1202(b), the defendants must remove CMI from the body of, or area around, the plaintiffs' work. Because the plaintiffs had failed to demonstrate the defendants had done so, the claim for violation of Section 1202(b) failed.[1164]

b. Agence France Presse v. Morel

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. In ruling on the motion of Agence France Presse (AFP) to dismiss the claim against it for falsification of CMI, the court found Morel's allegations that AFP labeled his photos with the credit lines "AFP/Getty/Daniel Morel" and "AFP/Getty/Lisandro Suero" to be sufficient to plead falsification of CMI. AFP had not contested that those credit lines constituted CMI. Morel also set forth a factual basis for alleging that AFP knew the CMI was false and intended to facilitate infringement. Morel alleged that an AFP photo editor viewed his photos before asking about identical photos on Suero's Twitpic page, and that when Morel failed to respond to the editor's email, AFP downloaded the pictures from Suero. Morel further alleged that AFP knew the photos were his because he was a well-known photographer and AFP had no reason to believe

[1161] 73 U.S.P.Q.2d 1090 (E.D. Pa. 2004).

[1162] Id. at 1101.

[1163] Id. at 1102.

[1164] Id.

Suero took the photos. However, AFP credited Suero without inquiry. As to Getty, Morel alleged that even after AFP issued a wire to change the photographer credit from Suero to Morel, Getty continued to license photos crediting Suero. Getty sought to obtain credit for the photographs even though it knew of Morel's reputation and had not investigated Suero's authorship. The court concluded that these allegations sufficiently plead knowledge and intent.[1165]

c. Personal Keepsakes v. PersonalizationMall.com

This case in discussed in Section II.G.1(b)(2)(i).k above.

(3) Exceptions and Limitations

Sections 1202(d) provides an exception for law enforcement, intelligence, and information security activities. Section 1202(e) limits the liability of persons for violations in the course of analog transmissions by broadcast stations or cable systems if avoiding the activity that constitutes a violation of the CMI integrity provisions is not technically feasible or would create an undue financial hardship.

(c) Remedies for Violations of Sections 1201 and 1202

Civil Remedies. Section 1203 provides civil remedies for any person injured by a violation of Section 1201 or 1202, including temporary and permanent injunctions (although Section 1203(b)(1) contains a provision prohibiting injunctions that constitute prior restraints on free speech or the press protected under the First Amendment), impounding, actual damages and any additional profits of the violator,[1166] statutory damages (in the amount of not less than $200 or more than $2,500 for each violation of Section 1201, and not less than $2,500 or more than $25,000 for each violation of Section 1202), costs and attorneys fees, and an order for the remedial modification or the destruction of any device or product involved in the violation. Under Section 1203(c)(4), damages may be trebled by the court for repeated violations within a three year period. Conversely, under Section 1203(c)(5), damages may be reduced or remitted entirely if the violator proves that it was not aware and had no reason to believe that its acts constituted a violation.

Criminal Penalties. Section 1204 provides for criminal penalties for the willful violation of Sections 1201 or 1202 for purposes of commercial advantage or private financial gain.

[1165] Agence France Presse v. Morel, 769 F. Supp. 2d 295, 304-05 (S.D.N.Y. Jan. 14, 2011).

[1166] Section 1203(c) provides:
(1) **In general.**—Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either –
(A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or
(B) statutory damages, as provided in paragraph (3).
(2) **Actual damages.**—The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.

Penalties include fines up to $1,000,000 and imprisonment for up to 10 years for repeated offenses.[1167]

(1) Statutory Damages and Disgorgement of Profits

(i) Sony Computer Entertainment America v. Filipiak

In Sony Computer Entertainment America, Inc. v. Filipiak,[1168] the court addressed the standard for computing statutory damages for a violation of the anti-circumvention provisions of the DMCA. The defendant Filipiak sold modification chips for the Sony PlayStation 2 console that circumvented the technological copyright protection measures in PlayStation consoles and allowed users to play unauthorized and illegal copies of PlayStation video games. The court found that Filipiak knew at the time he was selling them that the sale of the mod chips was illegal under the DMCA. Filipiak signed an agreement with SCEA that he would stop selling the mod chips, but nevertheless willfully violated the agreement and continued to sell them. Thereafter, he signed a stipulated consent judgment and injunction that prohibited him from marketing or selling the mod chips and agreed to pay $50,000 in damages, but still continued to sell the mod chips surreptitiously. When he was caught by SCEA doing so, he admitted that he shouldn't have been doing so and entered into a second consent judgment.[1169]

Based on various evidence, the court found that Filipiak had sold a minimum of 7,039 circumvention devices and proceeded to adjudicate the amount of statutory damages that Filipiak should pay. The court first ruled, by analogy to a statutory damages case under the Federal Communications Act, that Section 1203(c)(3)(A) authorizes a separate award of statutory damages for each device sold.[1170] Because there were no cases construing what "just" means under Section 1203(c)(3)(A), the court looked to cases construing the term under the general statutory damages provision of Section 504(c) of the copyright statute. Under the Section 504(c) case law, courts consider the following factors in determining the amount of a damages award: the expense saved by the defendant in avoiding a licensing agreement; profits reaped by the defendant in connection with the infringement; revenues lost to the plaintiff; the willfulness of the infringement; and the goal of discouraging wrongful conduct.[1171] Applying the factors, and particularly considering the willful nature of Filipiak's violations, the court awarded statutory damages of $800 per device sold before Filipiak entered into the first agreement with SCEA, and the maximum of $2500 per device sold or shipped thereafter, for a total award of $5,631,200.[1172]

[1167] The Digital Future Coalition has criticized Section 1202 as too draconian, in that it would impose civil penalties even in cases where no specific intent to infringe or promote infringement can be shown. "In other words, even someone who alters digital identifiers casually could be liable for a minimum of $2,500 in damages plus costs and attorney's fees." See position paper of the DFC at www.ari.net/dfc/docs/stwip.htm, p. 3.

[1168] 406 F. Supp. 2d 1068 (N.D. Cal. 2005).

[1169] Id. at 1070-74.

[1170] Id. at 1074.

[1171] Id. at 1074-75.

[1172] Id. at 1075-76.

(ii) Sony Computer Entertainment v. Divineo

The facts and rulings of the court in Sony Computer Entertainment America, Inc. v. Divineo[1173] are reported in Section II.G.1(m)(19) above. As a remedy for the DMCA violations found by the court, the plaintiff elected statutory damages. The court determined that the defendant had sold a total of 10,012 circumvention devices, and that sales of the devices constituted willful infringement, at least with respect to those sales after the filing of the lawsuit in 2004. Although the defendant had decided to stop selling the HDLoader software in early 2005, the defendant offered no credible explanation for its decision to continue selling its other circumvention devices after that point. Accordingly, the court awarded enhanced damages of $800 per device for sales after the first quarter of 2005 (an estimated 2,913 devices) and the minimum damages of $200 per device sold before that time, for a total statutory damages award of $3,750,200.[1174]

(iii) McClatchey v. The Associated Press

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. The Associated Press (AP) brought a motion in limine seeking to limit the number of statutory damage awards that the plaintiff could recover for the distributions of her photograph with CMI removed. The plaintiff claimed entitlement to a separate statutory award for each downstream distribution of the photograph to each of AP's 1,147 subscribers who had received the photograph. AP argued that the distribution of false CMI to all AP subscribers should be treated as only a single violation of the DMCA, entitling the plaintiff to but a single award of statutory damages.[1175] The court agreed with AP based on Congress' intent in providing statutory damages as an alternative type of damage award:

> Presumably, plaintiffs will elect statutory damages only when that calculation exceeds their actual damages. In other words, Congress has determined that in order to deter violations of the DMCA, plaintiffs electing statutory damages may receive a windfall. The Court's definition of the term "violation" will determine the extent of that windfall. This Court concludes that Congress would not have intended to make the statutory damages windfall totally independent of the defendant's conduct. Where one act by Defendant results in mass infringement, it is more likely that actual damages will yield the more favorable recovery. The DMCA damages provisions are clearly focused on the defendant's conduct. *Compare section 1203(c)(3)(A)* (calculating statutory damages "per act"). In essence, the term "each violation" is best understood to mean "each violative act performed by Defendant." Thus, AP would violate the DMCA each time it wrongfully distributed a photograph to its subscribers. In this case, the Court concludes that AP committed only one alleged violative act by distributing the

[1173] 457 F. Supp. 2d 957 (N.D. Cal. 2006).

[1174] Id. at 966-67.

[1175] McClatchey v. The Associated Press, 2007 U.S. Dist. LEXIS 40416 (W.D. Pa. June 4, 2007), at *13.

> End of Serenity photograph to its PhotoStream subscribers, even though there were 1,147 recipients.[1176]

Upon a motion for reconsideration of this ruling, the district court adhered to its original analysis, but certified the issue for interlocutory appeal and stayed all further proceedings pending resolution of that appeal.[1177]

(iv) Goldman v. Healthcare Management Systems

In this case, the plaintiff sought statutory damages for the defendants' distribution of infringing copies of a computer program with the plaintiff's CMI removed. The court cited the McClatchey case for the proposition that, for purposes of Section 1203(c)(3) statutory damages, the phrase "for each violation" means each violative act performed by the defendant. However, in the instant case, unlike a television signal or an AP wire story sent simultaneously to all subscribers, the alleged "violation" was not a singular, isolated event, but rather the provision of the same computer program at different times, under different circumstances, to multiple hospitals. Accordingly, there could be a separate statutory damages award for each computer program distributed to a hospital. However, the court further ruled that whether the subsequent distribution to the hospitals of any particular update to those computer programs would constitute an additional separate "violation" of the plaintiff's copyright was a factual question that would have to be resolved by a jury.[1178]

(v) Stockwire Research Group v. Lebed

In this case, the court entered a default judgment against the defendants, who were accused of violating Section 1201 by removing technical protection measures from the plaintiffs' documentary presentation, converting it a Windows media video and posting it on the web without the plaintiffs' permission, and of violating Section 1202 by removing CMI from the video in the form of the copyright notice, the title of the work, the information identifying one of the plaintiffs as the copyright holder, and the name of the other plaintiff who was credited in the work.[1179] The plaintiffs sought statutory damages. Following the McClatchey decision, the

---

[1176] Id. at *17-18. The plaintiff also sought statutory damages under Section 504 of the copyright statute. Citing Professor Nimmer's treatise, she argued that she was entitled to recover multiple statutory damages awards if a party is found to be jointly and severally liable with multiple parties who are not jointly and severally liable with each other. Id. at *8. The court rejected this argument, based on the language in Section 504(c)(1) that an award of statutory damages may be recovered for all infringements involved in the action "for which *any* two or more infringers are liable jointly and severally" (emphasis added). Id. at *9-10. Based on the presence of the word "any" rather than "all" in the statute, the court concluded that "the most plausible interpretation of the statute authorizes a single award when there is any joint and several liability, even if there is not complete joint and several liability amongst all potential infringers." Id. at *10. Moreover, the court noted that it need not reject Professor Nimmer's position in all circumstances, because in the instant case the only defendant, AP, was jointly and severally liable with all downstream infringers, so the plaintiff was entitled to only a single statutory damages award. Id. at *12.

[1177] McClatchey v. The Associated Press, 2007 U.S. Dist. LEXIS 41969 (W.D. Pa. June 8, 2007).

[1178] Goldman v. Healthcare Management Sys., 559 F. Supp. 2d 853, 867-68 (W.D. Mich. 2008).

[1179] Stockwire Research Group, Inc. v. Lebed, 577 F. Supp. 2d 1262, 1265 (S.D. Fla. 2008).

court ruled that, for purposes of statutory damages for removal of CMI, "each violation" means each time the product with CMI removed was posted for distribution by the defendant (here, three times), regardless of the number of end recipients.[1180] However, for purposes statutory damages for violation of the anti-circumvention prohibitions, "per act of circumvention" means each instance in which an end user gained access to the copyrighted material through unlawful circumvention – here, 11,786 unauthorized viewings, for which the court awarded statutory damages of $200 per viewing, for a total award of $2,357,200.[1181] Thus, CMI statutory damages focus on the acts of the defendant, whereas anti-circumvention statutory damages focus on the acts of the recipients.

(vi) MDY Industries, LLC v. Blizzard Entertainment, Inc.

The facts of this case and the court's various rulings on liability are set forth in Section II.G.1(a)(2) above. Blizzard requested that it should be entitled to a minimum statutory damages award of $24 million based upon MDY's sales of at least 120,000 Glider licenses (120,000 x $200). The district court, however, awarded statutory damages of $6.5 million, the amount of the damage award in the stipulated judgment between the parties. The court refused to make a reduction of damages on the basis of innocent infringement because MDY had designed its Glider software specifically to bypass the plaintiff's Warden software.[1182] On appeal, the Ninth Circuit reversed the district court on all rulings except as to MDY's liability for violation of Section 1201(a)(2) of the DMCA and remanded for trial on Blizzard's claim for tortuous interference with contract.[1183]

(vii) Stockart.com v. Engle

The plaintiff Stockart was in the business of licensing downloads of high end digital imagery through the Internet. Although the images were generally created by others, Stockart took title to the copyrights in the works and paid per-download fees to the creators. The defendant performed unauthorized downloads of several of Stockart's images and used them to create logos, which the defendant posted and sold on his own website. All images on Stockart.com contained a copyright notice and a © symbol at the bottom of the website screen on which each image appeared. On a motion for a default judgment, a magistrate judge found that such notice and symbol constituted protectable CMI, that by incorporating Stockart's images into his logos, the defendant had removed Stockart's CMI from the images, that such removal had been intentional, and that the defendant knew that the removal was a violation of the Copyright Act because, in order to establish an account with Stockart, the defendant had been required to acknowledge and accept a copyright warning in order to search and download images on the site, which warning stated that removal of images from the site or their separation from the copyright

---

[1180] Id. at 1267.

[1181] Id. at 1268.

[1182] MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 38260 at *4-6 (D. Ariz. Apr. 1, 2009).

[1183] MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 at *2-3 (9th Cir. Feb. 17, 2011).

management information on the site was not authorized and constituted a violation of copyright law.[1184]

Accordingly, the magistrate recommended that the district court conclude that Stockart had stated a viable claim for removal of CMI. Citing the Stockwire case, the magistrate noted that each time a defendant unlawfully posts an unauthorized work for distribution on the Internet, a single violation of the CMI provisions occurs for which a statutory damage award may be made. Here, the magistrate found that the defendant had extracted Stockart images into his logos and posted them on websites for sale a total of 34 times, resulting in 34 violations. The magistrate recommended that the district court award statutory damages of $10,000 per violation, for a total award of $340,000.[1185]

(viii) Nexon America v. Kumar

The plaintiff was the owner of a massively multiplayer online game called "MapleStory." The defendants operated a network of servers, websites and related products and services called "UMaple" that enabled users to copy, access, and play MapleStory. To play MapleStory on the defendants' servers, users were required to register for an account with UMaple and obtain a copy of the defendants' modified version of the MapleStory client (called "UMaple Launcher"), which bypassed the plaintiff's technical protection measures restricting access to MapleStory.[1186] Upon a default judgment against the defendants, the court considered the statutory damages award that the plaintiff was entitled to for violations of Section 1201 by trafficking in the UMaple Launcher. The court concluded that, because each UMaple member necessarily downloaded a copy of the UMaple Launcher, the number of UMaple members (17,938) was a reasonable approximation of the minimum number of DMCA trafficking violations the defendants had committed. The plaintiff sought the maximum amount of statutory damages, but the court rejected that request, observing from other reported cases that courts tend to award the statutory maximum only where doing so would not create a significant windfall for the plaintiff. Accordingly, the court chose the minimum statutory damages amount of $200 per violation, and awarded statutory damages in the total amount of $200 x 17,938 = $3,587,600.[1187]

(ix) Point 4 Data Corp. v. Tri-State Surgical Supply

In this case, the plaintiff Point 4 Data Corp. (Point 4), a distributor of a medical supply software system called Genesys, licensed the defendant Tri-State to use Genesys and a computer development platform called UniBasic on which Genesys operated. Because the

---

[1184] Stockart.com, LLC v. Engle, 2011 U.S. Dist. LEXIS 20470 at *3-6, 28-29.

[1185] Id. at *39-41. The magistrate also recommended a finding of willful infringement and an award of statutory damages under Section 504(b) for copyright infringement in the amount of $30,000 per infringed work. The magistrate based this recommendation on testimony that Stockart normally asked small businesses for a license fee of $10,000 for use of an image in a logo, and the majority of courts awarding statutory damages for willful infringement utilize a benchmark of two to three times the license fee for computing the award. Id. at *38.

[1186] Nexon American Inc. v. Kumar, 2012 U.S. Dist. LEXIS 47294 at *3-4, 15 (C.D. Cal. Apr. 3, 2012).

[1187] Id. at *15-20.

Genesys/UniBasic system repeatedly crashed, Tri-State began looking for a longer term solution to ensure that the system could operate following a server crash. Point 4 offered to upgrade Tri-State with the latest version of UniBasic and Genesys for $32,637, but Tri-State declined the offer and hired some consultants to repair the problem. The consultants loaded a copy of the Genesys/UniBasic system onto a spare computer and modified the UniBasic code in a way that bypassed the Genesys/UniBasic security system known as the Passport Licensing Security Software (Passport). Passport functioned to confirm that the computer user was running a proper and authenticated version of UniBasic and extracted information from a dongle concerning the number of authorized users. In the event there were licensing violations, such as an unauthorized number of users, Passport would display an error message and UniBasic would terminate execution. The modifications made by the consultants were such that each time a person logged on to UniBasic or Genesys, a script would run that bypassed Passport and its various checks.[1188]

A magistrate judge recommended a ruling that the bypassing of the Passport security system violated Section 1201. The plaintiffs sought both disgorgement of the defendants' profits and statutory damages. With respect to disgorgement under Section 1203(c)(2), which allows recovery of "any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages," the plaintiffs argued that, because Tri-State used the software in its daily business of selling medical supplies and surgical equipment, the entire amount of profits Tri-State earned in its business should be attributable to the software and, by extension the modifications thereto.[1189] The court rejected the plaintiffs' position, noting that were it to adopt the plaintiffs' view of what profits are "attributable" to a DMCA violation, it would ignore the plain language of Section 1203(c)(2) and "impermissibly blur the distinction between damages recoverable under the DMCA (in this case, those related to circumvention) and damages recoverable under the copyright statute (those related to use of the underlying protected works)."[1190]

Instead, the magistrate judge concluded that a DMCA plaintiff seeking to recover indirect profits under Section 1203(c)(2) must establish that the profits have a legally significant causal relationship to the DMCA violation – in this case, that the profits were attributable to the "cracking" of the Passport security system.[1191] "This limitation is especially warranted here, in light of the fact that the statute contains no provision shifting the burden of proof onto the defendant; under *section 1203(c)(2)*, the burden remains squarely on the plaintiff to establish the profits attributable to a DMCA violation."[1192] The court found that the plaintiffs had failed to show sufficient nexus between the circumvention and the defendants' profits. The court noted that it was undisputed that Tri-State was able to utilize the software and run its business without the crack, and had done so for many years, albeit with some hours of disruption following the

---

[1188] Point 4 Data Corp. v. Tri-State Surgical Supply & Equipment, Ltd., 2012 U.S. Dist. LEXIS 113791 at *3-10 (E.D.N.Y. June 13, 2012).

[1189] Id. at *14-16.

[1190] Id. at *17.

[1191] Id. at *26.

[1192] Id.

occasional server crash. The crack was simply the means by which Tri-State was able to avoid having to rely on its consultant to operate the software following a server crash. Accordingly, in the absence of proof of a link between the circumvention and revenue resulting from sales of Tri-State's medical and surgical equipment, the plaintiffs had not shown that all of Tri-State's profits were attributable to the crack.[1193]

The plaintiffs then offered three alternative theories for apportioning the defendants' profits. First, the plaintiffs claimed they were entitled to all profits derived from Tri-State invoices processed with Genesys. Second, they proposed that the court make percentage apportionments of profits based on the court's own evaluation of the qualitative contributions to revenues and profitability of Genesys and UniBasic in relation to the overall business. Third, the plaintiffs proposed subtracting from Tri-State's profits an estimate of what Tri-State's net income would have been had it processed orders by hand for a six month period and then switched to a different automated system. The court rejected these proposals on two grounds. First, each of the alternative theories was tied to profits that were calculated based on the *use* of the software, an approach the court found to be more appropriate to a copyright infringement claim. Second, the theories overlooked the fact that even absent the crack, Tri-State would have had the use of and access to the software. Accordingly, the court recommended granting Tri-State's motion for partial summary judgment as to any profits attributable to the crack, noting that the recommendation did not foreclose the plaintiffs from pursuing statutory damages, or as part of their actual damages, the reasonable licensing fee Tri-State avoided in implementing the crack.[1194]

The magistrate then turned to the plaintiffs' claim for statutory damages under Section 1203(c)(3)(A) for the circumventions accomplished by the crack. The plaintiffs argued that a separate, distinct act of circumvention took place each time a user logged into the modified system, because the crack functioned by launching a script when a user logged in that bypassed the Passport security system. The plaintiff therefore claimed that it was entitled to statutory damages based on 17,394 logins, carrying statutory damages ranging from a minimum of $3,478,800 to a maximum of $43,485,000. The defendants argued that, regardless of how the crack operated, the modification of the software was the only legally cognizable act of circumvention. The court reviewed the applicable precedent, and particularly the Stockwire case discussed above, and concluded that the plaintiffs' suggested approach was the correct one.[1195] "Here, after the Crack was implemented, it was Tri-State's employees, not third-party end-users, who then circumvented plaintiffs' software. Under these circumstances, the broad language of the statutory damages provision and the sparse precedent construing that provision support the conclusion that, assuming plaintiffs' version of the facts to be true, each user login gave rise to a separate 'act of circumvention.'"[1196] Accordingly, the magistrate recommended denial of Tri-

[1193] Id. at *26-29.

[1194] Id. at *31-34.

[1195] Id. at *35-42.

[1196] Id. at *42-43.

State's motion for partial summary judgment limiting statutory damages under the DMCA to a single act of circumvention.[1197]

The district court adopted the magistrate's recommendations in full.[1198] The district court noted in its opinion that it agreed with the magistrate's conclusion "that profits generated by use of a protected work subsequent to an act of circumvention are generally not disgorgeable under the DMCA. … [I]t would seem counterintuitive to hold that where the defendant accessed a protected work through an act of circumvention, a DMCA plaintiff may recover all the profits attributable to the defendant's use of that work, without bringing any claim for copyright infringement, even though the acts of use are not DMCA violations.""[1199] The court expressed no opinion whether, on similar facts, disgorgement might be appropriate if the plaintiffs could show that Tri-State used the crack to in fact exceed its prior user limit, and that new capability caused a demonstrable increase in Tri-State's sales and revenue. No such showing had been made here. The court also expressed the belief that, even if the DMCA could be interpreted to allow for disgorgement of profits generated through subsequent use of the protected material, the plaintiffs had not drawn an adequate connection between Tri-State's gross profits and the Genesys/UniBasic software or the crack – merely showing that the software was an important tool in the internal operations of Tri-State's business did not establish a sufficient causal connection under the DMCA.[1200] "Furthermore, the lack of a burden-shifting framework for apportioning profits under the DMCA suggests that a plaintiff has a more exacting duty than a copyright plaintiff to show a causal connection between the DMCA violations and the defendant's profits."[1201]

Finally, the district court noted that the plaintiffs had not objected to the magistrate's rejection of their alternative disgorgement theories, and the district court found no clear error in the magistrate's conclusions on those points. Similarly, no party had objected to the magistrate's recommendation regarding statutory damages, and finding no clear error, the court adopted the magistrate's conclusion that, on the facts accepted by both parties for purposes of the instant motion, each user log-in gave rise to a separate act of circumvention under Section 1203(c)(3). The court agreed with the magistrate's observation that this conclusion would not foreclose Tri-State from factually contesting how the crack operated or the total number of circumventions that occurred.[1202]

[1197] Id. at *50.

[1198] Point 4 Data Corp. v. Tri-State Surgical Supply & Equipment, Ltd., 2012 U.S. Dist. LEXIS 113997 (E.D.N.Y. Aug. 13, 2012).

[1199] Id. at *4.

[1200] Id. at *7-8, 12.

[1201] Id. at *9.

[1202] Id. at *14-15.

(x) Granger v. One Call Lender Services

In this case, the plaintiff was the owner of a computer program that estimated the rate or cost of real estate title insurance sold by title insurance agents. The defendants placed an infringing version of the rate calculator program on their website, though later took it down upon receipt of a demand letter from the plaintiff. The plaintiff had placed external copyright notices ("Copyright 1997-2002 by John Granger" and "All Rights Reserved") and the name of One Call Lender Services, LLC as web developer and author on the computer program, and had embedded within the computer program similar copyright tag lines and a watermark that, if not removed carefully, could leave a tell-tale sign as to the origin of the work. In posting the program onto their site, the defendants had removed these notices and the watermark. The court ruled that such removal violated the DMCA's CMI provisions on a motion for default judgment.[1203]

The plaintiff sought to recover a statutory damages award for the removal of each of the notices. The court rejected this request, ruling that the individual items of CMI that the defendants removed were immaterial. Citing Stockwire, the court noted that the number of violations of the CMI provisions was to be measured by the number of times the unauthorized product was posted on the Internet for distribution. Because the defendants had posted six different versions of the infringing rate calculator program onto the Internet (versions for six different states), the plaintiff was entitled to six awards of statutory damages. Because the plaintiff had sought only the minimum statutory damages award of $2,500 per violation, the court awarded statutory damages totaling $15,000.[1204]

(xi) Pacific Stock v. Macarthur & Co.

In this case, the defendant posted the plaintiff's photographic work on its website with the plaintiff's CMI on the work removed and false CMI inserted in its place. Upon a default judgment, the magistrate judge found that the plaintiff's actual damages from the defendant's act of copyright infringement were the license fee the plaintiff would have charged for the use of the work in the amount of $7,505. Noting that a statutory damages award under Section 1202 for the CMI violation should bear some relationship to actual damages, the magistrate judge recommended a statutory damages award of $10,000 under Section 1202 for the CMI violation, and a statutory damages award of $35,000 under Section 504(c)(1) for willful copyright infringement.[1205] The district court adopted the magistrate's recommendations and supporting opinion in full.[1206]

[1203] Granger v. One Call Lender Services, LLC, 2012 U.S. Dist. LEXIS 104885 at *2-4, 13 (E.D. Pa. July 26, 2012).

[1204] Id. at *13-14. The court also awarded statutory damages of $12,000 for copyright infringement. The court rejected the plaintiff's claim that it should be entitled to a statutory damages award for each infringing derivative work the defendants had created – i.e., versions of the program for New Jersey, Maryland, Florida, Indiana, and Virginia. "Plaintiff is entitled to recover for only one work since Defendants only infringed upon Plaintiff's single Rate Calculator, and all remaining calculators were merely derivative works of the Rate Calculator." Id. at *8-10.

[1205] Pacific Stock, Inc. v. MacArthur & Co., 2012 U.S. Dist. LEXIS 128258 at *413-16 (D. Haw. Sept. 10, 2012).

[1206] Pacific Stock, Inc. v. MacArthur & Co., 2012 U.S. Dist. LEXIS 142449 (D. Haw. Oct. 2, 2012).

(2) Jurisdictional Issues – Blueport Co. v. United States

In Blueport Co. v. United States,[1207] the Court of Claims ruled that the United States cannot be sued under the DMCA's anti-circumvention provisions because the DMCA contains no clear waiver of sovereign immunity, and waiver under the DMCA could not be inferred from waiver under the copyright laws because the DMCA is not a copyright statute. The Federal Circuit affirmed this ruling on appeal for the same reasons invoked by the Court of Claims, and also noted the rule that the Court of Claims lacks jurisdiction to adjudicate claims created by statutes, like the DMCA, which specifically authorized jurisdiction in the district courts.[1208]

(d) Alternative Approaches to the DMCA That Did Not Pass

Two of the alternatives bills that were introduced to implement the WIPO treaties which did not pass, S. 1146 and H.R. 3048, would have prohibited only certain defined circumvention conduct, rather than devices. Specifically, Section 1201 of S. 1146 and H.R. 3048 provided that no person, "for the purpose of facilitating or engaging in an act of infringement, shall engage in conduct so as knowingly to remove, deactivate or otherwise circumvent the application or operation of any effective technological measure used by a copyright owner to preclude or limit reproduction of a work or a portion thereof." Thus, these bills would not have banned circumvention undertaken for reasons other than facilitating or engaging in infringement, such as fair uses. In addition, Section 1201 of these bills expressly defined "conduct" not to include manufacturing, importing or distributing a device or a computer program.

Although Section 1201(a) of these bills referred only to technological measures used to preclude or limit reproduction of a copyrighted work, and did not refer to access to a copyrighted work (as is included in the DMCA), the definition of "effective technological measure" in Section 1201(c) of these bills included two references to access. Specifically, "effective technological measure" was defined as information included with or an attribute applied to a transmission or a copy of a work in a digital format which "encrypts or scrambles the work or a portion thereof in the absence of access information supplied by the copyright owner; or includes attributes regarding access to or recording of the work that cannot be removed without degrading the work or a portion thereof." This was a much more specific and narrower definition of effective technological measure than that contained in the DMCA.

Unlike Section 1201, Section 1202 of S. 1146 and H.R. 3048 was largely identical to Section 1202 of the DMCA with respect to removal, alteration or falsification of CMI. The most important difference was that Section 1202 of S. 1146 and H.R. 3048 contained language making clear that the conduct governed by that Section did not include the manufacturing, importing or distributing of a device (curiously, there was no reference to a computer program, as there was in the exclusion from Section 1201 of those bills).

[1207] 80 U.S.P.Q.2d 1585 (Ct. Fed. Claims 2006).

[1208] Blueport Co. v. United States, 533 F.3d 1374, 1382-84 (Fed. Cir. 2008).

(e) The Battle Between Content Owners and Technology Companies Over Built-In Technological Measures

A growing battle has been developing in recent years between holders of copyright on content, most notably the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), and technology companies over whether manufacturers of devices that can be used to play, copy or distribute copyrighted content should be required to build in to such devices technological protection measures that restrict access to or the use of such copyrighted content. In effect, content owners have sought through various proposed federal legislation to mandate the inclusion of technological measures in devices that would be covered by the anti-circumvention provisions of the DMCA. Computer, consumer electronic, and other technology companies have resisted such legislation mightily, arguing that they must be free to design their own products without legislative strictures.

On Jan. 14, 2003, the RIAA, the Business Software Alliance (BSA),[1209] and the Computer Systems Policy Project (CSPP)[1210] announced that they had reached agreement on a core set of seven principles to guide their public policy activities in the 108th Congress (2003) regarding the distribution of digital content.[1211] Pursuant to the agreement, the recording companies agreed that they would not seek government intervention to mandate technical solutions to prevent digital piracy and would in most instances oppose legislation that would require computers and consumer electronics devices to be designed to restrict unauthorized copying of audio and video material. In turn, the BSA and CSPP would not support legislation that seeks to clarify and bolster the rights of persons to use copyrighted material in digital format. Notably absent from the agreement were consumer electronics companies, who felt that legislation was needed to ensure that consumers can make fair use of digital copyrighted material even when secured with technology to prevent illegal copying, and the MPAA, whose members continued to be concerned that digital television broadcasts and movies copied from DVDs would soon be traded over the Internet in high volumes.[1212]

2. Anticircumvention Provisions Under the European Copyright Directive

The European Copyright Directive adopts the approach of the DMCA, in that it would outlaw both conduct and the manufacture or distribution of devices that could be used to defeat technological copyright protections. With respect to conduct, Article 6(1) provides that member states "shall provide adequate legal protection against the circumvention of any effective

---

[1209] Members of the BSA include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC/Mastercam, Dell, Entrust, HP, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, Novell, PeopleSoft, SeeBeyond, Sybase, and Symantec. "Recording, Technology Industries Reach Groundbreaking Agreement on Approach to Digital Content Issues," available on the BSA web site as of Jan. 15, 2003 at www.bsa.org/usa/press/newsreleases//2003-01-14.1418.phtml.

[1210] Members of the CSPP include Dell, Intel, HP, Motorola, NCR, IBM, EMC, and Unisys. Id.

[1211] The seven policy principles may be found on the BSA web site at www.bsa.org/usa/policyres/7_principles.pdf.

[1212] Amy Harmon, "Music Industry Won't Seek Government Aid on Piracy" (Jan. 15, 2003), available as of Jan. 15, 2003 at www.nytimes.com/2003/01/15/business/15PIRA.html.

technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective."[1213] The language of Article 6(1) includes a knowledge requirement that is not expressly present in the prohibition of Section 1201(a)(1)(A) of the DMCA. But unlike the DMCA, there are no enumerated exceptions to the ban on circumvention in the European Copyright Directive.[1214]

Like the DMCA, the European Copyright Directive does not require that the circumvention of the technical measures be done for the purpose of facilitating or engaging in an act of infringement. However, the commentary to Article 6 elaborates on the requirement of knowledge by the party liable for the circumvention in a way that suggests a standard of liability that may be somewhat akin to that of the Sony case in the United States: "This [requirement of knowledge] would allow for the necessary flexibility – a fundamental element for the industry – not to cover activities which are related to devices which may serve a legal or illegal use and are carried out without the actual knowledge that they will enable circumvention of technological protection devices."[1215] It remains to be seen how broadly this provision will be implemented by member states.

With respect to the manufacture or distribution of devices that could be used to defeat technological copyright protections, Article 6(2) provides that member states "shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

---

[1213] Notwithstanding the general prohibition on circumvention of effective technological measures, Article 6(4) provides that, "in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned."

[1214] Schollenberger, supra note 207, at 12. The European Copyright Directive attempts to deal with this issue via Article 6(4), which states that "Member States should promote voluntary measures taken by right holders, including the conclusion and implementation of agreements between rights holders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided for in national law." It further states that in the absence of such voluntary measures or agreements, within a reasonable period of time Member States are obliged to take appropriate measures to ensure that right holders provide beneficiaries of such exceptions or limitations with "appropriate means" of benefiting from them, by modifying an implemented technological protection measure or by other means. What such "appropriate measures" would be remains unclear. Id.

[1215] Commentary to Art. 6, ¶ 2.

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures."

The foregoing three criteria are very similar to the criteria enumerated in the prohibition of technology, devices and services contained in Sections 1201(a)(2) and 1201(b) of the DMCA. However, by prohibiting preparatory activities to circumvention, Article 6(2) goes further than the WIPO Copyright Treaty requires.[1216]

One possible difference between the European Copyright Directive and the DMCA may lie in the scope of what types of technological measures are prohibited from circumvention. Specifically, the prohibitions of the DMCA are expressly directed toward technology, devices and services that circumvent technological measures that effectively *control access* to a copyrighted work and *protect rights of a copyright holder*. By contrast, the definition of "technological measures" in the European Copyright Directive, at first glance, seems directed only toward protecting rights of a copyright holder, and not restricting access. Article 6(3) defines the expression "technological measures" to mean "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC."

However, the concept of access control seems to come into the European Copyright Directive indirectly, through the definition of "effective." Specifically, Article 6(3) provides that technological measures shall be deemed "effective" where "the use of a protected work or other subject-matter is controlled by the rightholders through application of an *access control* or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective" (emphasis added). Thus, through the interaction of these definitions of "technological measures" and "effective," it appears that the European Copyright Directive effectively prohibits the circumvention of technological measures that both control access and that protect the rights of a copyright holder, just as does the DMCA.

An important thing to note is that the anti-circumvention provisions of Article 6 of the European Copyright Directive do not apply to computer programs. Instead, a different, and more limited, set of anti-circumvention provisions apply to computer programs under Directive 91/250/EEC on the Legal Protection of Computer Programs (the "European Software Directive"), discussed in the next paragraph. Article 2(a) of the European Copyright Directive states that the "Directive shall leave intact and shall in no way affect existing Community provisions relating to the legal protection of computer programs." And Recital 50 of the European Copyright Directive states that its harmonized legal protection "does not affect the specific provisions on protection provided for by Directive 91/250/EEC [the European Software

[1216] Harrington & Berking, supra note 206, at 6.

Directive]. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive."

The narrower anti-circumvention provisions applicable to computer programs are set forth in Article 7(1)(c) of the European Software Directive, which requires member states to provide appropriate remedies against "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program." There are a couple of important distinctions between the anti-circumvention provisions of the European Software Directive and those of the European Copyright Directive:

-- The anti-circumvention provisions of the European Software Directive are aimed at preventing the manufacture and distribution of circumvention devices. Unlike the relevant provisions of the European Copyright Directive, they do not prohibit the actual conduct of circumvention itself.

-- The anti-circumvention provisions of the European Software Directive apply only to devices that have circumvention as their sole intended purpose, which is narrower than the anti-circumvention provisions of the European Copyright Directive that apply to devices that have circumvention as their primary purpose, or are promoted, advertised or marketed for the purpose of circumvention, or have only a limited commercially significant purpose or use other than to circumvent.

Article 7(1) of the European Copyright Directive deals with CMI, which the European Copyright Directive denominates "electronic rights management information." Specifically, Article 7(1) requires member states to prohibit any person knowingly performing without authority any of the following acts:

> "(a) the removal or alteration of any electronic rights-management information;
>
> (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic right-management information has been removed or altered without authority,
>
> if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the *sui generis* right provided in Chapter III of Directive 96/9/EC."

Article 7(2) defines "rights management information" broadly to mean "any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information. The first

subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC."

The scope of Article 7 is potentially narrower than that of the United States implementing legislation. The prohibitions of Article 7(1) are all expressly directed to "electronic" rights-management information. In addition, the commentary states that Article 7 "aims only at the protection of electronic rights management information, and does not cover all kinds of information that could be attached to the protected material."[1217] By contrast, the definition of CMI under the DMCA is broad enough to cover more than just electronic information.

3. Anti-Circumvention Provisions in Other Foreign Countries

Some countries outside the European Union have adopted anti-circumvention provisions in their copyright laws. For example, effective March 2001 Australia added a new Section 116A to its copyright law, which prohibits circumvention of a "technological protection measure," defined as "a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject-matter."[1218] In October of 2005, the High Court of Australia unanimously ruled that distributing mod chips to overcome region coding on the PlayStation video games was not a violation of Section 116A. The court reasoned that the region coding scheme did not constitute a technological protection measure.[1219]

In July of 2003, the Federal Court of Australia held that region access codes in CD-ROMs of PlayStation games, as well as a companion chip in the PlayStation console, constituted a valid "technological protection measure," and that the defendant had violated Section 116A by distributing modification chips that overcame the regional restrictions on play of the games.[1220]

In March of 2005, a German court, on the basis of the anti-circumvention provision of German copyright law, prohibited the German news site Heise from linking in an online article to a site where circumvention software was made available.[1221]

[1217] Commentary to Art. 7, ¶ 1.

[1218] "Australian Federal Court Upholds Region Coding Restrictions on Video Game System," *BNA's Electronic Commerce & Law Report* (Aug. 20, 2003) at 802.

[1219] Murray Griffin, "Fair Use Ruling on TPMs Raises Concern That Australian Law May Conflict with FTA," *BNA's Electronic Commerce & Law Report* (Oct. 12, 2005) at 982.

[1220] Id.

[1221] "Court Prohibits Linking to Circumvention Software" (Mar. 7, 2005), available as of Mar. 8, 2005 at http://constitutionalcode.blogspot.com/2005/03/court-prohibits-linking-to.html.

4. Fair Use

(a) United States Legislation That Did Not Pass

Both S. 1146 and H.R. 3048 – neither of which were ultimately adopted by Congress – contained identical provisions with respect to application of the fair use doctrine in a digital environment. These bills would have amended Section 107 of the copyright statute (the fair use exemption) in two ways. First, they would have added an amendment providing that the fair use doctrine applies to uses of a copyrighted work "by analog or digital transmission." Second, they would have added a new sentence to Section 107 providing that, in making a determination concerning fair use, a court should give no independent weight to the means by which the work has been performed, displayed or distributed under the authority of the copyright owner, or the application of an effective technological measure to protect the work. The import of this provision appears to have been (i) to clarify that digital uses of a copyrighted work may be a fair use notwithstanding that the copyright owner has authorized use of the work only in other media or modes and (ii) that the fair use exemption may apply even if an effective technological measure must be circumvented to use the work (as in the case of reverse engineering). However, as discussed above, both the RealNetworks and the Reimerdes cases held that fair use is not a defense to a claim for violation of the anti-circumvention provisions of Section 1201(a); thus, the fact that a defendant circumvented a technological protection measure in order to gain access to a copyrighted work to make fair uses of it does not provide a defense.

(b) The European Copyright Directive

Article 5(3) of the European Copyright Directive permits member states to adopt limitations to the rights of reproduction and of communication or making available to the public for the following fair use purposes:

– for illustration for teaching or scientific research for noncommercial purposes, as long as the source, including the author's name, is indicated;

– for the benefit of people with a disability, which are directly related to the disability and of a noncommercial nature, to the extent required by the specific disability;

– use of short excerpts in connection with the reporting of current events, so long as the source, including the author's name, is indicated;

– quotations for purposes such as criticism or review of a work that has been lawfully made available to the public, so long as the source, including the author's name, is indicated and the use is in accordance with fair practice;

– for public security or proper performance of an administrative or judicial procedure;

– use of political speeches or public lectures to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated;

– use during public religious or official celebrations;

– use of works of architecture or sculpture made to be located permanently in public places;

– incidental inclusion of a work in other material;

– use for advertising the public exhibition or sale of artistic works to the extent necessary to promote the event;

– use for caricature, parody or pastiche;

– use in connection with the demonstration or repair of equipment;

– use of an artistic work in the form of a building or a drawing or plan of a building for reconstructing the same;

– use by communication or making available to individual members of the public by dedicated terminals in publicly accessible libraries, educations establishments, museums or archives for noncommercial purposes; and

– use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that concern only analog uses and do not affect the free circulation of goods and services within the EC.

Article 5(5) provides that in all cases, the limitations "shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

5. Expansion of Library/Archives Exemptions

Section 404 of the DMCA expands the scope of the exemption in Section 108 of the copyright statute for libraries and archives. Specifically, Section 108 authorizes libraries and archives to make three copies of works for preservation purposes, rather than one. Section 108 also deletes the requirement that the copies be made "in facsimile form." According to Rep. Boucher, this phrase in the pre-amended version of Section 108 had been read to preclude the use of digital technologies to preserve works.[1222] Under the amended Section 108, a work may be copied for preservation purposes if it is currently in the collections of the library or archives and, if reproduced in digital format, it is not otherwise distributed in that format and is not made available to the public in that format outside the premises of the library or archives.

6. Distance Education

Section 403 of the DMCA requires that, within six months after enactment, the Register of Copyrights submit to Congress recommendations on how to promote distance education through digital technologies, including interactive digital networks, while maintaining an

[1222] "Latest Copyright Treaty Implementation Bill Limits Scope of Shrink-Wrap Agreements," *BNA's Electronic Information Policy & Law Report* (Nov. 26, 1997) at 1232.

appropriate balance between the rights of copyright owners and the needs of users of copyrighted works. The DMCA lists a number of factors that should be considered in making such recommendations.[1223]

7. Copying in the Course of Computer Maintenance or Repair

Title III of the DMCA added a new subsection to Section 117 of the copyright statute, providing that it is not an infringement for an owner or lessee of a machine to make or authorize the making of a copy of a computer program if such copy is made solely by virtue of the activation of a machine that lawfully contains an authorized copy of the program, for purposes only of maintenance or repair of that machine, provided the copy is used in no other manner and is destroyed immediately after the maintenance or repair is completed, and, with respect to any computer program or portion thereof that is not necessary for that machine to be activated, such is not accessed or used other than to make the new copy by virtue of the activation of the machine.

This amendment to the copyright statute was deemed necessary by its sponsors in view of judicial decisions such as MAI Systems Corp. v. Peak Computer,[1224] discussed above, and Triad Sys. v. Southeastern Express Co.,[1225] which held that copying portions of a computer program to memory in the course of turning on and running the machine constitutes a "reproduction" under Section 106 of the copyright statute. Under these decisions, a service technician who is not the owner or licensee of the system software commits copyright infringement by even booting up the machine for maintenance or repair. The revisions to Section 117 made by the DMCA change this result. In Telecomm Technical Services Inc. v. Siemens Rolm Communications, [1226] the court ruled that this provision is to be applied retroactively.

[1223] The factors include: The need for an exemption from exclusive rights of copyright owners for distance education through digital networks; the categories of works to be included under the exemption; the extent of appropriate quantitative limitations on the portions of works that may be used under the exemption; the parties who should be entitled to the benefits of the exemption; the parties who should be designated as eligible recipients of distance education materials under the exemption; whether and what types of technological measures can or should be employed as a safeguard against unauthorized access to and use or retention of copyrighted materials as a condition of eligibility for any exemption; and the extent to which the availability of licenses for the use of copyrighted works in distance education through interactive digital networks should be considered in assessing eligibility for the exemption.

Both S. 1146 and H.R. 3048 would have afforded a broader expansion of the exemptions in Section 110(2) of the copyright statute for certain performances or displays of copyrighted works for instructional activities performed by government or nonprofit educational institutions. The bills would have extended this exemption to distributions of a work, in addition to performances and displays, to cover the distribution of a work over a computer network. The bills would also have expanded the exemption from nondramatic literary or musical works to all works, and extended the exemption to apply to students officially enrolled in the course, not only courses held in a classroom.

[1224] 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

[1225] 64 F.3d 1330 (9th Cir. 1995), cert. denied, 116 S. Ct. 1015 (1996).

[1226] No. 1:95-CV-649-WBH (N.D. Ga. July 6, 1999).

The scope of the computer maintenance and repair right was construed very broadly in the case of Storage Technology Corporation v. Custom Hardware Engineering & Consulting, discussed in Section II.G.1(a)(14)(iv) above.

8. Other Provisions of the DMCA

The DMCA contains the following other miscellaneous provisions:

(a) Evaluation of Impact of Copyright Law on Electronic Commerce

Section 104 of the DMCA requires the Register of Copyrights and the Assistant Secretary for Communications and Information of the Commerce Department to study and report to Congress within two years of enactment of the DMCA with respect to the DMCA's impact on "the development of electronic commerce and associated technology," and "the relationship between existing and emergent technology" and Sections 109 and 117 of the copyright statute. The report required under Section 104 was issued in August of 2001 and is available online at www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.

In a nutshell, the executive summary of the report concludes, "We are not persuaded that title I of the DMCA has had a significant effect on the operation of sections 109 and 117 of title 17. The adverse effects that section 1201, for example, is alleged to have had on these sections cannot accurately be ascribed to section 1201. The causal relationship between the problems identified and section 1201 are currently either minimal or easily attributable to other factors such as the increasing use of license terms. Accordingly, none of our legislative recommendations are based on the effects of section 1201 on the operation of sections 109 and 117."[1227]

The report does, however, recommend two legislative changes: (i) that the copyright statute be amended "to preclude any liability arising from the assertion of a copyright owner's reproduction right with respect to temporary buffer copies that are incidental to a licensed digital transmission of a public performance of a sound recording and any underlying musical work"[1228] and (ii) that Congress "either (1) amend section 109 to ensure that fair use copies are not subject to the first sale doctrine or (2) create a new archival exemption that provides expressly that backup copies may not be distributed."[1229] The recommendation with respect to temporary buffer copies is discussed further in Section III.E.4(b) below.

(b) Clarification of the Authority of the Copyright Office

Section 401 of the DMCA clarifies the authority of the Copyright Office. Specifically, it provides that, in addition to the functions and duties of the Register of Copyrights already enumerated in the copyright statute, the Register shall perform the following functions: (1)

[1227] The quoted language is from the opening paragraph of Section III of the Executive Summary of the report. The Executive Summary may be found at www.loc.gov/copyright/reports/studies/dmca/dmca_executive.html.

[1228] Id. section III.b.2.c.

[1229] Id. section III.b.3.b.

Advise Congress on national and international issues relating to copyright; (2) Provide information and assistance to federal departments and agencies and the judiciary on national and international issues relating to copyright; (3) Participate in meetings of international intergovernmental organizations and meetings with foreign government officials relating to copyright; and (4) Conduct studies and programs regarding copyright, including educational programs conducted cooperatively with foreign intellectual property offices and international intergovernmental governments.[1230]

(c) Ephemeral Recordings

Section 402 of the DMCA expands the rights under Section 112 of the copyright statute of broadcast radio or television stations licensed by the FCC to make ephemeral recordings of material transmitted via analog broadcasts to include recordings of a performance of a sound recording in digital format on a non-subscription basis. This expansion of the ephemeral recording right was made necessary by the Digital Performance Right in Sound Recordings Act of 1995, which granted sound recording copyright owners the exclusive right to publicly perform their works by means of digital audio transmissions.

Section 402 responds to Congress' concern, expressed in the Conference Report, that if use of copy protection technologies becomes widespread, a transmitting organization might be prevented from engaging in its traditional activities of assembling transmission programs and making ephemeral recordings permitted by Section 112 of the copyright statute. Accordingly, Section 402 provides that where a transmitting organization entitled to make an ephemeral recording is prevented from making such recording by the application by the copyright owner of a technical measure that prevents reproduction of the work, the copyright owner must make available to the transmitting organization the necessary means for making the recording, if it

---

[1230] This provision is the outcome of a skirmish that developed between Bruce Lehman, the former Commissioner of Patents & Trademarks and Mary Beth Peters, the Register of Copyrights. Commissioner Lehman was pushing for creation of a new position of Under Secretary of Commerce for Intellectual Property Policy, or what some referred to as an "intellectual property czar." Under a proposed provision that did not pass Congress, the duties of the new position would have been to: (1) Promote exports of goods and services of the United States industries that rely on intellectual property; (2) Advise the President, through the Secretary of Commerce, on national and certain international issues relating to intellectual property policy, including issues in the areas of patents, trademarks, and copyrights; (3) Advise Federal departments and agencies on matters of intellectual property protection in other countries; (4) Provide guidance, as appropriate, with respect to proposals by agencies to assist foreign governments and international intergovernmental organizations on matters of intellectual property protection; (5) Conduct programs and studies related to the effectiveness of intellectual property protection throughout the world; (6) Advise the Secretary of Commerce on programs and studies relating to intellectual property policy that are conducted, or authorized to be conducted, cooperatively with foreign patent and trademark offices and international intergovernmental organizations; and (7) In coordination with the Department of State, conduct programs and studies cooperatively with foreign intellectual property offices and international intergovernmental organizations.

The effect of this provision would have been to vest responsibility for public policy issues relating to copyright (as well as trademarks and patents) in the new position, relegating the Copyright Office to a largely administrative role primarily related to registration of copyrights. The Copyright Office was obviously opposed to this, and appears to have been the victor of the skirmish, for Section 401 makes clear that responsibility for public policy issues relating to copyright lies with the Copyright Office, led by the Register of Copyrights.

technologically feasible and economically reasonable to do so. If the copyright owner fails to do so in a timely manner, then the transmitting organization is granted an exemption from liability under the provisions of the DMCA that would otherwise prohibit the transmitting organization from circumventing the technical measure.

(d) Statutory Licenses With Respect to Performances of Sound Recordings

Section 405 of the DMCA contains provisions relating to statutory compulsory licenses with respect to performances of sound recordings, including digital audio transmissions, and sets up procedures for voluntary negotiation proceedings to determine reasonable terms and rates of royalty payments for public performances of sound recordings. According to the Conference Report, Section 405 was intended to achieve two purposes: first, to further a stated objective of Congress when it passed the Digital Performance Right in Sound Recordings Act of 1995 to ensure that recording artists and record companies will be protected as new technologies affect the ways in which their creative works are used; and second, to create fair and efficient licensing mechanisms that address the complex issues facing copyright owners and copyrights users as a result of the rapid growth of digital audio services.[1231] The details of these provisions, which are lengthy and quite complex, are beyond the scope of this paper.

(e) Assumption of Contractual Obligations Related to Transfers of Rights in Motion Pictures

Section 406 of the DMCA adds a new Section 4001 to Title 28 of the United States Code to address the problem caused by the failure of motion picture producers to obtain, as part of a collective bargaining agreement, assumption agreements from distributors to make residual payments. New Section 4001 provides generally that transfers of copyright ownership not limited to public performance rights by exhibitors in motion pictures produced subject to a collective bargaining agreement will be subject to the assumption agreements applicable to the copyright ownership being transferred that are required by the applicable collective bargaining agreement, provided that the transferee knows or has reason to know at the time of the transfer of the collective bargaining agreement, or, in the event of a court order confirming an arbitration award against the transferor under the collective bargaining agreement, the transferor does not have the financial ability to satisfy the award within 90 days after the order is issued. Security interests and transfers related to exercise of security interests in such motion pictures are exempted from the provisions of Section 4001.

(f) Protection of Certain Industrial Designs

Title V of the DMCA adds a new Chapter 13 to the copyright statute entitled "Protection of Original Designs." Although as currently enacted, Chapter 13 protects only vessel hull

[1231] Id. at 79-80.

designs[1232] with a copyright-like design right, its provisions are drafted in the form of a general industrial design protection statute. Merely by changing a definition in the statute, Congress can in the future easily extend the scope of industrial designs that are protected. To obtain protection, the statute requires that the owner of the design register the design with the Copyright Office within two years of making the design public as embodied in a useful article. Title V of the DMCA originally provided that the design protection statute would be effective for an initial trial period of two years. However, Section 5005(a)(2) of the Intellectual Property and Communications Omnibus Reform Act of 1999[1233] deleted this two-year sunset provision.

(1) Protection of Designs Embodied in Useful Articles

Section 1301(a) of the statute provides generally that the "designer or other owner of an original design of a useful article which makes the article attractive or distinctive in appearance to the purchasing or using public may secure the protection provided by this chapter upon complying with and subject to this chapter." Section 1301(b)(2) defines a "useful article" as a "vessel hull or deck,[1234] including a plug or mold, which in normal use has an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information. An article which normally is part of a useful article shall be deemed to be a useful article." It is apparent that, although this definition is currently limited to vessel hulls and decks, the phrase "vessel hull or deck" in the definition could easily be replaced with a generic phrase such as "article," thereby extending protection to general industrial designs. Alternatively, enumerated categories of designs in addition to vessel hulls or decks could easily be added to the definition.

(2) Originality

The statute establishes a low threshold of originality for protection. Specifically, Section 1301(b)(1) provides that a design is original "if it is the result of the designer's creative endeavor that provides a distinguishable variation over prior work pertaining to similar articles which is more than merely trivial and has not been copied from another source." Although this is a low threshold, it is interesting to note that it is a higher threshold than under copyright law. Specifically, under copyright law a work of authorship is deemed original if it is simply not copied from another work, whether or not it embodies a distinguishable variation from prior works. Thus, two photographers could take identical photos from the edge of the Grand Canyon

---

[1232] Title V overrules Bonita Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989), in which the Supreme Court barred states from protecting unpatented boat hulls because such protection conflicts with the federal policy favoring free competition in inventions not qualifying for patent protection.

[1233] P.L. 106-113 (1999).

[1234] Section 1301(b)(3), as amended by Section 5005(a)(2) of the Intellectual Property and Communications Omnibus Reform Act of 1999, P.L. 106-113, defines a "vessel" as "a craft--(A) that is designed and capable of independently steering a course on or through water through its own means of propulsion; and (B) that is designed and capable of carrying and transporting one or more passengers." Under Section 1301(b)(4), as amended by the Vessel Hull Design Protection Amendments of 2008, P.L. 110-434, a "hull" is "the exterior frame or body of a vessel, exclusive of the deck, superstructure, masts, sails, yards, rigging, hardware, fixtures, and other attachments" and a "deck" is "the horizontal surface of a vessel that covers the hull, including exterior cabin and cockpit surfaces, and exclusive of masts, sails, yards, rigging, hardware, fixtures, and other attachments."

by standing in the same places, and each would produce an "original," and therefore copyrightable, photo. By contrast, under the design statute, a second designer who, as a result of independent development, happens to produce a design the same as a preexisting design, has not created an "original" design.

(3) Exclusions from Protection

Section 1302 excludes protection for a design that is:

> (1) not original;
>
> (2) staple or commonplace, such as a standard geometric figure, a familiar symbol, an emblem, or a motif, or another shape, pattern, or configuration which has become standard, common, prevalent, or ordinary;
>
> (3) different from a design excluded by clause (2) only in insignificant details or in elements which are variants commonly used in the relevant trades;
>
> (4) dictated solely by a utilitarian function of the article that embodies it;[1235] or
>
> (5) embodied in a useful article that was made public by the designer or owner anywhere in the world more than two years[1236] before registering the design with the Copyright Office.[1237] (Under Section 1310(b), a design is "made public" when an existing useful article embodying the design "is anywhere publicly exhibited, publicly distributed, or offered for sale or sold to the public by the owner of the design or with the owner's consent.")

(4) Adaptations of Unprotectable Elements

Section 1303 provides that a design employing elements not protectable under Section 1302 may nevertheless be protected if such design is a substantial revision, adaptation, or rearrangement of such unprotectable elements.

[1235] Section 1301(a)(2), as amended by the Vessel Hull Design Protection Amendments of 2008, P.L. 110-434, provides, "The design of a vessel hull, deck, or combination of a hull and deck, including a plug or mold, is subject to protection under this chapter, notwithstanding section 1302(4)."

[1236] Section 1302(5) as originally published at 112 Stat. 2906 reads "1 year" at this point in clause (5). However, this is apparently an error, for Section 1310(a) states that protection shall be lost "if application for registration of the design in not made within *2 years* after the date on which the design is first made public" (emphasis added).

[1237] Under the provisions of Section 1310, the registration of a design requires, among other things, the specific name of the useful article embodying the design, and two copies of a drawing or other pictorial representation of the useful article having one or more views adequate to show the design in a form and style suitable for reproduction. Section 1310(i) provides that when a design is embodied in more than one useful article, the design is protected as to all useful articles when protected as to one of them, but only one registration is required for the design. Section 1313(c) sets up certain procedures by which a registered design may be challenged and canceled. Under Section 1314, a registration constitutes prima facie evidence of the facts stated in the registration certificate.

(5) Duration of Protection and Design Notice

Protection commences on the earlier of the date of publication of the design's registration or its first being made public, and lasts for a term of ten years (including through the end of the calendar year of the tenth year). Section 1306 requires designs that have been made public to bear a design notice comprised of the words "Protected Design," the abbreviation "Prot'd Des.," or the letter "D" with a circle or the symbol "*D*"; the year of the date on which protection commenced; and the name of the owner or a recognized abbreviation or alternative name. After registration, the registration number may be used in the design notice in lieu of the second and third notice elements enumerated above. Under Section 1307, omission of the notice does not invalidate protection, but prevents any recovery of damages against an infringer until the infringer has notice of the design rights, and no injunction may issue against such infringer unless the owner reimburses the infringer for any reasonable expenditure or contractual obligation incurred before receiving notice.

(6) Rights of a Design Owner and Limitations

Under Section 1308, the owner of a protected design has the exclusive right to make, have made, or import, for sale or for use in trade, any useful article embodying the design, and to sell or distribute for sale or for use in trade any useful article embodying the design. Section 1309 places a number of limitations on who may be deemed infringers, however:

> -- First, under Section 1309(b), a seller or distributor who did not make or import an infringing article is itself deemed an infringer only if (i) the seller or distributor induced or acted in collusion with a manufacturer or importer (other than by merely placing an order for the infringing articles) or (ii) failed to make a prompt and full disclosure of its source of the infringing article upon request of the design owner, and the seller or distributor orders or reorders the infringing articles after receiving notice by registered or certified mail that the design is protected.
>
> -- Second, a person who makes, has made, imports, sells or distributes an article embodying an infringing design which was created without such person's knowledge that the design was protected and was copied from the protected design.
>
> -- Third, a person who incorporates into that person's product of manufacture an infringing article acquired from another in the ordinary course of business or who, without knowledge of the protected design embodied in an infringing article, makes or processes the infringing article for the account of another in the ordinary course of business, is not an infringer, except to the extent such person would be deemed an infringer under the seller/distributor provisions above.

(7) Standard of Infringement

Under Section 1309(a), to establish infringement, a design owner must prove that an "infringing article" has been made, imported, sold or distributed without the design owner's

consent. Section 1309(e) defines an "infringing article" as one embodying a design that was "copied" from a protected design, and provides that an infringing article "is not an illustration or picture of a protected design in an advertisement, book, periodical, newspaper, photograph, broadcast, motion picture, or similar medium." The statute does not directly define what it means to "copy" a design. However, Section 1309(e) provides, "A design shall not be deemed to have been copied from a protected design if it is original and not substantially similar in appearance to a protected design."[1238] Strictly speaking, this provision enumerates only one way in which an alleged infringer can rebut an allegation of copying, and it does not state that this is the only way. However, it is unclear what happens when an accused design is, by coincidence, substantially similar to a protected design but can be shown to have been independently developed. Such a showing of independent development would be sufficient to avoid liability under copyright law, and it seems logical that it should be sufficient to prove that the design was not "copied" under the design statute as well.

(8) Benefit of Foreign Filing Date

Under Section 1311, an applicant for registration of a design in the United States can claim the benefit of an earlier filing date in a foreign country for registration of the same design if (i) the foreign country extends similar design protection to citizens of the United States, and (ii) the application is filed in the United States within six months after the earliest date on which any such foreign application was filed.

(9) Vesting and Transfer of Ownership

Under Section 1320, design rights vest in the creator of the design, or, in the case of a design made within the regular scope of the designer's employment, in the employer. Property rights in a design may be assigned or mortgaged by an instrument in writing, and any such conveyance is void as against a subsequent purchaser or mortgagee for valuable consideration unless it is recorded in the Copyright Office within three months after its execution or before the date of such subsequent purchase or mortgage.

(10) Remedies of Injunctive Relief, Damages, Attorneys' Fees and Destruction

Section 1322 permits a court to award preliminary and permanent injunctive relief against infringement of protected designs. Under Section 1323(a), the owner of a protected design may recover "damages adequate to compensate for the infringement," but the damages awarded "shall constitute compensation and not a penalty." Section 1323(a) permits the court to increase the damages to such amount, not exceeding $50,000 or $1 per copy, whichever is greater, as the court deems just. As an alternative, under Section 1323(b), the court may award the owner of the

[1238] It is unclear what the relationship is between the standard of "substantially similar" for infringement purposes and the standard of "distinguishable variation" (in the definition of "original") for purposes of protectability. However, Section 1309(f) provides that if an accused infringer introduces an earlier work which is identical to an allegedly protected design or so similar as to make a prima facie showing that such design was copied, then the burden shifts to the owner of the allegedly protected design to prove its originality.

protected design the infringer's profits resulting from the sale of the infringing copies "if the court finds that the infringer's sales are reasonably related to the use" of the protected design. The owner is required to prove only the amount of the infringer's sales, and the infringer must then prove its expenses against such sales. Section 1323(d) allows the court to award attorneys' fees to the prevailing party and Section 1323(e) allows the court to order the destruction of plates, molds, and the like used to make infringing articles. Section 1323(c) sets up a three year statute of limitations.

(11) Private Rights of Action Against Pirated Designs

Section 1326 affords a powerful remedy for victims of pirated designs. Specifically, that Section allows a private right of action to recover civil fines of not more than $500 per offense for false marking with a design notice knowing that the design is not protected. The civil fines are split equally between the private plaintiff and the United States.

(12) Relation to Design Patents and Retroactive Effect

Finally, Section 1329 provides that the issuance of a design patent terminates any protection for the original design under the design statute, and Section 1332 provides that the design statute has no retroactive effect.

(g) Limitation of Liability of Online Service Providers

The DMCA contains elaborate provisions and safe harbors that limit the liability of online service providers for copyright infringement occurring through their services. These provisions are discussed in Section III.C.6 below.

(h) Subpoenas to Service Providers

Section 512(h) of the DMCA sets up a procedure through which a copyright owner may obtain a subpoena through a United States district court directing the service provider to release the identity of an alleged direct infringer acting through the service provider's system or network. The subpoena is issued by the clerk of any United States district court upon a request by the copyright owner (or one authorized to act on the owner's behalf) containing the proposed subpoena, "a copy of a notification described in subsection (c)(3)(A)," and a sworn declaration ensuring that the subpoena is solely to obtain the identity of the alleged infringer, which information will be used only to protect rights to the copyright.[1239] The subpoena, in turn, authorizes and orders the recipient service provider "to expeditiously disclose" information sufficient to identify the alleged infringer.[1240] The clerk "shall expeditiously issue" the subpoena if it is in proper form, the declaration is properly executed, and "the notification filed satisfies the provisions of subsection (c)(3)(A).[1241] The service provider, upon receipt of the subpoena, "shall

[1239] 17 U.S.C. § 512(h)(2).

[1240] Id. § 512(h)(3).

[1241] Id. § 512(h)(4).

expeditiously disclose" the information required by the subpoena to the copyright owner (or authorized person).[1242] The issuance, delivery and enforcement of subpoenas is to be governed (to the extent practicable) by the provisions of the Federal Rules of Civil Procedure dealing with subpoenas duces tecum.[1243]

(1) Jurisdictional Issues

The issue of where subpoenas under Section 512(h) must be sought and where they can be served was tested in two lawsuits brought by Massachusetts universities against the RIAA, Massachusetts Institute of Technology v. RIAA[1244] and Boston College v. RIAA.[1245] In those cases, the universities challenged the service in Massachusetts of Section 512(h) subpoenas issued by a federal district court in Washington, D.C. The court ruled that Fed. R. Civ. P. 45(a)(2) and (b)(2), which require a subpoena to issue from the district in which the production is to be made, do not permit a Section 512(h) subpoena for production issued in Washington, D.C. to be validly served in Massachusetts.[1246]

The RIAA contended that service of the subpoenas was proper because of language within the DMCA that the RIAA contended trumps Fed. R. Civ. P. 45. Specifically, the RIAA pointed to Section 512(h)(1), which authorizes a copyright owner to request the clerk of "any" U.S. district court to issue a subpoena. Second, Section 512(h)(5) requires the service provider to disclose the requested information "notwithstanding any other provision of law." Third, while Section 512(h)(6) provides that the rules regarding service of subpoenas will govern to the "greatest extent practicable," that provision also contains an important carve out: "unless otherwise provided by this section." The court rejected the RIAA's arguments, ruling that Section 512(h) does not trump the ordinary rules regarding service of subpoenas under the Federal Rules of Civil Procedure.[1247]

(2) RIAA v. Verizon Internet Services

The scope of Section 512(h) was first tested in the case of In re Verizon Internet Services, Inc.[1248] In that case, the Recording Industry Association of America (RIAA) served a subpoena under Section 512(h) on Verizon Internet Services seeking identifying information about an anonymous copyright infringer allegedly using Verizon's network to download copyrighted songs through peer-to-peer software provided by Kazaa. Along with the subpoena, RIAA provided Verizon with a list of more than 600 files allegedly downloaded by the user on one day.

[1242] Id. § 512(h)(5).

[1243] Id. § 512(h)(6).

[1244] 1:03-MC-10209-JLT (D. Mass. Aug. 7, 2003).

[1245] 1:03-MC-10210-JLT (D. Mass. Aug. 7, 2003).

[1246] "District of Columbia Court Lacks Authority to Issue DMCA Subpoenas to Boston Schools," *BNA's Patent, Trademark & Copyright Journal* (Aug. 15, 2003) at 458.

[1247] Id.

[1248] 240 F. Supp. 2d 24 (D.D.C. 2003).

The subpoena included the user's IP address and the time and date when the songs were downloaded, and a declaration, under penalty of perjury, that the information was sought in good faith and would only be used in connection with protecting the rights of RIAA members.[1249]

Verizon refused to comply with the subpoena, arguing that, because Section 512(h) requires a notice under Section 512(c)(3)(A) to accompany the subpoena application, the subpoena power applies only if the infringing material is stored or controlled on the Service Provider's system or network under subsection (c). Verizon further argued that, because it only provided the alleged infringer with an Internet connection, it fell under subsection (a) of Section 512 and was thus outside the subpoena authority of Section 512(h).[1250] The RIAA sought to enforce the subpoena against Verizon in court.

The district court rejected Verizon's arguments and ruled that the subpoena power of Section 512(h) applies to all service providers within the scope of the DMCA, not just to those service providers storing information on a system or network at the direction of a user. The court held that the plain language of Section 512(h) compelled this result, because it employs the term "service provider" repeatedly, and Section 512(k) provides two definitions of the term "service provider" – one directed to service providers falling under Section 512(a) and another directed to service providers falling under Sections 512(b) – (d).[1251] The court rejected Verizon's contention that it should infer that the subpoena authority applies only to subsection (c) in view of the reference in subsection (h)(2)(A) to the notification requirement of subsection (c)(3)(A). The court noted that "the notification provision in subsection (c) is also referenced elsewhere in the DMCA, including in subsections (b)(2)(E) and (d)(3). The latter references confirm the expectation that notifications like that described in subsection (c)(3) will at times be needed in settings under subsections (b) and (d), and hence are not confined to subsection (c) settings."[1252] The court also rejected a number of constitutional challenges to the Section 512(h) subpoena

---

[1249] Id. at 28.

[1250] Id. at 29.

[1251] Id. at 31.

[1252] Id. at 32-33. Verizon also relied on the fact that under subsection (c)(3)(A)(iii) a copyright owner must identify the infringing material "that is to be removed or access to which is to be disabled." Verizon argued that in order to remove or disable access to the material, the material must be stored on its system, thereby indicating that Congress intended Section 512(h) to apply only to those service providers who store infringing material on their systems. The court rejected this argument. "[A] subpoena issued pursuant to subsection (h) is used to identify the infringer, not to force the service provider to remove material or disable access to it. The requirement for the notification is simply that it identify the infringing material to be removed, not that removal be effectuated. In addition, a copyright owner can meet the requirement under subsection (c)(3)(A)(iii) if it can disable access to material. Here, Verizon certainly can disable access to the material by terminating the account altogether." Id. at 33 n.5. Since Verizon was a Section 512(a) service provider, and the requirement in subsection (c) to remove or disable access to infringing material stored on the service provider's system is not applicable to subsection (a), it is unclear what the court's reference to Verizon's ability to disable access to material by terminating accounts was intended to mean. Perhaps that service providers who are subject to the Section 512(a) safe harbor must nevertheless terminate the accounts of repeat infringers in order to qualify for the safe harbor, per the provisions of Section 512(i). This is only a possible implication, however, and the point of the court's passage is that Section 512(h) is focused on identification of the infringer, not removal or disabling of access to infringing material.

power identified by *amici curiae*, noting that Verizon itself had not directly asserted that the subpoena power in Section 512(h) was unconstitutional and that the issues raised by the *amici curiae* had not been fully briefed by the RIAA.[1253] In a subsequent ruling, the district court issued a more elaborated opinion on a number of constitutional challenges to the subpoena power in Section 512(h) raised by Verizon and *amici curiae* and again rejected those challenges.[1254]

On appeal, the D.C. Circuit reversed.[1255] The appellate court held, based on both the terms of Section 512(h) and its overall structure that a subpoena may be issued only to an ISP engaged in storing on its servers, or linking to, material that is infringing or the subject of infringing activity, and not to an ISP acting only as a conduit for data transferred between two Internet users. With respect to the language of Section 512(h) itself, the court noted that Section 512(h)(4) makes satisfaction of the notification requirement of Section 512(c)(3)(A) a condition precedent to issuance of a subpoena, which notification requirement must identify and provide information sufficient to locate infringing material that is to be removed or access to which is to be disabled. The court held that an ISP that is not storing the allegedly infringing material on its servers cannot "remove" or "disable access to" the infringing material no matter what information the copyright owner may provide.[1256]

The RIAA contended that an ISP can "disable access" to infringing material, even when it is providing only conduit functions, by terminating the offending subscriber's Internet account. The court rejected this argument, noting that the DMCA, in Sections 512(j)(1)(A)(i) and 512(j)(1)(A)(ii), sets up distinct statutory remedies in the form of injunctions against providing access to infringing material and injunctions against providing access to a subscriber who is engaged in infringing activity.[1257] "These distinct statutory remedies establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer."[1258] The court further noted that the RIAA's notification had identified absolutely no material Verizon could remove or access to which it could disable, which suggested that Section 512(c)(3)(A) "concerns means of infringement other than P2P file sharing."[1259]

Finally, the court rejected the RIAA's argument that the definition of "Service Provider" in Section 512(k)(1)(B) made Section 512(h) applicable to an ISP regardless what function it performed with respect to the infringing material – transmission per Section 512(a), caching per

---

[1253] Id. at 41-44.

[1254] In re Verizon Internet Services, Inc., 257 F. Supp. 2d 244, 257-68 (D.D.C. 2003). The court also rejected Verizon's argument that Section 512(h) violates Art. III of the Constitution because it authorizes federal courts to issue binding process in the absence of a pending case or controversy. Id. at 248-57.

[1255] Recording Industry Ass'n of Am. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003), cert. denied, 2004 U.S. LEXIS 6700 (2004).

[1256] Id. at 1235.

[1257] Id.

[1258] Id.

[1259] Id. at 1236.

Section 512(b), hosting per Section 512(c), or locating it per Section 512(d).[1260] The court stated that this argument "borders upon the silly. … Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A). And as we have seen, any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of § 512(c)(3)(A)(iii) and is therefore ineffective."[1261]

The court bolstered its conclusion by pointing to the overall structure of Section 512(h), noting that the presence in Section 512(h) of three separate references to Section 512(c) and the absence of any reference to Section 512(a) suggested the subpoena power of Section 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.[1262] The court rejected, however, Verizon's suggestion that the subpoena power could not apply to ISPs engaged in caching or linking functions under Sections 512(b) and (d). Noting that caching and linking were "storage functions," the court ruled that "the cross-references to § 512(c)(3) in §§ 512(b)-(d) demonstrate that § 512(h) applies to an ISP storing infringing material on its servers in any capacity – whether as a temporary cache of a web page created by the ISP per § 512(b), as a web site stored on the ISP's server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d) – and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber."[1263]

Accordingly, the court remanded the case to the district court with instructions to vacate its order enforcing the RIAA's subpoena and to grant Verizon's motion to quash the subpoena.[1264]

(3) The Charter Communications Litigation

In Oct. of 2003, Charter Communications filed a motion to quash nearly 150 subpoenas filed by the RIAA as part of its aggressive campaign against peer-to-peer file sharing of music files. Charter challenged the subpoenas on a number of grounds. First, Charter argued that the subpoenas, which demanded compliance within seven days, did not afford a reasonable or feasible time period for Charter to comply with its duties under the federal Cable Communications Act (CCA) to notify subscribers in advance of its compliance. Charter also argued that the CCA allows the turning over of subscribers' information only where a court order offered evidence that the subscribers were reasonably suspected of engaging in criminal activity, and where the subject of the information had a chance to appear and contest the validity of the claim.[1265]

[1260] Id.

[1261] Id.

[1262] Id. at 1236-37.

[1263] Id. at 1237.

[1264] Id. at 1239.

[1265] "Charter Communications Files Suit, Seeks to Quash RIAA File-Sharing Subpoenas," *BNA's Patent, Trademark & Copyright Journal* (Oct. 15, 2003) at 963.

Charter further challenged the subpoenas on the ground that they violated the DMCA by failing to identify the alleged acts of infringement (the subpoenas provided in each case only an e-mail address, date, and time of day, without any identification of copyrighted works that were allegedly infringed), seeking private information beyond the scope of the DMCA, and improperly combining requests for information about 93 different IP addresses into a single subpoena.[1266]

The district court issued the subpoenas and denied Charter's motion to quash. On appeal, the Eighth Circuit reversed.[1267] The court reviewed in detail the logic of the D.C. Circuit's opinion in the RIAA v. Verizon case and adopted both its reasoning and holding that Section 512(h) does not allow a copyright owner to request a subpoena for an OSP that acts merely as a conduit for data transferred between two Internet users.[1268] The Eighth Circuit did, however, in dicta express certain doubts about the validity of Section 512(h) in general:

> For purposes of this appeal, we do not address the constitutional arguments presented by Charter, but do note this court has some concern with the subpoena mechanism of § 512(h). We comment without deciding that this provision *may* unconstitutionally invade the power of the judiciary by creating a statutory framework pursuant to which Congress, via statute, compels a clerk of a court to issue a subpoena, thereby invoking the court's power. Further, we believe Charter has at least a colorable argument that a judicial subpoena is a court order that must be supported by a case or controversy at the time of its issuance. We emphasize, however, for purposes of this appeal we do not reach these issues and have decided this case on the more narrow statutory grounds.[1269]

(4) Fatwallet v. Best Buy

In this case, Fatwallet, Inc. filed a complaint against Best Buy Enterprises, Kohl's Department Stores and Target Corp. seeking declaratory relief related to the alleged unconstitutionality of the subpoena provisions and the notice and takedown provisions of Section 512(c) of the DMCA. The court dismissed the plaintiff's claims in their entirety on grounds of standing. Apparently only Best Buy had issued a subpoena to Fatwallet under the DMCA. The court ruled that Fatwallet did not have standing related to the subpoena because it was undisputed that Best Buy had never attempted to enforce the subpoena. Even if Best Buy had sought to enforce the subpoena, the court noted that it was difficult to see the harm that would befall Fatwallet as opposed to its subscribers, and the subscribers' interest in maintaining their anonymity was insufficient to invoke standing to a third party such as an ISP to challenge the subpoena when the ISP had not suffered an injury of its own. The court distinguished the Verizon decision on the ground that in that case, Verizon had refused to comply with the subpoena and there was a motion to compel, and in any event, the court disagreed with the

---

[1266] Id.

[1267] In re Charter Communications, Inc. Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005).

[1268] Id. at 776-77.

[1269] Id. at 777-78.

Verizon decision. The court also ruled that Fatwallet had no standing to assert challenges to the notice and takedown provisions of Section 512(c), because Fatwallet was suffering no injury as a result of those provisions. Because the provisions afford only a positive benefit (a safe harbor from liability), Fatwallet was free to ignore them and no harm would befall it that did not already exist irrespective of the DMCA.[1270]

(5) In re Subpoena to University of North Carolina at Chapel Hill

The case of In re Subpoena to University of North Carolina at Chapel Hill[1271] followed the logic of the RIAA v. Verizon and Charter Communications cases and ruled that Section 512(h) does not allow a copyright owner to obtain a subpoena for an OSP that acts merely as a conduit for data transfer.[1272] In addition, the court rejected the RIAA's argument, as did the courts in the Massachusetts Institute of Technology v. RIAA and Boston College v. RIAA cases discussed in Section II.G.6(h)(1) above, that Section 512(h) allows a party to seek a subpoena in any court in the nation for service in any other district. The court noted authority that the subpoena power of a court cannot be more extensive than its jurisdiction, and that Fed. R. Civ. Pro. 45(b)(2) applies only when a court action or other proceeding is preexisting, which is typically not the case when the subpoena power of Section 512(h) is invoked. Accordingly, the Section 512(h) subpoena must be issued by a court in the district in which the subpoena will be served.[1273]

(6) Subpoenas in John Doe Actions

In the wake of the rulings in the RIAA v. Verizon and Charter Communications litigations, copyright owners have turned to filing "John Doe" actions in order to seek subpoenas against OSPs who are mere conduits, and have had success in obtaining subpoenas requiring disclosure of information about subscribers allegedly engaged in copyright infringement through the OSP's service.

For example, in Electra Entertainment Group, Inc. v. Does 1-6, the court allowed the plaintiffs to take immediate discovery on the University of Pennsylvania to obtain the identity of each Doe defendant by serving a Rule 45 subpoena seeking the name, address, telephone number, email address, and Media Access Control (MAC) address for each defendant. The court required, however, that the Rule 45 subpoena instruct the University of Pennsylvania to distribute a copy of a notice specified by the court to each Doe defendant within seven days of service of the subpoena. The notice informed each defendant that a subpoena disclosing the defendant's identity had been sought and that his or her name had not yet been disclosed, but would be within 21 days if he or she did not challenge the subpoena. The notice contained a list of legal resources who might be able to help the defendant fight the subpoena. The notice further

---

[1270] Fatwallet, Inc. v. Best Buy, No. 03 C 50508 (April 12, 2004) (memorandum opinion).

[1271] 367 F. Supp. 2d 945 (M.D.N.C. 2005).

[1272] Id. at 952-56.

[1273] Id. at 956-58.

informed the defendant that if he or she did not live or work in Pennsylvania, or visit the state regularly, he or she might be able to challenge the Pennsylvania court's jurisdiction over him or her. Finally, the notice informed the defendant that the record companies were willing to discuss the possible settlement of their claims with the defendant, that the parties might be able to reach a settlement agreement without the defendant's name appearing on the public record, that the defendant might be asked to disclose his or her identity to the record companies if he or sought to pursue settlement, and that defendants who sought to settle at the beginning of a case might be offered more favorable terms by the record companies.[1274]

(7) Interscope Records v. Does 1-7

In Interscope Records v. Does 1-7,[1275] the court followed the Charter Communications and Verizon cases in holding that Section 512(h) does not authorize the issuance of subpoenas against Section 512(a) OSPs who act merely as conduits.[1276] The plaintiffs had sought such a subpoena against the College of William and Mary, which provided Internet services that the Doe defendants allegedly used to access a peer-to-peer online media distribution system for the purpose of downloading and distributing plaintiffs' copyrighted works.[1277]

(8) In re Maximized Living

In In re Maximized Living, Inc. v. Google, Inc.,[1278] the court ruled that the subpoena power of Section 512(h) is limited to currently infringing activity and does not reach former infringing activity that has ceased and can thus no longer be removed or disabled. In this case, because Google had already taken down the plaintiff's copyrighted scripts from an Internet blog hosted by Google, the use of a Section 512(h) subpoena to still seek to obtain the identity of the user who had posted those scripts was invalid.[1279]

9. Proposed Limitation of Scope of Shrinkwrap and Clickwrap Licenses That Did Not Pass

H.R. 3048 contained an interesting and potentially controversial provision that would have extended the scope of the preemption provisions of the copyright statute to limit certain provisions common to shrinkwrap and clickwrap license agreements. Specifically, H.R. 3048 would have added the following provision at the end of Section 301(a) of the copyright statute:

[1274] Order, Elektra Entertainment Group, Inc. v. Does 1-6, Civ. Action No. 04-1241 (Oct. 13, 2004). The language of the court's order, without the notice attached, may be found at 2004 U.S. Dist. LEXIS 22673.

[1275] 494 F. Supp. 2d 388 (E.D. Va. 2007).

[1276] Id. at 388.

[1277] Id.

[1278] 2011 U.S. Dist. LEXIS 147486 (N.D. Cal. Dec. 22, 2011).

[1279] Id. at *3-4, 13-16.

> When a work is distributed to the public subject to non-negotiable license terms, such terms shall not be enforceable under the common law or statutes of any state to the extent that they –
>
> > (1) limit the reproduction, adaptation, distribution, performance, or display, by means of transmission or otherwise, of material that is uncopyrightable under section 102(b) or otherwise; or
> >
> > (2) abrogate or restrict the limitations on exclusive rights specified in sections 107 through 114 and sections 117 and 118 of this title.

Clause (1) was apparently intended to establish an affirmative principle that subject matter which is not protected by copyright under Section 102(b) of the copyright statute (which includes "any idea, procedure, process, system, method of operation, concept, principle, or discovery") cannot be the subject of contractual prohibitions on reproduction, adaptation, distribution, performance or display in a license having non-negotiable terms (such as a shrinkwrap or clickwrap agreement). Although this provision is founded on a philosophical notion that subject matter which the copyright law deems free for the public to use should not be withdrawn from use, at least by virtue of a non-negotiable license, it might have had unintended consequences with respect to confidentiality clauses that protect trade secret material.

Specifically, many shrinkwrap or clickwrap agreements contain confidentiality clauses that prohibit the disclosure, use and reproduction of trade secret subject matter embodied in software that will typically fall within the enumerated subject matter of Section 102(b) of the copyright statute. Clause (1) could have been read to preempt these confidentiality clauses. This seems like a somewhat strange result in view of the Supreme Court's ruling that copyright law does not preempt state trade secret law.[1280] The authors of H.R. 3048 apparently saw a more pernicious effect from such clauses simply because they are contained in a non-negotiable license, although it is not clear why.

Clause (2) would have preempted clauses in a shrinkwrap or clickwrap agreement that have the effect of restricting the limitations on copyright rights enumerated in Sections 107 through 114, 117, and 118 of the copyright statute. This provision would have affected many shrinkwrap and clickwrap agreements in at least two ways. First, because many courts have ruled that disassembly of computer programs to extract ideas from them is a fair use under certain circumstances,[1281] the clauses which flatly prohibit disassembly or reverse engineering of software that are common in shrinkwrap and clickwrap agreements might have been preempted. Second, clauses which prohibit transfer of a copy of a computer program by the licensee to a third party (a right that would otherwise be available if the first sale doctrine of Section 109 of the copyright statute is deemed applicable by treating a shrinkwrap license transaction as a sale) might have been preempted.

[1280] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

[1281] See Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993); Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832 (Fed. Cir. 1992); DSC Communications Corp. v. DGI Technologies Inc., 898 F. Supp. 1183 (N.D. Tex. 1995).

It is unknown whether there will be efforts to reintroduce this provision in another session of Congress.

III. APPLICATION OF COPYRIGHT RIGHTS TO SPECIFIC ACTS ON THE INTERNET

As is apparent from Part II, copyright owners hold a potentially very broad panoply of rights that may be applicable to acts on the Internet. These rights may well be expanded by the recently adopted WIPO treaties. Part III of this paper analyzes the potential application of such rights to various actions on the Internet, such as browsing, caching, linking, operation of an Internet service or bulletin board, creation of derivative works, and resale or subsequent transfer of works downloaded from the Internet, as well as how various traditional defenses – such as fair use and the implied license doctrine – may be interpreted with respect to Internet activities.

A. Browsing

Browsing is probably the single most common activity of users on the Internet today. It provides a graphic illustration of the difficulty and uncertainty of applying traditional copyright rights, in which tangible objects are the paradigm for transfer of information, to the Internet medium, in which electronic transmissions are the paradigm for transfer of information. The difficulty arises principally from the fact that, unlike in the case of traditional media, reading or use of a copyrighted work on the Internet generally requires making a "copy" of the work (at least under the logic of the MAI case and its progeny and under the WIPO Copyright Treaty), and may require a distribution, transmission, and access of the work as well. Thus, although "reading" and "using" are not within a copyright holder's exclusive rights, copying, distribution, and (under the WIPO treaties) transmission and access, are. To the extent the latter acts are necessarily incidental to browsing a work on the Internet, such browsing may technically infringe multiple rights of the copyright holder.

Indeed, one recent decision held that the act of browsing an unauthorized copy of a copyrighted work constituted copyright infringement, because the browsing caused an additional copy of the work to be made in RAM. Specifically, in Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,[1282] the court, citing the MAI decision, stated, "When a person browses a website, and by so doing displays the [copyrighted material], a copy of the [copyrighted material] is made in the computer's random access memory (RAM), to permit viewing of the material. And in making a copy, even a temporary one, the person who browsed infringes the copyright."[1283]

In addition, browsing may implicate the right of public display and/or public performance. For example, the NII White Paper takes the position that browsing through copies of works on the Internet is a public display of at least a portion of the browsed work.[1284] In

[1282] 53 U.S.P.Q.2d 1425 (D. Utah 1999).

[1283] Id. at 1428.

[1284] NII White Paper at 45.

addition, at least isochronous downloading of performances of copyrighted works in the course of browsing by members of the public, such as from a commercial online service like America On Line (AOL), may constitute infringements of the public performance right.[1285] As noted in Part II above, the fact that potential recipients of transmitted displays and performances are geographically and/or temporally dispersed does not prevent a transmission to a single recipient in any given instance from creating a "public" display or performance.

In a great many instances, a copyright holder will have placed material on the Internet with the intent and desire that it be browsed. Browsing of such material will no doubt be deemed to be either within the scope of an implied license from the copyright holder or a fair use. For example, the court in Religious Technology Center v. Netcom On-Line Communication Services[1286] noted in dicta that much of digital browsing is probably a fair use or an innocent infringement:

> Absent a commercial or profit-depriving use, digital browsing is probably a fair use; there could hardly be a market for licensing the temporary copying of digital works onto computer screens to allow browsing. Unless such a use is commercial, such as where someone reads a copyrighted work online and therefore decides not to purchase a copy from the copyright owner, fair use is likely. Until reading a work online becomes as easy and convenient as reading a paperback, copyright owners do not have much to fear from digital browsing and there will not likely be much market effect.
>
> Additionally, unless a user has reason to know, such as from the title of a message, that the message contains copyrighted materials, the browser will be protected by the innocent infringer doctrine, which allows the court to award no damages in appropriate circumstances. In any event, users should hardly worry about a finding of direct infringement: it seems highly unlikely from a practical matter that a copyright owner could prove such infringement or would want to sue such an individual.[1287]

Although the Netcom court is no doubt correct in its observations under U.S. copyright law, nevertheless browsing raises important copyright problems that cannot be dismissed simply on the notion that doctrines such as fair use, implied license, or innocent infringement will remove the problems entirely. First, Internet activities are inherently global, and countries outside the U.S. may not apply defensive doctrines such as fair use and implied license as broadly as U.S. courts. At best, the rules may differ from country to country, which will breed uncertainty and the possibility of inconsistent results in different countries.

Second, as elaborated below in the discussion on caching, copyright owners may begin placing notices on their works governing the uses to which they may be put. Such notices may

---

[1285] The public digital performance right in a sound recording may also be implicated.

[1286] 907 F. Supp. 1361 (N.D. Cal. 1995).

[1287] Id. at 1378 n.25.

restrict use of the work in ways that are unclear or undesirable, and the applicability of the fair use or implied license doctrines may become more uncertain in the face of such notices.

Third, the fact that browsing, an activity akin to reading in traditional media, potentially constitutes literal infringement of so many copyright rights represents a significant shift in the balance between the rights of purchasers and users on the one hand, and the interests of copyright owners on the other. As one commentator recently stated:

> The conflict here of perspective, policy, and technology may be a defining issue in cyberspace. ... [T]he idea that reading a digital text entails a potential copyright violation shifts policy. That shift, even if desirable, should occur because of an express policy choice rather than because new technology technically triggers concepts originally designed for a world of photocopy machines, recorders, and the like.[1288]

Such policy shift, and the details of it, may not be expressly defined in U.S. copyright law (and perhaps in the copyright laws of other countries as well) until legislation implementing the WIPO treaties is considered.

B. Caching

Caching is another activity that is, under current technology, virtually ubiquitous on the Internet. Caching (sometimes known as "mirroring," usually when it involves storage of an entire site or other complete set of material from a source) means storing copies of material from an original source site (such as a Web page) for later use when the same material is requested again, thereby obviating the need to go back to the original source for the material. The purpose of caching is to speed up repeated access to data and to reduce network congestion resulting from repeated downloads of data. The cached material is generally stored at a site that is geographically closer to the user, or on a more powerful computer or one that has a less congested data path to the ultimate user. The cached information is usually stored only temporarily, although the times may vary from a few seconds to a few days, weeks, or more.

1. Types of Caching

Caching may be of the following types:

- Local Caching: Caching generally occurs locally at the end user's computer, either in RAM, on the hard disk, or some combination of both. Most browsers, for example, store recently visited Web pages in RAM or on the hard disk. When the user hits the "Back" key, for example, the browser will usually retrieve the previous page from the cache, rather than downloading the page again from the original site. This retrieval from cache is much faster and avoids burdening the network with an additional download.

[1288] R. Nimmer, Information Law ¶ 4.08[1], at 4-30 (2001).

- Proxy Caching: Proxy caching occurs at the server level, rather than at the end user's computer level. Specifically, a copy of material from an original source is stored on a server other than the original server. For example, an OSP such as AOL may store on its own server for a certain period of time Web pages that have been previously requested by AOL users. When another user subsequently requests a page previously stored, AOL may download the page from its own server, rather than fetching the page from the original source server.

The use of caching on the Internet stems from at least three reasons: to overcome transmission bandwidth limitations, to load balance serving up web pages (such as through search engines) or distributing other content in high demand through multiple sources, and to preserve archival versions of web pages for use in the event that web sites are removed or go down temporarily.

Caching presents difficult copyright issues on a number of fronts. Because caching involves the making of copies, it presents an obvious problem of potential infringement of the right of reproduction. In addition, proxy caching may give rise to infringement of the rights of public distribution, public display, public performance, and digital performance, since copies of copyrighted works may be further distributed and displayed or performed from the cache server to members of the public. Under the WIPO treaties, caching may also infringe the new rights of transmission and access. Because the situs of infringements of these rights under the WIPO treaties is most likely the server, caching may give rise to infringements at every proxy server. Large OSPs may have proxy servers at many sites around the globe.

2. The Detriments of Caching

From a legal perspective, because caching has obvious technical benefits in getting information from the Internet to a user faster, one might assume that a copyright owner who has placed information on the Internet and desires such information to reach end users as expeditiously as possible would have no incentive to assert its copyright rights against caching.[1289] In legal terms, one might be tempted to conclude that caching will fall within the fair use or implied license doctrines. However, the legal analysis is complex, because caching carries with it a number of potential detriments to the owner of the copyrighted material:[1290]

- Loss of Version Control: Caching interferes with the ability of a website operator to control what version of information is delivered to the end user.[1291] For example, a website may have been substantially improved, yet an old version of material from the site may reside on the proxy server of the end user's OSP. Many end users may

[1289] Indeed, in a poll taken during 1997 by *Interactive PR & Marketing News*, 82% of respondents answered "no" to the question, "Do you feel that caching of content of Web sites or online service providers constitutes infringement?" *Interactive PR & Marketing News*, Vol. 4, No. 28 (Aug. 8, 1997), at 1.

[1290] In addition to the detriments noted to the copyright owner, caching can give rise to potential liability on the part of the caching entity. For example, if an original site contains defamatory material, the caching entity may be deemed to have "republished" that defamatory information through the caching mechanism.

[1291] Eric Schlachter, "Caching on the Internet," *Cyberspace Lawyer*, Oct. 1996, at 2, 3.

therefore not see the improved version the website owner desired to present to the public. In a more serious vein, suppose a website owner is notified that its site contains infringing or defamatory material. To avoid liability, the website owner may remove such material promptly, yet it may continue to be distributed through old cached versions, giving rise to potential ongoing liability.

- Out of Date Information: Many websites may contain time sensitive information, such as stock quotes or sports scores. If information is obtained from a cache rather than the original site, and the cache has not been refreshed recently, the user may obtain out of date information or information that is no longer accurate. The problem is heightened by the fact that most caching is "invisible" to the user. In many instances the user will simply not know whether the information being presented is cached information, how recently the cache was refreshed, or whether the information contained in the cached version is now out of date as compared to information at the original site. A user may therefore unknowingly rely on inaccurate information to his or her detriment.

- Interference with Timed Information: Closely related to the problem of out of date information is the problem of interference with timed information. For example, a website owner may have contracted with an advertiser to display an advertising banner during a certain window of time, say 7:00 to 8:00 p.m. If a page from the site is downloaded into a cache at 7:30 p.m. and is not refreshed for several hours, users will see the ad for far more than the one hour the advertiser paid for, and may not see at all the ad that the next advertiser paid to have displayed from 8:00 p.m. to 9:00 p.m.[1292]

- Inaccurate Page Impression and Other Information: Many websites keep track of the number of "page impressions" at the site – i.e., the number of times a page is displayed from the site to users. Page impressions are often used as a measure for advertising charges – the more page impressions a site generates among users, the more the site can charge for advertisements placed on the site. Accesses to cached versions of a Web page may not be counted as page impressions at the original site,[1293] and the original website owner may not know how often a given page was viewed from the cache.[1294] Reduced page impression counts cost the website owner advertising revenues. In addition, many sites maintain "server logs" which record activities of users of the site, from which valuable information may be gleaned. Accesses to cached information will generate entries into the logs of the proxy server, not the original site.

[1292] See id. at 3.

[1293] David G. Post, "Bargaining in the Shadow of the Code: File Caching, Copyright, and Contracts Evolving in Cyberspace," at 7 (paper presented at the University of Dayton School of Law Symposium on "Copyright Owners' Rights and Users' Privileges on the Internet," Nov. 1-2, 1996; copy on file with the author).

[1294] At least one online service markets to website owners data about the number of page impressions delivered from its cache. Schlachter, supra note 1291, at 3.

- Loss of Limits on Access: Caching may also result in the loss of control over access to information at a site. For example, suppose a website owner desires to limit access to material on a site to a single user at a particular institution through use of a password. Such user could enter the password, download the information to a proxy server, and then other, unauthorized users might be able to gain access to it.[1295]

As discussed in detail in Section III.C below, the DMCA creates a safe harbor for caching by OSPs under defined circumstances, which in part anticipate, and condition the safe harbor upon, compliance with technical solutions that may develop and become industry standards. The safe harbor implicitly recognizes, and seems designed to minimize, the potential detriments of caching discussed above.

3. The Netcom Case and Application of the Fair Use Doctrine

As discussed in detail in Section III.C.6(b)(1)(ii) below, the DMCA creates a safe harbor for caching by OSPs under defined circumstances. Even if the conditions required under the DMCA are not met to take advantage of the safe harbor, a person performing caching of copyrighted material might nevertheless seek to justify it under either the fair use or implied license doctrines. Because of the potential detriments of caching, application of the fair use and implied license doctrines to caching is uncertain.

This subsection gives a general analysis of the legal issues that arise in applying the fair use doctrine to caching, from the perspective of an OSP performing proxy caching, since OSPs or similar entities seem the most likely targets for claims of infringement by copyright owners based on caching.[1296] The analysis uses as a springboard the first case to address the applicability of the fair use doctrine to an OSP in a factual setting akin to caching, Religious Technology Center v. Netcom On-Line Communication Services.[1297] Subsection 4 below discusses other cases since Netcom that have expressly adjudicated the application of the fair use and implied license doctrines to caching. In the Netcom case, the plaintiff sought to hold Netcom, an OSP, liable for allegedly infringing material that was "mirrored" on its server as part of providing Usenet news group services to its subscribers. The holding of that case with respect to the various fair use factors is analyzed below.

(a) Purpose and Character of the Use

The first statutory fair use factor looks to the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes. Proxy caching is generally done in the context of providing commercial services to end users, and is therefore likely to be for a commercial purpose. However, the Netcom court noted that

---

[1295] Post, supra note 1293, at 8.

[1296] One commentator argues that even local caching might give rise to suit by a copyright owner: "For example, such a suit might arise in the case of a large company where the cumulative effects of local caching by many Web browsers (perhaps combined with statutory damages and attorneys fees) are significant." Schlachter, supra note 1291, at 4.

[1297] 907 F. Supp. 1361.

Netcom's use of copyrighted material as part of its Usenet services, "though commercial, also benefits the public in allowing for the functioning of the Internet and the dissemination of other creative works, a goal of the Copyright Act."[1298] The court noted that the commercial nature of Netcom's activity should therefore not be dispositive, concluding that "[b]ecause Netcom's use of copyrighted materials served a completely different function than that of the plaintiffs, this factor weighs in Netcom's favor."[1299]

In many instances, however, it may be unclear whether an OSP's particular form of caching serves a "completely different function" than that of the copyright owner's use of its material. For example, material may be cached from a source website and accessed by users from the proxy server in exactly the same way that it would have been accessed from the original server. The copyright holder might use this fact to distinguish the Netcom court's holding with respect to the first statutory fair use factor.

(b) Nature of the Copyrighted Work

The second statutory fair use factor looks to the nature of the copyrighted work. Fair use rights are generally construed more broadly with respect to factual or published works than with respect to fictional or unpublished works. Although all material available on the Internet is published, such material varies tremendously as to its substantive nature. Thus, whether a particular cached work is factual, fictional, or in between, will vary from case to case, and the application of the second statutory factor to any particular instance of caching cannot necessarily be predicted in advance.

In the Netcom case, the court held that the precise nature of the works at issue was not important to the fair use determination "because Netcom's use of the works was merely to facilitate their posting to the Usenet, which is an entirely different purpose than plaintiffs' use."[1300] As noted with respect to the first statutory fair use factor, however, the same may often not be true in particular instances of caching. Accordingly, it is difficult to say how the second statutory factor may be applied to caching in particular instances.

(c) Amount and Substantiality of the Portion Used

The third statutory fair use factor looks to the amount and substantiality of the portion used in relation to the copyrighted work as a whole. Caching routinely involves the making of copies of entire Web pages, which may in turn contain entire copyrighted works,[1301] so in many instances all or a substantial portion of a copyrighted work will be copied in the course of caching. Generally, no more of a work may be copied than is necessary for the particular use.[1302]

[1298] Id. at 1379.

[1299] Id.

[1300] Id.

[1301] Schlachter, supra note 1291, at 4.

[1302] See, e.g., Supermarket of Homes v. San Fernando Valley Board of Realtors, 786 F.2d 1400, 1409 (9th Cir. 1986).

Although copying an entire work will ordinarily militate against a finding of fair use,[1303] one could argue that caching inherently requires copying all or a substantial portion of the cached material in order to derive the benefits of the caching, and this factor should therefore not be dispositive of fair use.

For example, the Netcom court noted that "the mere fact that all of a work is copied is not determinative of the fair use question, where such total copying is essential given the purpose of the copying."[1304] Because Netcom had copied no more of the plaintiff's works than necessary to function as a Usenet server, the court concluded that the third statutory factor should not defeat an otherwise valid defense.[1305]

OSPs that engage in copying of whole works may be able to rely on this logic by arguing that such copying is essential given the nature and purpose of caching. Such an argument may, however, be vulnerable to attack, depending upon the way in which the caching is performed. Caching by an OSP of only that material that has been requested by users in some previously defined time period may be said to be "essential" because such material has at least a demonstrated basis for expecting that it will be accessed again. But what about extensive "mirroring," where an OSP copies, for example, entire websites from geographically remote sites to more local servers? Such caching is not based on actual demand usage. Should this matter? Could the OSP argue that such caching is "essential" to avoid potential network bottlenecks from the remote site to its users' computers? The case of Field v. Google, discussed in Section III.B.4(a) below, found extensive caching by Google using automated robots to be a fair use.

(d) Effect of Use on the Potential Market

The fourth statutory fair use factor looks to the effect of the use upon the potential market for or value of the copyrighted work. This factor is generally considered the most important of the four factors.[1306] In analyzing this factor, a court may look to "'whether unrestricted and widespread conduct of the sort engaged in by the defendant … would result in a substantially adverse impact on the potential market' for the original."[1307] Because caching is inherently widespread on the Internet, a court may well look beyond the individual actions of a particular caching entity and assess the potential aggregate impact of caching on a copyright owner.

The application of this factor is very difficult to predict in advance, without knowing the particular factual circumstances of the caching that is being challenged. There are no doubt many instances of caching that do not harm the potential market for a copyright owner's work,

---

[1303] Sony Corp. v. Universal Studios, Inc., 464 U.S. 417, 449-50 (1984).

[1304] Netcom, 907 F. Supp. at 1380 (citing the Supreme Court's decision in Sony, in which the Court held that total copying of copyrighted broadcast programs for the purpose of time-shifted viewing was a fair use).

[1305] Netcom, 907 F. Supp. at 1380.

[1306] See 4 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 13.05[A][4], at 13-180 to –181 (1999) (citing, inter alia, Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 566 (1985)).

[1307] Campbell v. Acuff-Rose Music, Inc., 114 S. Ct. 1164, 1177 (1994) (quoting 3 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 13.05[A][4]).

especially with respect to caching of material from non-commercial websites that make material available for free. However, even in the case of non-commercial sites, one or more of the detriments of caching noted in subsection 2 above may be applicable, and the copyright owner might use such detriments as the basis for an argument of harm to the potential market for the copyrighted material. For example, a website owner might put promotional material up on its site that is updated frequently. If caching caused the latest updated material not to be available, the owner might argue that the "market" for its website material had been harmed.

With respect to commercial sites, one can more readily imagine instances in which caching could cause harm to the market for copyrighted works. For example, if caching reduces the number of page impressions generated by a home page containing copyrighted material on which advertising is sold, the owner could argue that its advertising revenues for ads placed in conjunction with such copyrighted material (which, in this instance, is arguably the very "market" for such material) will be harmed.

In the Netcom case, the court held that potential harm under the fourth fair use factor precluded a ruling that the OSP's posting of the plaintiffs' copyrighted material in its Usenet service was a fair use. The plaintiffs had argued that the Internet's extremely widespread distribution of its copyrighted religious materials multiplied the potential effects of market substitution for its materials by groups using such materials to charge for Scientology-like religious training.[1308]

In sum, it seems that the application of the fourth fair use factor will be highly fact specific, and there may be instances in which a copyright holder could establish sufficient harm to its potential markets from caching as to preclude a finding of fair use. It therefore seems unwise to make a blanket assumption that the fair use doctrine will automatically protect all forms of caching.

The potential harm to copyright owners from caching also introduces uncertainty with respect to whether the implied license doctrine may apply to caching in various instances. Courts often tend to construe implied licenses narrowly.[1309] A court might therefore be hesitant to construe any implied license from a copyright owner based on its posting of material for browsing on the Web to cover uses (such as caching) that cause palpable harm to the owner.

[1308] Netcom, 907 F. Supp. at 1380.

[1309] See, e.g., MacLean Assocs. Inc. v. Wm. M. Mercer-Meidinger-Hansen Inc., 952 F.2d 769 (3d Cir. 1991) (defendant obtained an implied license to use a computer program prepared by an independent contractor, but only in the furtherance of its business relationship with one particular client for which the contractor had been engaged to support); Oddo v. Reis, 743 F.2d 630 (9th Cir. 1984) (scope of implied license included the right to market an unmodified computer program to third parties, subject to an obligation to account for profits to the developer, but did not include a right to modify); see also Microstar v. Formgen, Inc., 942 F. Supp. 1312, 1318 (S.D. Cal. 1996); Meadows, "Practical Aspects of 'Implied License,'" *Computer Law Strategist* (May 1993) at 1. See generally Barry & Kothari, "Other People's Property: There May Be Implied Licenses for Content on Web Pages," *San Francisco Daily Journal* (Aug. 28, 1997) at 5.

4. Cases Adjudicating Caching Under the Fair Use and Implied License Doctrines

(a) Field v. Google

In Field v. Google[1310] the plaintiff, Field, alleged that by allowing Internet users to access copies of his copyrighted works stored by Google in its online cache, Google was violating his exclusive rights to reproduce and distribute copies of those works. The court ruled that Google's acts were covered by the fair use and implied license doctrines.

The challenged acts arose in the context of Google's search engine and its accompanying Web crawler, the Googlebot. The Googlebot automatically and continuously crawled the Internet to locate and analyze Web pages and to catalog those pages into Google's searchable Web index. As part of the process, Google made and analyzed a copy of each Web page the Googlebot found and stored the HTML code from those pages in a cache so as to enable those pages to be included in the search results displayed to users in response to search queries. When Google displayed Web pages in its search results, the first item appearing was the title of a Web page which, if clicked, would take the user to the online location of that page. The title was followed by a short snippet of text from the Web page in a smaller font. Following the snippet, Google typically provided the full URL for the page. Then, in the same smaller font, Google often displayed another link labeled "Cached." When clicked, the "Cached" link directed a user to the archival copy of a Web page stored in Google's system cache, rather than to the original Web site for that page. By clicking on the "Cached" link for a page, a user could view the snapshot of that page as it appeared the last time the site was visited and analyzed by the Googlebot.[1311]

The court noted that Google provided "Cached" links for three principal reasons – to allow viewing of archival copies of pages that had become inaccessible because of transmission problems, censorship, or because too many users were trying to access the content at a particular time; to enable users to make Web page comparisons to determine how a particular page had been altered over time; and to enable users to determine the relevance of a page by highlighting where the user's search terms appeared on the cached copy of the page.[1312]

Of particular relevance to the court's rulings were certain widely recognized and well publicized standard protocols that the Internet industry had developed by which Web site owners could automatically communicate their preferences to search engines such as Google. The first mechanism was the placement of meta-tags within the HTML code comprising a given page to instruct automated crawlers and robots whether or not the page should be indexed or cached. For example, a "NOINDEX" tag would indicate an instruction that the Web page in which it was embedded should not be indexed into a search engine, and a "NOARCHIVE" tag would indicate

---

[1310] 412 F. Supp. 2d 1106 (D. Nev. 2006).

[1311] Id. at 1110-11.

[1312] Id. at 1111-12.

that the page should not be cached or archived. When the Googlebot visited a page, it would search for meta-tags in the HTML of the page and obey them.[1313]

The second mechanism by which Web site owners could communicate with search engines' robots was by placing a "robots.txt" file on the Web site containing textual instructions concerning whether crawling of the site was allowed. If the Googlebot encountered a robots.txt file with a command disallowing crawling, it would not crawl the Web site, and there would therefore be no entries for that Web site in Google's search results and no "Cached" links. The court noted that the Internet industry had widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994.[1314]

In the court's words, Field decided to "manufacture a claim for copyright infringement against Google in the hopes of making money from Google's standard practice"[1315] of caching by placing his copyrighted works on a Web site available to the public for free and creating a robots.txt file on the site with the permissions set within the file to *allow* all robots to visit and index all of the pages on the site, knowing that this would cause the Googlebot to cache his copyrighted works. Field testified in his deposition that he had consciously chosen not to use the NOARCHIVE meta-tag on his Web site. When Google learned that Field had filed (but not served) a complaint for copyright infringement, Google promptly removed the "Cached" links to all of the pages on his site.[1316]

Field alleged only claims of direct copyright infringement against Google (and made no claims for contributory or vicarious liability), asserting that Google directly infringed his copyrights when a Google user clicked on a "Cached" link to the Web pages containing his copyrighted materials and downloaded a cached copy of those pages from Google's system cache.[1317] As discussed in Section II.A.4(l) above, the court ruled that Google was not a direct infringer because it lacked the necessary volitional act in responding with a purely automated download process to users who clicked on the "Cached" links.

In addition, the court granted summary judgment to Google on its three defenses of implied license, estoppel, and fair use. With respect to the implied license defense, the court found that Field was aware of the industry standard mechanisms by which he could have indicated a desire not to have his Web site crawled or cached, and that, with knowledge of how Google would use the copyrighted works he placed on his site, by choosing not to include meta-tags on the site that he knew would have caused the Googlebot not to archive his site, his conduct should reasonably be interpreted as a license to Google for crawling and archiving the site.[1318]

[1313] Id. at 1112-13.

[1314] Id. at *1113.

[1315] Id.

[1316] Id. at *1113-14.

[1317] Id. at *1115.

[1318] Id. at *1115-16.

The court also found that Field should be estopped from asserting a copyright claim based on the challenged behavior by Google. Field knew of Google's allegedly infringing conduct well before any supposed infringement of his works took place and knew "that Google would automatically allow access to his works through 'Cached' links when he posted them on the Internet unless he instructed otherwise."[1319] Yet, he remained silent regarding his unstated desire not to have "Cached" links provided to his Web site and intended Google to rely on this silence knowing that it would. Google was not aware that Field did not wish to have Google provide "Cached" links to his works, and Google detrimentally relied on Field's silence. Accordingly, the court found the four factors for estoppel present, and granted Google's summary judgment on the defense of estoppel.[1320]

The court then turned to application of each of the four factors of the fair use defense. Concerning the first factor, purpose and character of the use, the court, relying on Kelly v. Arriba Soft,[1321] found Google's search engine was a transformative use of Field's works in that Google's presentation of "Cached" links did not serve the same functions to enrich and entertain others that Field's original posting of the works did. Rather, the "Cached" links allowed users to locate and access information that was otherwise inaccessible, and allowed users to understand why a page was responsive to their original query. The object of enabling users to more quickly find and access the information they were searching for was not served by the original page.[1322] Nor did Google's use of "Cached" links substitute for a visit to the original page. The court noted that Google had included at the top of each listing a prominent link to the original Web page. The "Cached" links were displayed in smaller font and in a less conspicuous location, and there was no evidence that Internet users accessed the pages containing Field's works via Google's "Cached" links in lieu of visiting those pages directly. Google's status as a commercial enterprise also did not negate the first factor weighing in Google's favor, because there was no evidence that Google profited in any way by the use of any of Field's works. Field's works were merely among billions of works in Google's database, and when a user accessed a page via Google's "Cached" links, Google did not display advertising to the user or otherwise offer a commercial transaction.[1323]

The court found that the second factor, the nature of the copyrighted works, weighed only slightly in Field's favor. Even assuming that Field's copyrighted works were creative, the court noted that he had published them on the Internet, thereby making them available to the world at his Web site, thus indicating a desire to make his works available to the widest possible audience for free.[1324] The court found the third factor, the amount and substantiality of the use, to be

---

[1319] Id. at 1116-17.

[1320] Id. at 1117.

[1321] 336 F.3d 811 (9th Cir. 2003).

[1322] Field v. Google, 412 F. Supp. 2d at 1118-19.

[1323] Id. at 1119.

[1324] Id. at 1120.

neutral. The transformative and socially valuable purposes served by Google's caching could not be effectively accomplished by using only portions of the Web pages.[1325]

The court ruled that the fourth factor, the effect of the use upon the potential market for or value of the copyrighted work, weighed strongly in favor of a fair use determination. The court noted that here there was no evidence of any market for Field's works, and Field had made the works available to the public for free in their entirety and admitted he had never received any compensation from selling or licensing them.[1326] In a significant holding, the court rejected Field's argument that Google's caching harmed the market for his works by depriving him of revenue he could have obtained by licensing Google the right to present "Cached" links for the pages containing his works. The court recognized the bootstrapping nature of the argument: "Under this view, the market for a copyrighted work is always harmed by the fair use of the work because it deprives the copyright holder of the revenue it could have obtained by licensing that very use. The Supreme Court has explained that the fourth fair use factor is not concerned with such syllogisms [citing Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 592 (1994)]. … Where there is no likely market for the challenged use of the plaintiff's works, the fourth fair use factor favors the defendant."[1327]

Finally, the court noted that in adjudicating fair use, courts may consider other factors beyond the four enumerated ones in the copyright statute. In this case, the court found it significant that Google had acted in good faith, as evidenced by the fact that Google honored the industry standard protocols that site owners could use to instruct search engines not to provide "Cached" links for the pages of their sites. Google also provided an automated mechanism for promptly removing "Cached" links from Google's search results if undesired links ever appeared. And Google had, without being asked, promptly removed the "Cached" links to the pages of Field's site upon learning that he objected to them.[1328] Accordingly, balancing all the factors, the court granted summary judgment for Google on its fair use defense.[1329] As discussed further in Section II.C.5(b)(1)(ii).a below, the court also concluded that Google was entitled to the safe harbor of Section 512(b)(1) of the DMCA.[1330]

(b) Perfect 10 v. Google (aka Perfect 10 v. Amazon)

In Perfect 10 v. Google,[1331] discussed in detail in Section II.C.4 above, the district court ruled, contrary to the Intellectual Reserve case discussed in Section III.D.6 above, that the caching that occurs in an Internet user's web browser constitutes a fair use:

[1325] Id. at 1120-21.

[1326] Id. at 1121.

[1327] Id. at 1121 n.9.

[1328] Id. at 1122-23..

[1329] Id. at 1125.

[1330] Id. at 1123-24.

[1331] 416 F. Supp. 2d 828 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

> [Plaintiff] argues that merely by viewing such websites [containing infringing photographs], individual users of Google search make local "cache" copies of its photos and thereby directly infringe through reproduction. The Court rejects this argument. Local browser caching basically consists of a viewer's computer storing automatically the most recently viewed content of the websites the viewer has visited. It is an automatic process of which most users are unaware, and its use likely is "fair" under 17 U.S.C. § 107. *But cf. Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999). Local caching by the browsers of individual users is noncommercial, transformative, and no more than necessary to achieve the objectives of decreasing network latency and minimizing unnecessary bandwidth usage (essential to the internet). It has a minimal impact on the potential market for the original work, especially given that most users would not be able to find their own local browser cache, let alone locate a specific cached copy of a particular image. That local browser caching is fair use is supported by a recent decision holding that Google's own cache constitutes fair use. *Field v. Google, Inc.*, [412 F. Supp. 2d 1106 (D. Nev. 2006).] If anything, the argument that local browser caching is fair use is even stronger. Whereas Google is a commercial entity, individual users are typically noncommercial. Whereas Google arranges to maintain its own cache, individual users typically are not aware that their browsers automatically cache viewed content. Whereas Google's cache is open to the world, an individual's local browser cache is accessible on that computer alone.[1332]

On appeal, the Ninth Circuit affirmed this ruling, holding that, "even assuming such automatic copying could constitute direct infringement, it is a fair use in this context. The copyright function performed automatically by a user's computer to assist in accessing the Internet is a transformative use. Moreover, as noted by the district court, a cache copies no more than is necessary to assist the user in Internet use. It is designed to enhance an individual's computer use, not to supersede the copyright holders' exploitation of their works. Such automatic background copying has no more than a minimal effect on Perfect 10's rights, but a considerable public benefit."[1333]

(c) Ticketmaster L.L.C. v. RMG Technologies, Inc.

In Ticketmaster L.L.C. v. RMG Technologies, Inc.[1334] the plaintiff Ticketmaster sought to hold the defendant liable for direct and indirect copyright liability based upon the defendant's development and marketing of an automated tool that enabled users (such as ticket brokers) to access and navigate rapidly through the Ticketmaster site and purchase large quantities of tickets. The court granted a preliminary injunction against the defendant, finding that the defendant was highly likely to be found liable for direct copyright infringement because it had, during the course of development of the tool, accessed the defendant's site and made copies of web pages

---

[1332] Id. at 852 n.17.

[1333] Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

[1334] 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

from the site in the RAM of its computers, which copies the court held, citing MAI v. Peak, fell within the Copyright Act's definition of "copy." The court found such copying unauthorized because it violated the Terms of Use posted on Ticketmaster's site, which prohibited use of any areas of the site for commercial purposes and use of any automated devices to search the site.[1335]

The court rejected the defendant's argument, based on Perfect 10 v. Google, that such RAM copying should be deemed a fair use. The court distinguished that case on the ground that the Ninth Circuit had ruled only that automatic cache copies made by users who link to infringing web sites should be deemed a fair use because, in that particular context, the caching was noncommercial, transformative and had a minimal impact on the potential market for the original work. By contrast, in the instant case, the court ruled that the defendant was not an "innocent" third party visitor to another person's infringing site. Instead, the purpose of the defendant's viewing the Ticketmaster web site and the copying that entailed was to engage in conduct that violated the site's Terms of Use in furtherance of the defendant's own commercial objectives.[1336] "Furthermore, in this case, such copying has a significant, as opposed to minimal, effect on Plaintiff's rights because Defendant's conduct empowers its clients to also violate the Terms of Use, infringe on Plaintiff's rights, and collectively cause Plaintiff" harm.[1337]

The court also found the defendant highly likely to be liable for contributory infringement because it had supplied a tool that enabled its users to gain unauthorized access and use of the Ticketmaster site, thereby making infringing copies of web pages from the site, and had also induced the infringing behavior by advertising its tool as "stealth technology [that] lets you hide your IP address, so you never get blocked by Ticketmaster."[1338]

(d) Parker v. Yahoo!, Inc.

In Parker v. Yahoo!, Inc.,[1339] the plaintiff, author of several works that he made freely available on his web site, sued Yahoo and Microsoft for copyright infringement, alleging that their search engines created and republished unauthorized cached copies of his works based on the fact that when an Internet user used either of the defendants' search engines, the search results included hyperlinks to cached copies of the web pages responsive to the user's inquiry. The user could view those search results either by following a hyperlink to the original web site or by viewing the cached copy hosted on the defendants' computers. The plaintiff conceded in his complaint that the defendants each provided opt-out mechanisms, through the robots.txt protocol, that would prevent his web sites from being cached, but that he had not made use of them.[1340]

[1335] Id. at 1105-09.

[1336] Id. at 1109-10.

[1337] Id. at 1110.

[1338] Id. at 1110-11 (emphasis in original).

[1339] 2008 U.S. Dist. LEXIS 74512 (E.D. Pa. Sept. 26, 2008).

[1340] Id. at *1-2.

The court ruled that, as a result of the plaintiff's failure to employ the robots.txt protocol on his web site or to send the defendants a takedown notice, the defendants had an affirmative defense of implied license for acts of caching prior to the lawsuit. From the plaintiff's silence and lack of earlier objection, the defendants could properly infer that the plaintiff knew of and encouraged the search engines' activity. However, the court refused to dismiss entirely the plaintiff's count for direct copyright infringement because the defendants had allegedly continued to display the plaintiff's works even after the filing of the lawsuit. The court noted several decisions holding that a nonexclusive implied license can be revoked where no consideration has been given for it, and initiation of a lawsuit itself may constitute revocation of an implied license if there was no consideration for the license.[1341]

However, the court dismissed the plaintiff's counts for contributory and vicarious copyright infringement on the part of the defendants based on allegedly infringing copies of the plaintiff's content made when an Internet user's browser stored a temporary copy of a file that was necessary for the user to view the web site. The court ruled that, by publishing his works online with no registration requirement or any other access measure taken, the plaintiff had impliedly authorized Internet users at large to view his content and, consequently, to make incidental copies necessary to view that content over the Internet. And even if search engine users did directly infringe the plaintiff's copyright, the court held that the plaintiff had not set forth any plausible allegation that either defendant financially benefitted from such infringement. Nor had the plaintiff alleged that either defendant had knowledge of any third party's infringement.[1342]

5. Other Caching Cases

(a) Facebook v. Power Ventures

In Facebook, Inc. v. Power Ventures, Inc.,[1343] the defendants operated an Internet service called Power.com that collected user information from Facebook's web site outside of the "Facebook Connect" application programmer's interface (API). After a user provided his or her user names and passwords, the Power.com service used the access information to scrape user data from those accounts. Facebook alleged that the defendants committed direct and indirect copyright infringement when they made cached copies of Facebook's web site during the process of extracting user information. The defendants brought a motion to dismiss the copyright claims. The court denied the motion, ruling that Facebook's allegation that the defendants made an unauthorized cache copy of the web site on each occasion of access to scrape data was sufficient to survive a motion to dismiss.[1344]

[1341] Id. at *14-16.

[1342] Id. at *18-20.

[1343] 2009 U.S. Dist. LEXIS 42367 (N.D. Cal. May 11, 2009).

[1344] Id. at *1-11.

C. Liability of Online Service Providers

Much of the Internet copyright debate in recent years has centered around the issue of copyright liability of OSPs, BBS operators, system operators, and other service providers for infringing activities taking place through their facilities. Indeed, to date, almost all of the reported Internet copyright decisions have centered around the issue of liability of OSPs and BBS operators. Copyright owners have sought to hold OSPs and BBS operators liable on theories of direct liability, contributory liability, and vicarious liability. This Section discusses each of these three theories in turn and the cases raising those theories that have been decided to date involving the Internet. This Section also discusses the relevant provisions of the DMCA that limit the liability of OSPs for the infringing acts of third parties committed through their online services.

1. Direct Liability

As discussed in detail in Section II.A.4 above, a majority of the cases decided to date seem to require that there be some kind of a direct volitional act in order to establish direct infringement liability on the part of an OSP or BBS for infringing postings and unauthorized uses by users. For example, the Netcom court refused to hold an OSP directly liable for automatic pass through of allegedly infringing messages posted to Usenet by a subscriber.[1345] The subsequent MAPHIA case[1346] and the Sabella case[1347] extended the logic of Netcom, refusing to hold liable as a direct infringer the operator of a BBS for the uploading and downloading by subscribers of unauthorized copies of Sega's videogames through the BBS, even though the operator encouraged the initial uploading, because the operator had not participated in the very acts of uploading or downloading themselves. And the CoStar,[1348] Ellison,[1349] and Perfect 10 v. Cybernet Ventures[1350] cases suggest that an OSP will not have direct liability for infringing material posted on its service by users or available through its service on third party sites where the OSP has not encouraged such posting or had advance knowledge of it.

The logic of the Ninth Circuit's decision in Subafilms, Ltd. v. MGM-Pathe Communications Co.[1351] also suggests there should not be direct liability for persons who merely place material on a network for subsequent unauthorized copying, display, performance or the like. Subafilms held that no independent "right of authorization" was created by the copyright statute's reference in Section 106 of the exclusive right "to do or to authorize" the acts enumerated therein. Rather, the reference to "authorize" was meant only to establish potential

---

[1345] Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361 (N.D. Cal. 1995).

[1346] Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

[1347] Sega Enterprises Ltd. v. Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

[1348] CoStar v. Loopnet, 164 F. Supp. 2d 688 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

[1349] Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002), aff'd in part and rev'd in part, 357 F.3d 1072 (9th Cir. 2004).

[1350] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[1351] 24 F.3d 1088 (9th Cir. 1994).

liability for contributory infringement on the part of a person who causes an infringement by authorizing it. Under the reasoning of the Subafilms decision, even if loading material onto a server encourages (or authorizes) copying through downloading, that authorization does not suffice for direct liability.[1352]

However, as discussed in greater detail in Sections II.A.4, II.C, and II.D above, the Frena, Webbworld, Sanfilippo and Hardenburgh cases seem to go further in their willingness to impose direct liability on a BBS operator, at least where an actor such as a BBS operator or website operator has some form of direct involvement in the anticipated acts that lead to infringement or in the infringing acts themselves (such as resale of the infringing material). Such acts of direct involvement in the infringement process may be sufficient for a finding of enough volitional activity to impose direct liability. As noted below, however, legislation limiting the liability of OSPs might negate or limit the holdings of these cases.

(a) Louis Vuitton v. Akanoc Solutions

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,[1353] the defendants operated hosting services for a number of web sites overseas from which counterfeit Louis Vuitton merchandise could be purchased. The plaintiff brought claims for direct and contributory infringement of its copyrights. A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with respect to the claims.[1354] The defendants argued that they could not be liable for contributory copyright infringement because, among other things, the acts of direct infringement – the reproduction of counterfeit merchandise and the storage of digital images of that merchandise on the servers of their web site – occurred extraterritorially in China and the digital images could not be "copies" of the copyrighted merchandise.[1355]

The court rejected these arguments. With respect to territoriality, the court noted that unauthorized copying and public display of a copyrighted work within the United States triggers application of U.S. copyright law, and under Section 602, unauthorized importation into the United States of copies acquired extraterritorially is prohibited, acts which the defendants clearly had done.[1356] Concerning the public display right, the court noted that the Ninth Circuit had adopted in Perfect 10 v. Amazon.com[1357] the "server test," under which a computer owner storing an electronic image as electronic information and serving that information directly to the user is displaying the information in violation of the copyright holder's exclusive display right.

[1352] R. Nimmer, Information Law ¶ 4.10, at 4-39 (2001).

[1353] 2010 U.S. Dist. LEXIS 85266 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part on other grounds, 658 F.3d 936 (9th Cir. 2011).

[1354] Id. at *1-2.

[1355] Id. at *5-6.

[1356] Id. at *7-9.

[1357] 508 F.3d 1146 (9th Cir. 2007).

Here, the evidence established that the defendants' servers in China stored and served data, including pictures of the plaintiff's copyrighted merchandise, for sale to U.S. customers, which was sufficient for direct infringement of the display right. The court also rejected the defendants' argument that the images could not be "copies" of the physical copyrighted merchandise. Accordingly, the court denied the defendants' motion for JMOL as to direct infringement.[1358]

(b) Flava Works v. Gunter

In Flava Works, Inc. v. Gunter,[1359] the defendants were the operators of a web site called myVidster.com, a social networking web site through which site members could store and bookmark video files and post links to third party web sites on which the files were available. Such files were then available for other myVidster users to view or download. The plaintiff, owner of copyrights in adult entertainment products, alleged that users of myVidster had uploaded the plaintiff's copyrighted videos and images, or links to those videos, to the site. The plaintiff sent myVidster seven DMCA notices of copyright infringing specifying the infringing material, identifying users that the plaintiff suspected to be repeat infringers, and demanding that the material be taken down. The plaintiff's complaint did not allege that myVidster had failed to remove the material identified in the notices from the site, but did allege that after the notices were sent, the web site continued to be updated with more and more infringing material from its users. The complaint also alleged that the site did not have in place any filters or identifiers to prevent the plaintiff's copyrighted material from being re-posted by repeat infringers and the site took no action to stop, reprimand or ban repeat infringers. The plaintiff sought to hold myVidster directly, contributorily, and vicariously liable for infringement of its copyrights. The defendants filed a motion to dismiss on the common law claims, although the motion was apparently not based on any of the DMCA safe harbors.[1360]

The court granted the motion with respect to the claim of direct infringement, citing the CoStar case for the proposition that to establish liability for direct copyright infringement, a plaintiff must demonstrate that the defendant engaged in volitional conduct that causes a copy to be made. Because the only volitional copying alleged in the complaint was alleged to have been done by myVidster users, not its operators, the complaint failed to state a claim for direct copyright infringement.[1361] The court's rulings with respect to contributory, vicarious, and inducement liability are set forth in Sections III.C.2(m), III.C.3(o), and III.C.4(e) below, respectively.

[1358] Akanoc, 2010 U.S. Dist. LEXIS 85266 at *11-15.

[1359] 2011 U.S. Dist. LEXIS 5006 (N.D. Ill. May 20, 2011).

[1360] Id. at *1-4.

[1361] Id. at *6-8.

On appeal, although the Seventh Circuit vacated the district court's preliminary injunction based on the other claims, the court agreed that the users who uploaded infringing copies of the plaintiff's videos, and myVidster, were the direct infringers.[1362]

2. Contributory Liability

A party may be liable for contributory infringement where "with knowledge of the infringing activity, [it] induces, causes or materially contributes to the infringing activity of another."[1363] The standard of knowledge is objective: to know or have reason to know that the subject matter is copyrighted and that the particular uses were violating copyright law.[1364] For liability for contributory infringement, there must be a direct infringement[1365] to which the contributory infringer has knowledge and encourages or facilitates.

The requirement of knowledge may eliminate contributory liability on the part of an OSP or BBS operator with respect to many instances of infringement for which the OSP or BBS is merely a passive information conduit and has no knowledge of the infringement. However, given knowledge (or reason to know), a number of cases suggest that a system provider cannot simply continue to provide the facility that enables infringement.

(a) The Netcom Case

In Religious Technology Center v. Netcom On-Line Communication Services,[1366] the court held that the OSP Netcom could be contributorily liable for infringing postings by an individual named Erlich of copyrighted religious materials to Usenet through the provider after the service was given notice of the infringing material. "If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement since its failure to simply cancel Erlich's infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in Erlich's public distribution of the message."[1367] The court held that the copyright notices in the posted works were sufficient to give Netcom notice that the works were copyrighted.[1368]

[1362] Flava Works, Inc. v. Gunter, 2012 U.S. App. LEXIS 15977 at *12 (7th Cir. Aug. 2, 2012).

[1363] E.g., Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); Cable/Home Communications Corp. v. Network Prods., Inc., 902 F.2d 829, 845 (11th Cir. 1990).

[1364] R. Nimmer, Information Law ¶ 4.11, at 4-40 (2001); see also Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996) ("The standard for the knowledge requirement is objective, and is satisfied where the defendant knows or has reason to know of the infringing activity.") (citing Casella v. Morris, 820 F.2d 362, 365 (11th Cir. 1987)).

[1365] Given the ubiquitous nature of copies on the Internet and the strength of the copyright holder's other rights discussed in this paper, establishing a direct infringement in a network transmission should not be difficult.

[1366] 907 F. Supp. 1361 (N.D. Cal. 1995).

[1367] Id. at 1374.

[1368] Id.

However, the court was careful to note that where an operator is unable to verify a claim of infringement, there may be no contributory liability:

> Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is a likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.[1369]

Nevertheless, the court clearly imposed a duty on the operator to actively attempt to verify a claim of infringement and to take appropriate action in response:

> Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs' copyrighted works, to hold Netcom liable for contributory infringement where Netcom has knowledge of Erlich's infringing postings yet continues to aid in the accomplishment of Erlich's purpose of publicly distributing the postings.[1370]

(b) The MAPHIA Case

In addition to the Netcom case, the court in the subsequent MAPHIA case[1371] (also out of the Northern District of California) held a BBS and its system operator liable for contributory infringement for both the uploading and the subsequent downloading of copies of Sega's video games by users where the system operator had knowledge that the infringing activity was going on through the bulletin board, and had specifically solicited the uploading of the games for downloading by users of the bulletin board. The court cited the Ninth Circuit's decision in Fonovisa, Inc. v. Cherry Auction, Inc.[1372] for the proposition that providing the site and facilities for known infringing activity is sufficient to establish contributory liability. "In this case, Sherman provided the BBS as a central depository site for the unauthorized copies of games, and allowed subsequent distribution of the games by user downloads. He provided the facilities for copying the games by providing, monitoring, and operating the BBS software, hardware, and phone lines necessary for the users to upload and download games."[1373] This suggests that mere operation of a BBS, at least if the operator knows that infringing activity is taking place, may be sufficient for contributory liability.

However, the court went on to hold that Sherman would have been liable as a contributory infringer even under a higher standard requiring more direct participation in the infringement that the court believed the Netcom decision established:

[1369] Id.

[1370] Id. at 1375.

[1371] Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

[1372] 76 F.3d 259 (9th Cir. 1996).

[1373] MAPHIA, 948 F. Supp. at 933.

However, even under an alternative and higher standard of "substantial participation," Sherman is liable. Under this standard, Sherman is only liable if he knew of the users' infringing actions, and yet substantially participated by inducing, causing or materially contributing to the users' infringing conduct. Netcom, 907 F. Supp. at 1382. In this case, Sherman did more than provide the site and facilities for the known infringing conduct. He actively solicited users to upload unauthorized games, and provided a road map on his BBS for easy identification of Sega games available for downloading. Additionally, through the same MAPHIA BBS medium, he offered copiers for sale to facilitate playing the downloaded games.[1374]

(c) The Peer-to-Peer Filing Sharing Cases

(1) The Napster Cases

In December of 1999, the Recording Industry Association of America, Inc. (RIAA), on behalf of 18 of its members, filed a complaint in federal court in the Northern District of California for contributory and vicarious copyright infringement against Napster, Inc., the operator of a Web site (www.napster.com) designed to enable its members to locate music files in the MP3 format[1375] stored on the hard disks of other members, and to initiate downloads of such files through a "peer-to-peer" architecture – i.e., transfers directly from the computer of one user to the computer of another user without passing through the Napster servers.

1. Factual Background. Napster offered to its members a piece of proprietary software called "MusicShare" for download from its website free of charge. When a Napster user logged on, the MusicShare software would interact with the Napster server software to connect the user to one of many servers operated by Napster, would read a list of names of MP3 files that the user had elected to make available on his or her personal computer for sharing with other users (by placing them in certain designated directories on his or her hard disk known as the "user library"), and would then store the names of those files in an index maintained on the Napster server. Once the file names were successfully uploaded to the index, each user library, identified by a user name, would become a "location" on the Napster servers. Napster locations were short-lived – they were respectively added or purged every time a user signed on or off of the network. Thus, a particular user's MP3 files designated for sharing would be accessible to other users only while that user was online.[1376]

An account holder could use the search tools included in the MusicShare software to find MP3 files being shared by other users by searching the index containing the names of MP3 files

---

[1374] Id. The court further held that because Sega had established contributory liability on the part of Sherman, the court need not address whether Sherman was also liable under the theory of vicarious liability. Id.

[1375] MP3 stands for Motion Picture Expert Group 1, Audio Layer 3. MP3 is an algorithm that compresses a digital music file by a ratio of approximately 12:1, thereby reducing the size of the file so that it more easily and quickly can be downloaded over the Internet. A&M Records Inc. v. Napster Inc., 54 U.S.P.Q.2d 1746, 1747 n.1 (N.D. Cal. 2000).

[1376] A&M Records Inc. v. Napster Inc., 114 F. Supp. 2d 896, 905 (N.D. Cal. 2000).

that online users saved in their designated user library directories. Users wishing to search for a song or artist could do so by entering the name of the song or artist in the search fields of the MusicShare software and then clicking a "Find It" button. The Napster servers would perform a text search of the file names in the index and respond by sending the requesting user a list of files that included the same term(s) the requesting user entered on the search form. Alternatively, users could access MP3 files via a "hotlist" function. This function enabled a Napster user to archive other user names and learn whether account holders who accessed the network under those names were online. A requesting user could access or browse all files listed in the user libraries of hotlisted users.[1377]

In either case, once a requesting user located and selected a desired file from a list of search results or a list of files made available by a hotlisted user, the Napster server software would then engage in a dialog with the MusicShare software of the requesting user and that of the "host user" (i.e., the user who made the desired MP3 file available for downloading). The Napster server would obtain the necessary Internet Protocol (IP) address information from the host user, communicate the host user's address or routing information to the requesting user, and the requesting user's computer would then employ this information to establish a "peer-to-peer" connection directly with the host user's MusicShare software and download the MP3 file from the host user's library. The content of the actual MP3 file would be transferred over the Internet between the users, not through the Napster servers. No MP3 music files were stored on the Napster servers themselves.[1378]

The plaintiffs, owners of the copyrights in many of the sound recordings being downloaded by users through the Napster system, brought claims for contributory and vicarious copyright infringement and sought a preliminary injunction against Napster. A second, very similar case, was filed against Napster in federal district court in the Northern District of California on Jan. 7, 2000.[1379] That case was a class action filed by named plaintiffs Jerry Leiber, Mike Stoller, and Frank Music Corp. on behalf of themselves and "those music publisher-principals of The Harry Fox Agency, Inc."[1380] The complaint alleged that Napster's Web site constituted inducement and contributory infringement of the copyrights in various musical compositions held by the members of the class.[1381] The complaint further alleged that Napster was contributing to the unauthorized reproduction and distribution of "phonorecords" embodying the copyrighted musical compositions of members of the class without obtaining the necessary authority from The Harry Fox Agency.[1382] Those two cases were consolidated before Judge Marilyn Hall Patel.

[1377] Id. at 906.

[1378] Id. at 907.

[1379] Leiber et al. v. Napster Inc., No. C 00 0074 ENE (N.D. Cal. Jan. 7, 2000).

[1380] Id. ¶ 10.

[1381] Id. ¶¶ 1, 29.

[1382] Id. ¶ 30.

Several other copyright holders, including the artists Metallica and Dr. Dre and several independent recording artists and labels, as well as the Academy of Motion Picture Arts and Sciences (AMPAS), ultimately also filed lawsuits against Napster for copyright infringement, all of which were eventually consolidated before Judge Patel in the Northern District of California under the Multi-District Litigation (MDL) rules of the federal courts. In July of 2000, the district court entered a broad preliminary injunction against Napster. Before it took effect, however, the Ninth Circuit stayed the injunction pending an expedited appeal by Napster.

After appeal, the Ninth Circuit issued an opinion affirming in part and reversing in part, with a remand to the district court to enter a modified preliminary injunction of narrower scope, which the district court did on Mar. 5, 2001. Both sides filed a second appeal to the Ninth Circuit based on the Mar. 5 preliminary injunction. The Mar. 5 order was clarified by the district court in a memorandum dated Apr. 26, 2001, then orally modified by the court from the bench on July 11, 2001. Ten days before the oral modification of the injunction, on July 1, 2001, Napster voluntarily suspended file sharing through its service. On July 18, 2001, the Ninth Circuit stayed the district court's July 11 oral modification of the preliminary injunction. Both Napster and the plaintiffs pursued further appeals to the Ninth Circuit in view of the July 11 oral order. The Ninth Circuit consolidated those appeals with the earlier appeals of the Mar. 5 modified injunction.

The Napster cases raised a number of issues of significant importance to online copyright law, and the district court and the Ninth Circuit took somewhat different approaches with respect to various of the issues. With respect to each issue, the district court's analysis will first be described, followed by the Ninth Circuit's analysis of the issue. Because there were multiple appeals to the Ninth Circuit, the first opinion issued by the Ninth Circuit will be referred to as "Napster I," to distinguish it from the later opinion issued by the Ninth Circuit as a result of the subsequent consolidated appeals, which will be referred to as "Napster II."

2. Whether Any Otherwise Direct Infringement by Napster's Users Was Immunized by the AHRA. The district court ruled that Napster was both contributorily and vicariously liable for infringing downloads of copyrighted material by its users via the Napster system. The court ruled that the plaintiffs had established a prima facie case of direct copyright infringement by Napster users because "virtually all Napster users engage in the unauthorized downloading or uploading of copyrighted music; as much as eighty-seven percent of the files available on Napster may be copyrighted, and more than seventy percent may be owned or administered by plaintiffs."[1383] The Ninth Circuit in Napster I agreed, concluding that (i) the mere uploading of file names to the search index by Napster users, thereby making the files corresponding to those file names *available* for downloading (whether or not they were in fact downloaded by other users) constituted an infringement of the plaintiffs' exclusive distribution rights and (ii) the unauthorized downloading of files containing copyrighted music by Napster users violated the plaintiffs' exclusive reproduction rights.[1384]

[1383] Napster, 114 F. Supp. 2d at 911.

[1384] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001) ("Napster I").

Napster argued that its users' downloads of music for their own personal use were immunized by the Audio Home Recording Act of 1992 (AHRA).[1385] The AHRA made two major substantive changes to copyright law. First, Subchapter D of the AHRA (Section 1008) immunizes certain noncommercial recording and use of musical recordings in digital or analog form.[1386] Section 1008 provides:

> No action may be brought under this title alleging infringement of copyright[1387] based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.

Second, Subchapters B and C (Sections 1002-1007) of the AHRA require (i) that any "digital audio recording device" conform to the "Serial Copyright Management System" (SCMS), which allows unlimited first generation copies of an original source, but prohibits second generation copies (i.e., copies of a copy), and (ii) that manufacturers and distributors of digital audio recording devices and digital audio recording media (such as DAT tape and recordable CDs) pay royalties and file various notices and statements to indicate payment of those royalties.[1388]

Napster argued that under the direct language of Section 1008, no action for infringement of copyright could be brought against Napster's users, who were consumers and who were engaged in the noncommercial making and sharing (distribution) of digital musical recordings. Because the actions of Napster's users were immune, Napster argued that it could not be contributorily or vicariously liable for those actions.[1389] Napster cited the following legislative history of the AHRA as support for its argument that Congress intended to afford a very broad immunity for non-commercial copying of audio recordings:

- S. Rep. 102-294 (1992) at 51 ("A central purpose of the Audio Home Recording Act of 1991 is conclusively to resolve [the] debate" over the "copyright implications of private audio recording for noncommercial use.").

- H. Rep. 102-873(I) (1992) at 24 ("In the case of home taping, the exemption protects all noncommercial copying by consumers of digital and analog musical recordings.").

[1385] Pub. L. No. 102-563, 106 Stat. 4244 (1992), codified at 17 U.S.C. §§ 1001-1010.

[1386] *Nimmer* § 8B.01 (2000).

[1387] The immunity applies with respect to copyrights in both the sound recordings and any musical compositions embodied therein. Id. § 8B.07[C][2], at 8B-90.

[1388] Id. §§ 8B.02 & 8B.03 (2000).

[1389] Opposition of Defendant Napster, Inc. to Plaintiffs' Motion for Preliminary Injunction, A&M Records, Inc. v. Napster, Inc., Civ. Nos. C99-5183 MHP (ADR) & C00-0074 MHP (ADR) (July 5, 2000), at 5-6 (hereinafter, "Napster's PI Opp. Br."), on file with the author.

- Contemporaneous comments by Jason Berman, former head of the RIAA, acknowledging that the immunity provisions of the AHRA were intended to have a broad scope, stating: "The [AHRA] will eliminate the legal uncertainty about home audio taping that has clouded the marketplace. The bill will bar copyright infringement lawsuits for both analog and digital home audio recording by consumers …." H.R. 4567, Serial No. 102-139 (March 1992).

- Comments by Senator DeConcini, who was influential in passing the AHRA: "[The AHRA] makes clear the private, non-commercial taping, of both analog and digital material, is permissible under the copyright law. As new and improved technologies become available, such clarification in the law becomes more important." 137 Cong. Rec. S11845 (1992).[1390]

Napster also cited a report by the Office of Technology Assessment (OTA) on home taping as evidence that Congress, in enacting the AHRA, fully understood that consumers would share music with family, friends and others. In particular, the OTA report deemed taping CDs or records borrowed from friends, and giving copies of one's own CDs or records to friends, to be synonymous with "personal use," "private copying," "home use," and "private use."[1391] The OTA report noted that, even by 1989, copying for personal use was widespread: 37% of the home tapers surveyed copied music they borrowed from a friend or other family members; 26% gave away the last copy they made to others outside their household or to family members; and 41% had within the last year borrowed a friend's music to copy so they would not have to buy it themselves.[1392] Napster argued that Congress had knowingly legislated a very broad form of immunity for all of this conduct.[1393]

Finally, Napster argued that the Ninth Circuit's decision in Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.[1394] supported its argument that the AHRA immunized the sharing of musical recordings by Napster's users. At issue in that case was whether the "Rio" device, a small device with headphones that allowed a user to download MP3 files from a computer hard drive and listen to them elsewhere, was a "digital audio recording device" subject to the SCMS requirements of the AHRA. The Ninth Circuit held that it was not, on the following rationale. A "digital audio recording device" is defined as a device having a digital recording function whose primary purpose is to make a "digital audio copied recording," which is defined as a reproduction of a "digital musical recording." 17 U.S.C. § 1001(1), (3). However, a "digital musical recording" is defined to *exclude* a material object "in which one or more computer programs are fixed." Id. § 1001(5)(B)(ii). The Ninth Circuit ruled that a computer hard drive falls within this exemption, and therefore that MP3 files stored on a hard

---

[1390] Id. at 6.

[1391] U.S. Congress, OTA, *Copyright and Home Copying: Technology Challenges the Law*, OTA-CIT-422, at 5, 156 (U.S. GPO, Oct. 1989).

[1392] Id. at Tables 6-10, 6-12 at 270 & Table 7-4 at 274.

[1393] Napster's PI Opp. Br., supra note 1389, at 6-7.

[1394] 180 F.3d 1072 (9th Cir. 1999).

drive do not constitute a "digital musical recording."[1395] Because the Rio did not make copies from "digital musical recordings," it was not a "digital audio recording device" and was therefore not subject to the SCMS requirements of the AHRA.[1396]

As support for its decision, the Ninth Circuit stated the following about the immunity provisions of the AHRA:

> In fact, the Rio's operation is entirely consistent with the [AHRA's] main purpose – the facilitation of personal use. As the Senate Report explains, "[t]he purpose of [the] Act is to ensure the right of consumers to make analog or digital recordings of copyrighted music for their private, noncommercial use." The Act does so through its home taping exemption, see 17 U.S.C. § 1008, which "protects all noncommercial copying by consumers of digital and analog musical recordings." The Rio merely makes copies in order to render portable, or "space-shift," those files that already reside on a user's hard drive."[1397]

Napster argued that in the preceding passage from the Diamond decision, the Ninth Circuit had ruled that Section 1008 of the AHRA gives a consumer the right to create personal MP3 files, and that copying a music file from one's hard drive to a portable device was also appropriate. Napster concluded that, if a consumer can copy an MP3 file from his or her hard drive without violating the copyright laws, Napster's directory service did not violate the copyright laws either.[1398]

In response, the plaintiffs argued that, because Section 1008 states that no action for infringement may be brought based on "the noncommercial use by a consumer of *such a device* [i.e., a digital audio recording device] … for making digital musical recordings" (emphasis added), and because the Ninth Circuit held in Diamond that a computer hard drive is not a "digital audio recording device," the immunity of Section 1008 does not extend to MP3 files stored on a computer hard drive. The Napster case, then, presented an issue of first impression of whether the definitions of Section 1001 should be read to limit *both* the scope of the SCMS/royalty requirements *and* the scope of the immunity of the AHRA.[1399]

[1395] Id. at 1078.

[1396] Id. at 1078-79.

[1397] Id. at 1079 (citations omitted).

[1398] Napster's PI Opp. Br., supra note 1389, at 5-6.

[1399] Prof. Nimmer notes that the Ninth Circuit's Diamond decision could be read to mean that the immunity provisions of the AHRA are not limited by that Court's own construction of the definitions of the technical terms that it held to limit the scope of the SMCS/royalty requirements: "Based on the legislative history's characterization of '*all* noncommercial copying by consumers of digital and analog musical recordings' as falling under the protection of the home taping exemption, the court appears ready to apply that provision beyond its precise wording." *Nimmer* § 8B.07[C][4], at 8B-94.

Napster also argued that a narrow application of § 1008 would lead to the absurd construction that a manufacturer of a device capable of copying a CD (which is clearly a digital musical recording) onto a hard drive would be immune, yet when a consumer used that very same device to copy her musical recording from

The district court, in a terse analysis of the AHRA in a footnote, rejected the argument that Section 1008 of the AHRA immunized the actions of Napster's users for two reasons. First, the court ruled that the "AHRA is irrelevant to the instant action" because "[n]either the record company nor music publisher plaintiffs have brought claims under the AHRA."[1400] Second, the court labeled the passage from Diamond quoted above and cited by Napster as "dicta" and found it to be "of limited relevance":

> The *Diamond Multimedia* court *did* opine that making copies with the Rio to space-shift, or make portable, files already on a user's hard drive constitutes "paradigmatic noncommercial personal use entirely consistent with the purposes of the Act [i.e. the facilitation of personal use]." However, this dicta is of limited relevance. Because plaintiffs have not made AHRA claims, the purposes and legislative history of the AHRA do not govern the appropriateness of a preliminary injunction against Napster, Inc. Furthermore, as explained below, the court is not persuaded that space-shifting constitutes a substantial, noninfringing use of the Napster service. The Ninth Circuit did not discuss the fair use doctrine in *Diamond Multimedia*.[1401]

On appeal in Napster I, the Ninth Circuit affirmed the conclusion that the AHRA did not immunize the activities of Napster users in sharing audio files, although on a different rationale from the district court. The Ninth Circuit did not endorse the district court's rationale that the AHRA was inapplicable merely because the plaintiffs had not brought claims under the AHRA. Instead, the Ninth Circuit cited its rulings in Diamond that computers and their hard drives are not "digital audio recording devices" and that computers do not make "digital musical recordings," as those terms are defined in the AHRA. Accordingly, the AHRA does not cover the downloading of MP3 files to computer hard drives.[1402]

3. The Fair Use Doctrine Generally. Napster also contended that its users did not directly infringe plaintiffs' copyrights because the users were engaged in a noncommercial, fair use of the materials. The district court rejected this argument, ruling that the downloading of musical recordings through Napster did not qualify generally under the four fair use factors. With respect to the first factor – the purpose and character of the use – the district court held that downloading MP3 files was not transformative and, although Napster did not charge for its service, was commercial in nature:

---

the hard drive back onto a CD or onto a Rio for her own or a friend's personal use, she would not have immunity. Napster argued that constructions of statutory language that lead to absurd results clearly contrary to legislative intent must be rejected, citing *United Steel Workers v. Weber*, 443 U.S. 193, 204 (1979); *Train v. Colorado Public Interest Research Group*, 426 U.S. 1, 7 (1975); *Ozawa v. United States*, 260 U.S. 178, 194 (1922). Napster's PI Opp. Br., supra note 1389, at 8 n.8.

[1400] Napster, 114 F. Supp. 2d at 915 n.19.

[1401] Id. (citations omitted; emphasis in original).

[1402] Napster I, 239 F.3d at 1024-25.

> Although downloading and uploading MP3 music files is not paradigmatic commercial activity, it is also not personal use in the traditional sense. Plaintiffs have not shown that the majority of Napster users download music to sell – that is, for profit. However, given the vast scale of Napster use among anonymous individuals, the court finds that download and uploading MP3 music files with the assistance of Napster are not private uses. At the very least, a host user sending a file cannot be said to engage in a personal use when distributing that file to an anonymous requester. Moreover, the fact that Napster users get for free something they would ordinarily have to buy suggests that they reap economic advantages from Napster use.[1403]

The Ninth Circuit affirmed this ruling in Napster I, agreeing with the district court that the downloading was not transformative, and that Napster users were engaging in commercial use of the copyrighted materials because (i) users could not be said to be engaged in a "personal use" when distributing a file to an anonymous requester and (ii) Napster users get something for free they would ordinarily have to buy.[1404] "Direct economic benefit is not required to demonstrate a commercial use. Rather, repeated and exploitative copying of copyrighted works, even if the copies are not offered for sale, may constitute a commercial use."[1405] Because the record demonstrated that Napster users' repeated copying was made to save the expense of purchasing authorized copies, such uses were commercial, causing the first factor to weigh in favor of plaintiffs.[1406]

The district court held that the second factor – nature of the copyrighted work – weighed against fair use because the copyrighted sound recordings and compositions at issue were creative in nature. The third factor – amount and substantiality of the portion used in relation to the whole – also weighed against fair use because copies of entire works were being downloaded.[1407] Finally, the district court found that the fourth factor – the effect on the potential market for the copyrighted work – weighed against fair use because the plaintiffs had produced evidence that Napster use harmed the markets for their copyrighted works by (i) reducing CD sales among college students and (ii) raising barriers to plaintiffs' own entry into the market for digital downloading of music because of competition from a service from which recordings could be obtained free.[1408] The Ninth Circuit affirmed all of these rulings in Napster I.[1409]

[1403] Napster, 114 F. Supp. 2d at 912.

[1404] Napster I, 239 F.3d at 1015.

[1405] Id.

[1406] Id.

[1407] Napster, 114 F. Supp. 2d at 913.

[1408] Id. Napster submitted survey evidence which it argued showed that Napster use actually stimulated more sales of CDs containing the plaintiffs' works than it displaced. The court did not find this evidence credible, and instead credited evidence submitted by the plaintiffs' experts which the plaintiffs claimed showed that Napster use was likely to reduce CD purchases by college students. Id. at 909-10.

[1409] Napster I, 239 F.3d at 1016-17.

4. The Sony Doctrine of Substantial Noninfringing Uses. Napster argued that it could not be contributorily or vicariously liable for operating the Napster service under the doctrine of Sony Corp. of Am. v. Universal City Studios, Inc.,[1410] which held that a manufacturer is not liable for contributory infringement for selling a staple article of commerce that is "capable of commercially significant noninfringing uses,"[1411] even if that article is used to commit copyright infringement. Napster raised a number of uses of the Napster system that it argued were both actual and potential commercially significant noninfringing uses. The district court found that the specific uses raised by Napster were in fact infringing:

5. Sampling. Napster argued that many users use Napster to sample unfamiliar music and then, if they like it, go purchase the music on CD. Napster argued that downloads initiated for sampling purposes and followed up by a purchase of the music, constituted fair use. The district court rejected this argument, ruling that sampling on Napster was not a "personal use in the traditional sense that courts have recognized – copying which occurs within the household and does not confer any financial benefit on the user," and that instead sampling on Napster amounted to "obtaining permanent copies of songs that users would otherwise have to purchase; it also carries the potential for viral distribution to millions of people."[1412] The court distinguished this kind of sampling activity from the time-shifting of viewing that the Supreme Court found a fair use in Sony, where time-shifting enabled a viewer to witness a broadcast that the viewer had been invited to view in its entirety free of charge; by contrast, the court noted that the plaintiffs almost always charged for their music. In addition, the court noted that the majority of VCR purchasers in Sony did not distribute taped television broadcasts, whereas a Napster user who downloads a copy of a song could make that song available to millions of other individuals.[1413] "The global scale of Napster usage and the fact that users avoid paying for songs that otherwise would not be free militates against a determination that sampling by Napster users constitute personal or home use in the traditional sense."[1414]

[1410] 464 U.S. 417 (1984).

[1411] Id. at 442.

[1412] Napster, 114 F. Supp. 2d at 913. This language suggests that the court may have misunderstood Napster's argument about sampling, for the court included under the "sampling" rubric instances in which users downloaded and retained a permanent copy of songs which they "would otherwise have to purchase." Napster defined "sampling" to be those instances in which a user downloaded a song, then followed up with a purchase of the CD containing the song. In such instances, users would not be obtaining music that they "would otherwise have to purchase," and Napster argued that such instances of true sampling should be deemed a fair use. In any event, the district court found not credible a survey submitted by Napster's expert showing that 60% of online users who download free digital music do so to preview music before buying the CD, because Napster's expert did not conduct the survey. The court further found a survey that the expert did conduct not to be credible because the court found it inadequately supervised by the expert. Id. at 914. Finally, the court ruled that even if sampling did enhance sales of plaintiffs' CDs, that would not tip the balance in favor of fair use, because "courts have rejected the suggestion that a positive impact on sales negates the copyright holder's entitlement to licensing fees or access to derivative markets."Id.

[1413] Id. at 913.

[1414] Id. at 914.

On appeal, Napster argued that the district court erred in concluding that sampling is a commercial use because it conflated a noncommercial use with a "personal use"; erred in determining that sampling adversely affects the market for plaintiffs' copyrighted music; and erroneously concluded that sampling is not a fair use because it determined that samplers may also engage in other infringing activity.[1415] The Ninth Circuit in Napster I rejected these challenges, ruling that the plaintiffs had "established that they are likely to succeed in proving that even authorized temporary downloading of individual songs for sampling purposes is commercial in nature," based on evidence in the record that the record company plaintiffs collect royalties for song samples available on Internet retail sites and that such samples, unlike in the case of Napster, are only partial samples of the whole work and often time out after download.[1416] In addition, the Ninth Circuit concluded that the record supported the district court's preliminary determinations that the more music that sampling users download, the less likely they are to eventually purchase the recordings on CD, and even if the audio market is not harmed, Napster had adverse effects on the developing digital download market.[1417] "[P]ositive impact in one market, here the audio CD market, [should not] deprive the copyright holder of the right to develop identified alternative markets, here the digital download market."[1418]

6. Space-Shifting. As an additional noninfringing use, Napster argued that many Napster users use the service to "space-shift," i.e., "converting a CD the consumer already owns into MP3 format and using Napster to transfer the music to a different computer – from home to office, for example."[1419] The district court found that such use was a de minimis portion of Napster use and not a significant aspect of Napster's business, and could therefore not qualify as a substantial noninfringing use under Sony:

> According to the court's understanding of the Napster technology, a user who wanted to space-shift files from her home to her office would have to log-on to the system from her home computer, leave that computer online, commute to work, and log-on to Napster from her office computer to access the desired file. Common sense dictates that this use does not draw users to the system.[1420]

As support for its argument that space-shifting constitutes a fair use, Napster invoked the passage, quoted in subsection 2 above, discussing the AHRA from the Ninth Circuit's decision in Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.[1421] In particular, Napster focused on the last sentence of that passage, in which the Ninth Circuit stated, "The Rio merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard

---

[1415] Napster I, 239 F.3d at 1018.

[1416] Id.

[1417] Id.

[1418] Id.

[1419] Napster, 114 F. Supp. 2d at 904.

[1420] Id. at 904-05.

[1421] 180 F.3d 1072 (9th Cir. 1999).

drive."[1422] Napster argued that by virtue of this passage, the Ninth Circuit had held that space-shifting of works already owned constitutes a fair use.

The district court rejected this argument, ruling that Napster's reliance on the Diamond decision was erroneous because that was "a case involving an inapplicable statute [the AHRA]."[1423] The court also rejected any implication that space-shifting was sufficiently analogous to the time-shifting of television broadcasts that the Supreme Court found to be a substantial noninfringing use in Sony. In particular, the court ruled that in Sony, the Supreme Court had determined that time-shifting represented the principal, rather than an occasional use of VCRs, whereas Napster had failed to show that space-shifting constituted a "commercially significant" use of Napster. "Thus, even if space-shifting is a fair use, it is not substantial enough to preclude liability under the staple article of commerce doctrine."[1424]

On appeal in Napster I, the Ninth Circuit agreed with the district court that the "shifting" analyses of both Sony and Diamond were inapposite because "the methods of shifting in these cases did not also simultaneously involve distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user."[1425]

7. Authorized Distributions. Napster argued that many artists had authorized distributions of their works through the Napster system, and that such authorized uses constituted substantial noninfringing uses under Sony. Napster set up a "New Artist Program," pursuant to which new or unsigned artists could promote their works and distribute them in MP3 format via the Napster service. Napster accepted enrollment of new artists in its program only if the artist explicitly authorized Napster users to share the artist's music.[1426] The district court, however, held that "the New Artist Program may not represent a substantial or commercially significant aspect of Napster,"[1427] essentially ruling that it had been an afterthought: "[T]he court finds that the New Artist Program accounts for a small portion of Napster use and did not become central to defendant's business strategy until this action made it convenient to give the program top billing. An early version of the Napster website advertised the ease with which users could find their favorite popular music without 'wading through page after page of unknown artists.' Defendant did not even create the New Artist Program that runs on its Internet website until April 2000 – well after plaintiffs filed this action."[1428]

[1422] Id. 1079 (citations omitted).

[1423] Napster, 114 F. Supp. 2d at 915.

[1424] Id. at 916.

[1425] Napster I, 239 F.3d at 1019.

[1426] Napster, 114 F. Supp. 2d at 907.

[1427] Id. at 917. It is unclear why the court used the term "may," since that leaves open the possibility that the New Artist Program might constitute a substantial or commercially significant aspect of Napster, which in turn would affect the analysis under the Sony doctrine.

[1428] Id. at 904 (citations omitted). One of plaintiffs' experts submitted results of a sample of 1150 files on the Napster service, in which were contained only 11 new artists and 14 of their music files. Id.

In any event, the court concluded that, because it believed the activity under the New Artist Program to be separable from the infringing activity of the unauthorized distribution of the plaintiffs' works, the New Artist Program was insufficient to save Napster under the Sony doctrine: "Napster's primary role of facilitating the unauthorized copying and distribution of established artists' songs renders *Sony* inapplicable. … Because plaintiffs do not ask the court to shut down such satellite activities, the fact that these activities may be noninfringing does not lessen plaintiffs' likelihood of success."[1429]

In conclusion, the district court rejected applicability of the Sony doctrine on the ground that "any potential noninfringing use of the Napster service is minimal or connected to the infringing activity, or both. The substantial or commercially significant use of the services was, and continues to be, the unauthorized downloading and uploading of popular music, most of which is copyrighted."[1430]

On appeal in Napster I, the Ninth Circuit disagreed with the district court's overall conclusion that the Napster system was incapable of substantial noninfringing uses: "The district court improperly confined the use analysis to current uses, ignoring the system's capabilities. … Consequently, the district court placed undue weight on the proportion of current infringing uses as compared to current and future noninfringing use."[1431] The Ninth Circuit therefore concluded that the Napster system was in fact capable of substantial noninfringing uses.[1432] Nevertheless, for the reasons set forth in the next subsection, that conclusion was not sufficient to save Napster from liability under the Sony doctrine.

8. Ongoing Control by Napster Over Its Service. In addition to rejecting all of Napster's arguments of noninfringing uses of its system, the district court ruled that the Sony doctrine was inapplicable to Napster for one final reason – because Napster exercised ongoing control over its service (which was the same control that the court concluded provided a basis in part for its finding of both contributory and vicarious liability, as analyzed below). The plaintiffs had argued that the Sony doctrine was applicable only to the manufacture and sale of an article of commerce, and not to a service. Although the district court appears not to have accepted this device/service distinction per se, the district court did note that in Sony, the defendant's participation did not extend past the manufacturing and selling of the VCRs, and the defendant had no ongoing participation in the use of the devices to commit infringing acts:[1433]

> Courts have distinguished the protection *Sony* offers to the manufacture and sale of a device from scenarios in which the defendant continues to exercise control over the device's use. … Given defendant's control over the service, as opposed

---

[1429] Id. at 917. On appeal, the Ninth Circuit, with no further analysis, simply noted that the plaintiffs had not requested that Napster's New Artist Program be enjoined. Napster I, 239 F.3d at 1019.

[1430] Napster, 114 F. Supp. 2d at 912.

[1431] Napster I, 239 F.3d at 1021.

[1432] Id.

[1433] Napster, 114 F. Supp. 2d at 916-17.

to mere manufacturing or selling, the existence of a potentially unobjectionable use like space-shifting does not defeat plaintiffs' claims.[1434]

On appeal, the Ninth Circuit in Napster I also did not draw a distinction between a device and a service for purposes of applying the Sony doctrine, but rather, like the district court, distinguished between the Napster service itself and Napster's relation to the operational use of the system: "We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system."[1435] Thus, Napster could not be contributorily liable merely for offering a service that could be used for infringing uses, but could be liable if it had sufficient specific knowledge of use of the service for infringing purposes in particular instances.[1436] This knowledge requirement is discussed further in the next subsection.

9. The Elements of Contributory Liability. In order to establish contributory liability for the acts of direct infringement by Napster's users, the district court noted that the plaintiffs were required to show that Napster had knowledge of the infringing activity and that it induced, caused or materially contributed to the infringing conduct.[1437]

(i) The Knowledge Prong. With respect to the knowledge prong, the district court found the plaintiffs had presented convincing evidence that Napster had both actual and constructive knowledge of its users' infringements. The district court found actual knowledge because: (1) a document authored by a co-founder of Napster, Sean Parker, mentioned the need to remain ignorant of users' real names and IP addresses "since they are exchanging *pirated* music";[1438] and (2) the RIAA had informed Napster of more than 12,000 infringing music files being shared through the Napster system.[1439] Although Napster had terminated the accounts of the users offering those files, the district court noted that the songs were still available using the Napster service, as were other copyrighted works identified in the Schedules to the plaintiffs' complaint.[1440] The district court found constructive knowledge on Napster's part because: (1) Napster executives had recording industry experience; (2) Napster possessed enough sophistication about intellectual property laws to make claims against a rock band that copied its logo; (3) Napster executives had downloaded copyrighted songs from the system; and (4) they had promoted the site with screen shots listing infringing files.[1441]

[1434] Id. at 917 (citations omitted).

[1435] Napster I, 239 F.3d at 1020.

[1436] Id. at 1020-21.

[1437] Napster, 114 F. Supp. 2d at 918 (citing Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

[1438] 114 F. Supp. 2d at 918 (emphasis in original).

[1439] Id.

[1440] Id.

[1441] Id. at 919.

Napster had argued that the law of contributory infringement requires actual knowledge of specific acts of infringement (which Napster argued that it did not have),[1442] that mere generalized knowledge that the Napster system might be used for infringing transmissions was not sufficient for contributory liability, and that in every instance in which Napster received actual knowledge from the plaintiffs of infringing acts by a specific user, Napster had acted to terminate such infringing activity. The district court rejected this argument, ruling that actual knowledge of specific acts of infringement is not required for contributory liability, citing Gershwin Publ'g Corp. v. Columbia Artists Management, Inc.,[1443] which the court characterized as holding that general knowledge that third parties performed copyrighted works satisfied the knowledge element of contributory infringement. Accordingly, "the court rejects defendant's argument that titles in the Napster directory cannot be used to distinguish infringing from noninfringing files and thus that defendant cannot know about infringement by any particular user of any particular musical recording or composition."[1444]

The district court also rejected Napster's reliance on the following passage from the Netcom decision concerning contributory liability of service providers:

> Where a BBS [bulletin board service] operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.[1445]

The district court held that this language was dicta because the plaintiffs in that case raised a genuine issue of material fact regarding knowledge. But more importantly, the court ruled that Napster "is not an Internet service provider that acts as a mere conduit for the transfer of files."[1446]

One of the important issues on appeal was whether constructive knowledge is sufficient for contributory liability, or whether actual knowledge of infringing uses is required for liability.

[1442] Napster argued that it had no specific knowledge that any particular use of a file through its system was unauthorized. In particular, Napster argued that it could not know, any more than a photocopier or video recorder manufacturer, which uses of its system were fair or not. Napster further argued that it could not know the copyright status of its users' files. Neither CD audio files nor the resultant MP3 files carried any copyright notice or watermark. MP3 file names are created by users, contain errors, and are variable and undependable. Finally, Napster argued that song titles could not be used to distinguish authorized files from others because many song titles are used by multiple artists or there may be multiple recordings of the same work – some of which are authorized to be shared and others not. Napster's PI Opp. Br., supra note 1389, at 18-19.

[1443] 443 F.2d 1159, 1163 (2d Cir. 1971).

[1444] Napster, 114 F. Supp. 2d at 918.

[1445] Religious Technology Center v. Netcom Online Communication Services, Inc., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995).

[1446] Napster, 114 F. Supp. 2d at 919.

The Ninth Circuit in Napster I began its analysis of the knowledge prong by stating that contributory liability "requires that the secondary infringer 'know or have reason to know' of direct infringement."[1447] The Ninth Circuit also stated, "It is apparent from the record that Napster has knowledge, both actual and constructive, of direct infringement."[1448] Both of these statements suggest that constructive knowledge is sufficient to impose contributory liability on a service provider.

However, further analysis by the Ninth Circuit in its Napster I opinion suggests that constructive knowledge in the general sense that a service provider may know that its system could potentially be used for infringing purposes, is insufficient. Specifically, the Ninth Circuit stated, "We are bound to follow Sony, and will not impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights."[1449] Nevertheless, the Ninth Circuit found that "the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights."[1450]

The Ninth Circuit endorsed the analysis of the Netcom decision, "which suggests that in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement."[1451] The reference to "actual knowledge" raises the question whether the Ninth Circuit meant to exclude constructive knowledge as being sufficient. However, the Ninth Circuit went on to state that the "court [in Netcom] determined that for the operator to have sufficient knowledge, the copyright holder must 'provide the necessary documentation to show there is likely infringement.'"[1452] From this statement, it appears that specific notice from the copyright holder of activity on the service sufficient to show that there is "likely" infringement can constitute "reason to know." Thus, the form of constructive knowledge the Ninth Circuit in Napster I appears to contemplate as giving rise to potential liability is only one that flows from very specific notice by a copyright holder of particular potentially infringing activity on the service. What is unclear, however, as further analyzed below, is the extent to which, once a service provider has been notified of a particular infringing instance of a work on the service, the service provider then has "constructive knowledge" of the presence of that work on its service that gives rise to a duty to police for other infringing occurrences of that work on the system.

Summarizing its endorsement of the Netcom approach, the Ninth Circuit ruled in Napster I that "if a computer system operator learns of specific infringing material on his system and fails

---

[1447] Napster I, 239 F.3d at 1020 (citing Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845 & 846 n.29 (11th Cir. 1990).

[1448] Napster I, 239 F.3d at 1020.

[1449] Id. at 1020-21.

[1450] Id. at 1021.

[1451] Id. (citing Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361, 1371 (N.D. Cal. 1995)).

[1452] Napster I, 239 F.3d at 1021 (quoting Netcom, 907 F. Supp. at 1374).

to purge such material from the system, the operator knows of and contributes to direct infringement. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[1453] The Ninth Circuit concluded that the record established sufficient knowledge to impose contributory liability on Napster "when linked to demonstrated infringing use of the Napster system. The record supports the district court's finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material."[1454] Again, the Ninth Circuit's reference to "actual" knowledge raises confusion about the extent to which constructive knowledge can give rise to contributory liability.

(ii) The Material Contribution Prong. With respect to the material contribution prong of the contributory liability test, the district court ruled that Napster had materially contributed to the infringing acts of its users. For support, the court cited Fonovisa, Inc. v. Cherry Auction, Inc.,[1455] in which the owners of copyrights for musical recordings stated a contributory infringement claim against the operators of a swap meet at which independent vendors sold counterfeit recordings, because it would have been difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet. The district court found that Napster was essentially an Internet swap meet and that Napster was materially contributing to the infringing activity of its users by supplying the MusicShare software, search engine, servers, and means of establishing a connection between users' computers.[1456] "Without the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts."[1457]

On appeal in Napster I, the Ninth Circuit found that the district court had correctly applied the reasoning of Fonovisa. "We agree that Napster provides 'the site and facilities' for direct infringement."[1458] The Ninth Circuit's view of the material contribution prong appears to be very broad sweeping, for it would seem that all service providers provide "the site and facilities" for any direct infringement that may occur on the service. If this is the only test for material contribution, it may be difficult for a service provider to use the material contribution prong as a defense to common law contributory liability.

[1453] Napster I, 239 F.3d at 1021 (citations omitted).

[1454] Id. at 1022 (citations omitted; emphasis in original). The second element in the second sentence – that Napster could block access to the system by suppliers of infringing material – hints of a requirement of "control" over the infringing activity in the contributory liability analysis. As analyzed below with respect to the imposition of vicarious liability on Napster, a "control" test has generally been relevant only to vicarious liability. It is unclear whether the Ninth Circuit really meant to introduce a new "control" test into contributory liability.

[1455] 76 F.3d 259 (9th Cir. 1996).

[1456] Napster, 114 F. Supp. 2d at 919-20.

[1457] Id. at 920.

[1458] Napster I, 239 F.3d at 1022.

10. The Elements of Vicarious Liability and the Duty to Police.[1459] In order to establish vicarious liability for the acts of direct infringement by Napster's users, the district court noted that the plaintiffs were required to show that Napster had the right and ability to supervise the infringing activity of its users and had a direct financial interest in such activity.[1460] Napster argued that it did not have the ability to supervise the allegedly infringing activity because it was impossible to police the activity of each of its individual users. Napster argued that it could never know the use to which a particular file was put on its system, and thus could not control whether a use was fair or not. Napster also pointed to Section 512(m) of the DMCA,[1461] which provides that a service provider has no affirmative duty to police its users, and cannot be expected to monitor individual users until put on notice by the copyright holder of particular alleged infringing materials. Napster argued that, were service providers required affirmatively to identify and exclude all copyrighted materials, there could be no file sharing or, indeed, even a World Wide Web.[1462] Napster also argued that it received no direct financial benefit from the infringing activity, but at most only a generalized financial benefit, since the many noninfringing uses of the Napster system drew many users to its system.[1463]

The district court rejected these arguments and ruled that Napster was vicariously liable. The court found that Napster's ability to block users about whom rights holders complain was "tantamount to an admission that defendant can, and sometimes does, police its service."[1464] The court ruled that a defendant need not exercise its supervisory powers to be deemed capable of doing so. The district court also held that the plaintiffs had shown a reasonable likelihood that Napster had a direct financial interest in the infringing activity, citing documents stating that Napster would derive revenues directly from increases in its user base and deposition testimony by Napster's former President that the Napster service attracted more and more users by offering an increasing amount of quality music for free. The court found this to be similar to the type of direct financial interest that the Ninth Circuit found sufficient for vicarious liability in the Fonovisa case. Accordingly, the district court ruled that the plaintiffs had shown a reasonable likelihood of success on their vicarious infringement claims.[1465]

The Ninth Circuit's rulings on appeal in Napster I with respect to the vicarious liability issue are some of the most significant holdings in the case. In a very important initial ruling, the

---

[1459] Although the issue of online vicarious liability is treated generally in Section III.C.3 below, the vicarious liability issues in the Napster case will be treated here in order, for clarity, to present the entire analysis of secondary liability issues involved in the case in a single place.

[1460] Napster, 114 F. Supp. 2d at 920.

[1461] That section provides as follows: "Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) [the safe harbors] on – (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)." 17 U.S.C. § 512(m)(1).

[1462] Napster's PI Opp. Brief, supra note 1389, at 20-21.

[1463] Id. at 21.

[1464] Napster, 114 F. Supp. 2d at 921.

[1465] Id. at 921-22.

Ninth Circuit held that the "staple article of commerce" doctrine of Sony has *no* applicability to vicarious liability. This ruling seems a bit odd, since the Sony opinion uses the phrase "vicarious liability" several times. The Ninth Circuit acknowledged as much, but concluded that "when the Sony Court used the term 'vicarious liability,' it did so broadly and outside of a technical analysis of the doctrine of vicarious copyright infringement." Under this holding, it appears that the Sony doctrine will not afford any immunity to service providers from vicarious liability.

The Ninth Circuit's view of the vicarious liability doctrine was broad on both the financial benefit and supervision prongs. With respect to the financial benefit prong, the Ninth Circuit, citing Fonovisa, agreed with the district court that "financial benefit exists where the availability of infringing material 'acts as a "draw" for customers.'"[1466] The Ninth Circuit relied on the district court's finding that more users register with the Napster system as the quality and quantity of available music increases.[1467]

With respect to the supervision prong, the Ninth Circuit noted that "Napster has an express reservation of rights policy, stating on its website that it expressly reserves the 'right to refuse service and terminate accounts in [its] discretion, including, but not limited to, if Napster believes that user conduct violates applicable law … or for any reason in Napster's sole discretion, with or without case.'"[1468] The Ninth Circuit ruled that this reservation of rights policy was, of itself, sufficient evidence of Napster's right and ability to supervise its users' conduct, and (in one of the most important aspects of the entire opinion), gave rise to a *duty to police* the Napster system: "To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability."[1469]

This holding raises a number of significant issues. First, the ruling that a reservation of rights policy by itself satisfies the supervision prong of the vicarious liability test puts service providers in a potential Catch 22 situation with the DMCA. As discussed further below, under Section 512(i) of the DMCA, in order to be eligible for the safe harbors of the DMCA, a service provider must adopt and reasonably implement a "policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." Under the Ninth Circuit's ruling in Napster I, however, the adoption of such a policy would seem to expose the service provider to vicarious liability under the supervision prong. The service provider is therefore put in a Catch 22 – whether it should avoid adoption of a reservation of rights policy in order to avoid common law liability, thereby potentially giving up its DMCA safe harbors, or preserve its DMCA safe harbors by adopting such a policy, thereby potentially increasing its exposure to vicarious liability.

[1466] Napster I, 239 F.3d at 1023 (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996)).

[1467] Napster I, 239 F.3d at 1023.

[1468] Id.

[1469] Id.

Second, the duty to police seems contrary to Section 512(m) of the DMCA, which states that a service provider need not "monitor[] its service or affirmatively seek[] facts indicating infringing activity, except to the extent consistent with a standard technical measure" in order to be eligible for the DMCA safe harbors. Thus, the Ninth Circuit's opinion in Napster I seems to require that a service provider do more than is required by the DMCA in order to avoid common law secondary liability.

Third, the Ninth Circuit did not specifically define what constitutes a "detectable" act of infringement, and the scope of the duty to police for such acts is therefore unclear under its opinion. The Ninth Circuit noted, however, that the district court's original injunction (discussed in detail in subsection 13 below) had gone too far in what it required Napster to do. The district court's original injunction ruled that "Napster bears the burden of developing a means to comply with the injunction," which would have required Napster to develop new blocking technology that did not exist in its system. The preliminary injunction further required that Napster "must insure that no work owned by plaintiffs which neither defendant nor Napster users have permission to use or distribute is uploaded or downloaded on Napster."

The Ninth Circuit ruled in Napster I that this preliminary injunction went too far in the burden it placed on Napster to police. Analogizing to the Fonovisa case, which imposed secondary liability on the operator of the swap meet because the operator had the right and ability to police the premises of the swap meet, the Ninth Circuit ruled that the district court "failed to recognize that the boundaries of the premises that Napster 'controls and patrols' are limited. … Put differently, Napster's reserved 'right and ability' to police is cabined by the system's current architecture. As shown by the record, the Napster system does not 'read' the content of indexed files, other than to check that they are in the proper MP3 format."[1470] The Ninth Circuit went on to rule that Napster's duty to police must be limited by the existing architecture of its system:

> Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. The file name indices, therefore, are within the "premises" that Napster has the ability to police. We recognize that the files are user-named and may not match copyrighted material exactly (for example, the artist or song could be spelled wrong). For Napster to function effectively, however, file names must reasonably or roughly correspond to the material contained in the files, otherwise no user could ever locate any desired music. As a practical matter, Napster, its users and the record company plaintiffs have equal access to infringing material by employing Napster's "search function."[1471]

This passage suggests that Napster's obligations to police its system for infringing files was to be limited to monitoring the names of files made available for sharing by Napster users using the existing search function of the Napster system, which the Ninth Circuit noted was

---

[1470] Id. at 1023-24.

[1471] Id. at 1024.

equally available to both the plaintiffs and Napster for policing for infringing files. Unlike the district court's original preliminary injunction, then, the Ninth Circuit in Napster I did not contemplate that Napster would be required to develop new technology for policing not based on file name searches (such as digital "fingerprinting" of the content of files or other techniques).

11. Summary of Secondary Liability Under the Ninth Circuit's Decision. At the end of its opinion in Napster I, the Ninth Circuit offered the following summary of its standard for contributory liability and vicarious liability:

> [C]ontributory liability may potentially be imposed only to the extent that Napster: (1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings; (2) knows or should know that such files are available on the Napster system; and (3) fails to act to prevent viral distribution of the works. The mere existence of the Napster system, absent actual notice and Napster's demonstrated failure to remove the offending material, is insufficient to impose contributory liability.
>
> Conversely, Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. Napster has both the ability to use its search function to identify infringing musical recordings and the right to bar participation of users who engage in the transmission of infringing files.[1472]

This summary replicates many of the ambiguities noted earlier with respect to (i) whether constructive knowledge is sufficient for liability (the summary first speaks of "knowledge of specific infringing files" but then speaks of whether Napster "should know" that such files are available on its system) and (ii) the scope of the duty to police (the summary speaks of blocking access to "potentially" infringing files without defining when a file is "potentially" infringing, and of preventing "viral distribution" of "works," without saying whether, by use of the term "works," it meant to reference only particular files of which Napster has notice, or any files that may contain the copyrighted "work").

12. Other Defenses Raised by Napster Rejected by the District Court and the Ninth Circuit.[1473] The court also rejected a number of other miscellaneous defenses to liability that Napster had raised, which may be summarized briefly as follows:

(i) First Amendment. Napster argued that the requested injunction would impose an overbroad prior restraint on its free speech rights to publish a directory of where files were located on its users' computers, as well as that of its users and the unsigned artists who depend on the Napster service to gain exposure by distributing their music through Napster. The district court rejected this argument, finding that free speech concerns "are protected by and coextensive

---

[1472] Id. at 1027 (citations omitted).

[1473] Napster also raised defenses under the safe harbors of the DMCA, which are discussed in Section III.C.6(b) below.

with the fair use doctrine."[1474] The parties sharply disputed the extent to which infringing and noninfringing aspects of the Napster service were separable, and whether it was therefore practical for the court to enjoin only the infringing aspects. The district court ruled, however, that even if it were "technologically impossible for Napster, Inc. to offer such functions as its directory without facilitating infringement, the court still must take action to protect plaintiffs' copyrights."[1475] On appeal in Napster I, the Ninth Circuit, in a very terse analysis of the First Amendment issue, simply ruled that "First Amendment concerns in copyright are allayed by the presence of the fair use doctrine. … Uses of copyrighted material that are not fair uses are rightfully enjoined."[1476]

(ii) Copyright Misuse. Napster argued that the plaintiff record labels were engaged in copyright misuse by attempting to aggrandize their monopoly beyond the scope of their copyrights by restricting the flow of unsigned artists' music, which competed with their own, and by controlling the distribution of music over the Internet. The district court rejected this argument, concluding that most of the copyright misuse cases involved the attempt to enlarge a copyright monopoly through restricted or exclusive licensing, and the plaintiffs in the instant case had granted no licenses to Napster, let alone impermissibly restrictive ones.[1477] On appeal in Napster I, the Ninth Circuit affirmed the ruling of the district court, finding no evidence that the plaintiffs sought to control areas outside their grant of monopoly. "Rather, plaintiffs seek to control reproduction and distribution of their copyrighted works, exclusive rights of copyright holders."[1478] In a footnote, however, the Ninth Circuit did note that the copyright misuse doctrine is not limited entirely to situations of restrictive licensing – "a unilateral refusal to license a copyright may constitute wrongful exclusionary conduct giving rise to a claim of misuse, but [we] assume that the 'desire to exclude others … is a presumptively valid business justification for any immediate harm to consumers."[1479]

(iii) Waiver. Napster asserted that the plaintiffs had waived their right to enforce their copyrights against Napster. Napster introduced evidence that the plaintiffs had known of the existence of "ripping" software for creating MP3 files for years, and had known that making MP3 files from CDs was the most prevalent means by which sound recordings became available for transfer over the Internet in the first place, yet had failed to take any actions to stop or even slow its widespread proliferation, and indeed had actively formed partnerships with and invested in companies that directed consumers to MP3 encoding software that would enable them to transfer music files over the Internet.[1480] The district court responded as follows:

[1474] Napster, 114 F. Supp. 2d at 922 (citing Nihon Keizai Shimbun, Inc. v. Comline Bus. Data, Inc., 166 F.3d 65, 74 (2d Cir. 1999)).

[1475] Napster, 114 F. Supp. 2d at 923.

[1476] Napster I, 239 F.3d at 1028.

[1477] Napster, 114 F. Supp. 2d at 923.

[1478] Napster I, 239 F.3d at 1027.

[1479] Id. at 1027 n.8 (citing Image Tech. Servs. V. Eastman Kodak Co., 125 F.3d 1195, 1218 (9th Cir. 1997)).

[1480] Napster's PI Opp. Brief, supra note 1389, at 22.

> This limited evidence fails to convince the court that the record companies created the monster that is now devouring their intellectual property rights. Although plaintiffs have not sued their business partners for contributory infringement, they typically have asked them to discourage unauthorized ripping and have made security part of their agreements. Defendant fails to show that, in hastening the proliferation of MP3 files, plaintiffs did more than seek partners for their commercial downloading ventures and develop music players for files they planned to sell over the Internet.[1481]

On appeal in Napster I, the Ninth Circuit affirmed this ruling, citing the district court's finding that "in hastening the proliferation of MP3 files, plaintiffs did [nothing] more than seek partners for their commercial downloading ventures and develop music players for files they planned to sell over the Internet."[1482]

(iv) Failure to Present Evidence of Copyright Registration. Finally, Napster argued that, under section 411(a) of the copyright statute,[1483] in order to claim infringement of multiple works, the plaintiffs were required to specify the works with particularity and provide proof of copyright registration for those works. Napster noted that the plaintiffs had identified only a discrete number of works allegedly infringed, together with their registration numbers, in a Schedule to their complaint, and argued that the plaintiffs had no jurisdiction to assert the copyrights in other unidentified works. The court rejected this argument, citing a 1990 case from the D.C. Circuit as authority for the proposition that a court may enter an injunction in a copyright case covering works owned by the plaintiff but not in suit, particularly where there has been a history of continuing infringement and there exists a significant threat of future infringement.[1484]

On appeal in Napster I, the Ninth Circuit failed to address this argument directly. Instead, it simply ruled that the plaintiffs had sufficiently demonstrated "ownership" for purposes of a prima facie case of direct infringement, quoting the district court's statement that "as much as eighty-seven percent of the files available on Napster may be copyrighted and more than seventy percent may be owned or administered by plaintiffs."[1485]

13. The Mar. 5, 2001 Preliminary Injunction. The district court ruled that, because the plaintiffs had shown a reasonable likelihood of success on the merits of their contributory and vicarious[1486] copyright infringement claims, they were entitled to a presumption of irreparable

---

[1481] Napster, 114 F. Supp. 2d at 924.

[1482] Napster I, 239 F.3d at 1026.

[1483] That section provides that "no action for infringement of the copyright in any work shall be instituted until registration of the copyright claim has been made in accordance with this title." 17 U.S.C. §411(a).

[1484] Napster, 114 F. Supp. 2d at 925 (citing Walt Disney Co. v. Powell, 897 F.2d 565, 568 (D.C. Cir. 1990)).

[1485] Napster I, 239 F.3d at 1013 (quoting Napster, 114 F. Supp. 2d at 911) (emphasis added). It is puzzling why a showing that a certain percentage of the works on Napster "may" be copyrighted and "may" be owned by plaintiffs is sufficient to meet the very specific jurisdictional requirements of 17 U.S.C. § 411(a).

[1486] The court's rationale for its rejection of Napster's defense under the safe harbors of the DMCA is discussed in Section III.C.6 below.

harm, and a preliminary injunction should issue. The district court therefore enjoined Napster "from engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of the rights owner."[1487] The court further noted that "[b]ecause defendant has contributed to illegal copying on a scale that is without precedent, it bears the burden of developing a means to comply with the injunction. Defendant must insure that no work owned by plaintiffs which neither defendant nor Napster users have permission to use or distribute is uploaded or downloaded on Napster. The court ORDERS plaintiffs to cooperate with defendant in identifying the works to which they own copyrights."[1488]

On July 28, 2000 (the day the district court had set for the preliminary injunction to go into effect), the Ninth Circuit issued a stay of the injunction, noting that the case "raised substantial questions of first impression going to both the merits and the form of the injunction."[1489] As discussed above, the Ninth Circuit ultimately ruled in Napster I that the district court's original preliminary injunction was overbroad, and remanded the case for entry of a narrower preliminary injunction consistent with the Ninth Circuit's opinion. Napster subsequently filed a petition with the Ninth Circuit for rehearing *en banc*, which was denied by order dated June 22, 2001.

On remand, both the plaintiffs and Napster each submitted proposed preliminary injunctions. On March 5, 2001, the district court entered a revised, narrower preliminary injunction requiring the plaintiffs to give notice to Napster of specific infringing file names on the Napster system and requiring Napster to block access to those file names through its search index, as well as reasonable variants of such file names that the parties might generate. The modified preliminary injunction required use of Napster's file name search function as the centerpiece of Napster's duty to police. The district court also permitted the record company plaintiffs to submit notices to Napster of new sound recordings in advance of their release, and required Napster to make efforts to do prophylactic blocking of such new recordings. Specifically, the revised preliminary injunction provided as follows in pertinent part:[1490]

> "Plaintiffs shall provide notice to Napster of their copyrighted sound recordings by providing for each work:
>
> (A) the title of the work;
> (B) the name of the featured recording artist performing the work ("artist name");
> (C) the name(s) of one or more files available on the Napster system

[1487] Napster, 114 F. Supp. 2d at 927.

[1488] Id. The court ordered the plaintiffs to post a bond in the amount of $5 million – far below what Napster had requested – to compensate Napster for losses in the event that the injunction was reversed or vacated. Id.

[1489] Order, A&M Records, Inc. v. Napster, Inc., No. 00-16401, 2000 U.S. App. LEXIS 18688 (9th Cir. July 28, 2000).

[1490] The text of the complete preliminary injunction may be found at 2001 U.S. Dist. LEXIS 2186 (N.D. Cal. Mar. 5, 2001).

containing such work; and

(D) a certification that plaintiffs own or control the rights allegedly infringed.

Plaintiffs shall make a substantial effort to identify the infringing files as well as the names of the artist and title of the copyrighted recording."[1491]

"All parties shall use reasonable measures in identifying variations of the filename(s), or of the spelling of the titles or artists' names, of the works identified by plaintiffs. If it is reasonable to believe that a file available on the Napster system is a variation of a particular work or file identified by plaintiffs, all parties have an obligation to ascertain the actual identity (title and artist name) of the work and to take appropriate action within the context of this Order."[1492]

"The Ninth Circuit held that the burden of ensuring that no copying, downloading, uploading, transmitting or distributing of plaintiffs' copyrighted works occurs on the system is shared between the parties. The court 'place[d] the burden on plaintiffs to provide notice to Napster' and imposed on Napster the burden 'of policing the system within the limits of the system.' It appears to the court on the basis of the factual representations by the parties at the March 2, 2001 hearing that it would be difficult for plaintiffs to identify all infringing files on the Napster system given the transitory nature of its operation. This difficulty, however, does not relieve Napster of its duty. The court anticipates that it may be easier for Napster to search the files available on its system at any particular time against lists of copyrighted recordings provided by plaintiffs. The court deems that the results of such a search provide Napster with 'reasonable knowledge of specific infringing files' as required by the Ninth Circuit."[1493]

"Once Napster 'receives reasonable knowledge' from any sources identified in preceding Paragraphs … of specific infringing files containing copyrighted sound recordings, Napster shall, within three (3) business days, prevent such files from being included in the Napster index (thereby preventing access to the files corresponding to such names through the Napster system)."[1494]

"Within three (3) business days of receipt of reasonable notice of infringing files, Napster shall affirmatively search the names of all files being made available by all users at the time those users log on (i.e., prior to the names of files being

---

[1491] Id. ¶ 2.

[1492] Id. ¶ 3.

[1493] Id. ¶ 4 (citations omitted).

[1494] Id. ¶ 5.

included in the Napster index) and prevent the downloading, uploading, transmitting or distributing of the noticed copyrighted sound recordings."[1495]

"Plaintiffs may provide to Napster in advance of release the artist name, title of the recording, and release date of sound recordings for which, based on a review of that artist's previous work, including but not limited to popularity and frequency of appearance on the Napster system, there is a substantial likelihood of infringement on the Napster system. Napster shall beginning with the first infringing file block access to or through its system to the identified recording. As Napster presently has the capability (even without enhancing its technology) to store information about and subsequently screen for a particular recording, the burden is far less and the equities are more fair to require Napster to block the transmission of these works in advance of their release. To order otherwise would allow Napster users a free ride for the length of time it would take plaintiffs to identify a specific infringing file and Napster to screen the work."[1496]

Napster appealed, and the plaintiffs cross-appealed, the Mar. 5 modified preliminary injunction of the district court.

14. The Apr. 26, 2001 Clarification of the Preliminary Injunction. Many disputes between the plaintiffs and Napster quickly arose over the meaning and obligations imposed on the parties by the Mar. 5 modified injunction. First, the parties disputed whether the plaintiffs were required to provide notice to Napster of the names of specific files available on the Napster system containing the plaintiffs' copyrighted sound recordings.[1497] The plaintiffs argued that the Ninth Circuit's decision in Napster I required them to provide specific filenames only in support of their claims for contributory infringement, and not in support of their claims for vicarious liability, based on the following passage from Napster I:

The preliminary injunction we stayed is overbroad because it places on Napster the entire burden of ensuring that no "copying, downloading, uploading, transmitting, or distributing" of plaintiffs' works occur on the system. As stated, we placed the burden on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content. Napster, however, also bears the burden of policing the system within the limits of the system. Here, we recognize that this is not an exact science in that the files are user named. In crafting the injunction on remand, the district court should recognize that

---

[1495] Id. ¶ 6. It is unclear what the difference is between the requirements of this paragraph and that of the previous paragraph. The district court may not have fully understood that the steps recited in this paragraph would be the same steps that Napster would take to comply with the previous paragraph.

[1496] Id. ¶ 7.

[1497] Memorandum, In re Napster, Inc. Copyright Litigation, MDL No. C 00-1369 MHP (N.D. Cal. Apr. 26, 2001), at 1.

> Napster's system does not currently appear to allow Napster access to users' MP3 files.[1498]

The plaintiffs read this passage in two parts: First, they read that portion placing the "burden on plaintiffs to provide notice to Napster … before Napster has the duty to disable access to the offending content," as relating only to claims for contributory infringement; and second, that portion imposing on Napster the "burden of policing the system within the limits of the system," as relating only to claims of vicarious infringement. Plaintiffs therefore maintained that they were required to provide specific file names only to obtain preliminary relief on their claims of contributory infringement, but did not need to provide filenames to obtain preliminary relief on their claims of vicarious infringement.[1499] The district court, although noting that the plaintiffs' reading of the paragraph might be "a prescient reading," nevertheless rejected it because the plain language of the paragraph did not allow for two separate standards, but rather "only one with several elements."[1500]

The parties also disputed whether the provision of the Mar. 5 modified injunction regarding the availability of the plaintiffs' copyrighted works prior to the official release of those works adequately resolved the plaintiffs' concerns. To aid its resolution of this issue, the court requested the parties to submit declarations of persons who could assist the court in understanding how far in advance of release the record companies generally knew that a particular recording would be released on a specific date.[1501] Finally, the parties disagreed as to the present and future capabilities of the Napster system to screen the plaintiffs' copyrighted works. The court appointed a neutral expert, Dr. A. J. Nichols, to serve as a technology advisor in the matter, and requested that he work with the parties' technology experts and prepare a report to the court on the present and future capabilities of the Napster system to screen the plaintiffs' copyrighted works.[1502]

15. The July 11, 2001 Oral Modification of the Preliminary Injunction. Even after the Apr. 26 clarification, the parties continued to dispute bitterly the scope of the obligation on the part of the plaintiffs to supply filenames to Napster, as well as Napster's compliance with the modified preliminary injunction. The plaintiffs alleged that infringing files were still rampant on the Napster system, while Napster insisted that it was adequately blocking all filenames of which it had been made aware by the plaintiffs, as well as many variants of those filenames, including all files containing the names of many particular artists that had been noticed as illegally appearing on the system, and all files having titles or variants of those titles alleged to be infringing, regardless of the artist performing a work by that title – thereby resulting in substantial "overblocking" of files on the system.

[1498] Id. at 1-2 (quoting Napster I, 239 F.3d at 1027).

[1499] Memorandum at 2.

[1500] Id.

[1501] Id.

[1502] Id.

During the months ensuing after the Apr. 26 clarification, Dr. Nichols issued a series of reports to the district court concerning Napster's ability to remove infringing files from its system. Also during this time, Napster voluntarily developed and switched to a new technology known as "fileID" for blocking allegedly infringing files from the Napster system. The new technology, unlike the old, was not based primarily on filenames, but rather on a technical analysis of the digital musical content contained in a file, including acoustic waveform recognition, to generate a "fingerprint." The parties disputed the effectiveness of the new technology and whether Napster's use of this technology was sufficient to comply with the modified preliminary injunction. The plaintiffs insisted that the preliminary injunction required Napster's system to be 100% free of infringing files, and that there was still infringing material being shared through the system. Napster insisted, however, that no technology could ever be 100% accurate in screening out allegedly infringing materials from its system, and that neither the preliminary injunction, nor the Ninth Circuit's decision in Napster I, required its system to be 100% infringement free. Instead, Napster insisted that it was required to exert only reasonable efforts to block infringing material from its system, and only within the limits of the architecture of its system.

On July 1, 2001, Napster voluntarily shut down the file sharing operation of its system, after discovering flaws in its fileID fingerprinting technology, and conducted testing on its technology between July 2 and 9. The parties' disputes over Napster's compliance with the Mar. 5 modified injunction came to a head at a status conference before the district court on July 11, 2001. At that hearing, Napster told the court that, based on its testing, its newly implemented fileID technology was more than 99% effective and that it was prepared to resume allowing file sharing through its system.[1503]

The district court rejected Napster's proposal to resume file sharing, stating from the bench, "I think we're at a point where it has to stay that way [i.e., file sharing shut down] until you satisfy Dr. Nichols and me that when the system goes back up it will be able to block out or screen out copyrighted works that have been noticed."[1504] Napster pressed the district court to clarify whether the Mar. 5 modified injunction was meant to require its system to be 100% accurate in screening of allegedly infringing materials. The court ruled orally as follows: "It's not good enough until every effort has been made to, in fact, get zero tolerance. Now that has to be the objective. If there's a little – it gets a little messy around edges, if there are some glitches and so forth, I can understand that. But this system is not going to go back up in such a manner as to permit copying and downloading other than to test that for the purposes of determining the error rate until you've satisfied Dr. Nichols. And then, he can notify me."[1505]

The district court denied Napster's request to stay her oral modified order and Napster immediately requested the Ninth Circuit to issue a stay. On July 18, 2001, the Ninth Circuit ordered "that the order issued by the district court on July 11, 2001, in open court, modifying the

---

[1503] "Napster Asks 9th Circuit to Modify 1 Order, Vacate Another," *Mealey's Cyber Tech & E-Commerce Litigation Reporter* (Aug. 2001) 4-5.

[1504] Id. at 5.

[1505] Id.

Preliminary Injunction issued March 5, 2001, is hereby stayed pending a further order of this court."[1506] Despite the stay of the district court's oral modified order, Napster chose not to resume file sharing through its system.

Both Napster and the plaintiffs pursued further appeals to the Ninth Circuit in view of the July 11 oral order. The Ninth Circuit consolidated those appeals with the earlier appeals of the Mar. 5 modified injunction. Its opinion in the consolidated appeals is discussed in subsection 17 below.

16. Napster's Motions to Dismiss the Complaints of the Independent Artists and AMPAS. While the consolidated appeals were pending, Napster filed a motion to dismiss the complaints of various independent artists and labels and of AMPAS for failure to state a claim. Napster based its motion on the Ninth Circuit's opinion in Napster I, which Napster argued fundamentally altered copyright liability in the online context.[1507] Napster framed the basis for its motion as a pure question of law – whether notice is an element of contributory and vicarious copyright infringement – and rested the motion on the following two arguments:

> First, Napster contends that [Napster I] held that the traditional formulation of constructive knowledge for contributory infringement does not apply in the digital realm. Instead, copyright liability may only be imposed when a computer service provider has actual knowledge of specific infringing files. Second, Napster believes that the Ninth Circuit held that notice is a required element for both contributory and vicarious infringement. This notice, Napster contends, must be provided (1) by plaintiffs (2) prior to suit and (3) must list specific infringing files. Additionally, Napster reads [Napster I] to limit liability for contributory and vicarious infringement to cases in which after receiving notice, Napster fails to disable the infringing material. Simply put, Napster believes that the Ninth Circuit carved out a special niche in copyright law for computer service providers.[1508]

In response, the district court ruled that "there is a simple answer to Napster's 'pure question of law.' There is no requirement that plaintiffs allege that they provided notice of specific infringing works prior to filing suit. The court agrees that computer system operators cannot be held liable for secondary copyright liability based *solely* on the transmission of unidentified (and unidentifiable) material through a computer system. To do otherwise would violate the basic tenet of Sony. However, according to plaintiffs' complaints, Napster has gone far beyond simply providing a peer-to-peer file sharing system; it has engaged in music piracy of magnificent proportions."[1509] Accordingly, the court concluded that the plaintiffs had

---

[1506] Order, A&M Records, Inc. v. Napster, Inc., No. 01-16308 (9th Cir. July 18, 2001).

[1507] Fonovisa v. Napster, Inc., 2002 U.S. Dist. LEXIS 4270 (N.D. Cal. Jan. 28, 2002), at *11.

[1508] Id. at *11-12.

[1509] Id. at *38-39 (emphasis in original).

sufficiently pleaded the elements of contributory and vicarious infringement, and denied Napster's motion.[1510]

The court based its conclusions on various significant interpretations of the Napster I opinion with respect to contributory and vicarious liability. With respect to contributory liability, the court noted that under Napster I, the secondary infringer must "know or have reason to know" of the direct infringement; "[a]ctual knowledge is not required; a defendant may possess constructive knowledge if he has reason to know a third party's direct infringement."[1511] The district court rejected Napster's argument that Napster I created a stricter standard of knowledge for service providers in an online context – namely, actual knowledge in the form of notice of specific copyrighted works from the plaintiffs prior to suit. Napster argued that it could not be held liable until such notice was given because its duty under Napster I to disable the offending material arose only after the plaintiffs provided notice.[1512] The court ruled that "[c]ontrary to Napster's contention, Napster I did not create a new knowledge standard for contributory infringement. Instead, the court relied on the traditional formulation that either constructive or actual knowledge is sufficient to impose liability on Napster for contributory infringement."[1513]

The district court acknowledged some lack of clarity in the Ninth Circuit's Napster I opinion on the issue of knowledge, as discussed earlier in this paper: "The court is aware that the Ninth Circuit's reference to actual knowledge and failure to remove access might lead to some confusion. Lacking a more definitive statement from the Court of Appeals, the court understands the Ninth Circuit to hold that a range of conduct, when linked to Napster's system, may give rise to constructive or actual knowledge. Conduct sufficient for liability may take forms other than as a combination of actual knowledge and failure to block access. … Plaintiffs allege that Napster knew of music piracy on its system, that it had the ability to patrol its database, that Napster had knowledge of some specific infringing files, and did nothing to prevent continued infringement. If these allegations are true, plaintiffs are entitled to at least preliminary injunctive relief under the reasoning of [Napster I]."[1514]

With respect to vicarious liability, the court noted that Napster had not challenged the plaintiffs' allegations of control and financial interest, but instead had argued that notice is an additional required element for both vicarious and contributory copyright infringement on the part of online service providers.[1515] The court therefore turned to the issue of notice as a separate element of secondary infringement. Napster based its notice argument on the Ninth Circuit's modification in Napster I of the district court's original July 2000 preliminary injunction as being overbroad and its statement that "the burden [is] on plaintiffs to provide notice to Napster of

---

[1510] Id. at *39.

[1511] Id. at *14-15.

[1512] Id. at *15-16.

[1513] Id. at *16.

[1514] Id. at *23-24.

[1515] Id. at *26.

copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content."[1516] Napster argued that this statement mandated notice as a necessary element of secondary infringement, and that any complaint failing to allege both notice prior to suit and Napster's subsequent failure to disable infringing material was deficient.[1517]

The district court found Napster's interpretation of the Ninth Circuit's opinion to be problematic:

> First, Napster reads the statement out of context. The burden-shifting statement upon which Napster relies addressed only the scope of injunctive relief. The Ninth Circuit was clearly concerned with the overbreadth of the injunction and believed that any liability based solely on the architecture of Napster's system implicated Sony. In tailoring injunctive relief to avoid violating Sony, the Ninth Circuit shifted the burden to plaintiffs to provide notice of specific infringing works and files. This burden-shifting alleviated concerns that Napster was being penalized simply because of its peer-to-peer file sharing system. More fundamentally, the Ninth Circuit's modification balanced the broad equitable discretion of this court with the doctrine that injunctive relief should avoid prohibiting legitimate conduct. … Simply put, the Ninth Circuit's burden-shifting is case-specific, designed to alleviate Sony concerns.[1518]

Moreover, the district court was troubled that Napster's argument might imply that even if it had actual knowledge of specific infringement, Napster could simply wait until the plaintiffs discovered the infringement and then remove the offending files. The court believed such an argument would turn copyright law on its head and encourage willful blindness.[1519] Finally, the court expressed the belief that, had the Ninth Circuit intended to overhaul copyright liability and carve out special protections for computer service providers, "it would have explicitly stated such a change."[1520] Accordingly, the court concluded that the plaintiffs had adequately pleaded claims for contributory and vicarious liability.[1521]

[1516] Id. at *28-29 (quoting Napster I, 239 F.3d at 1027).

[1517] Fonovisa v. Napster, 2002 U.S. Dist. LEXIS 4270, at *29.

[1518] Id. at *30.

[1519] Id. at *31.

[1520] Id. at *33. The court also rejected Napster's interpretation of the Netcom decision, discussed in Section II.A.4(a) above, as requiring notice of specific infringing files prior to filing suit. "Notice was an issue in Netcom only because notice was the means by which Netcom acquired knowledge of infringement. It was undisputed that prior to notice Netcom did not have the requisite knowledge for contributory infringement. … [T]he issue in the present actions is not how Napster came by knowledge of infringement, but whether such knowledge exists." Id. at *35-36. The district court found the Ninth Circuit's reading of Netcom in Napster I to be in accord. "The Ninth Circuit noted that the situation in Netcom, where a computer service provider has actual knowledge of specific infringing files, is *sufficient* to give rise to liability. The court never stated that actual knowledge (or notice for that matter) was *necessary* for liability." Id. at *36-37 (emphasis in original).

[1521] Id. at *39.

17. The Second, Consolidated Appeal to the Ninth Circuit. In the second appeal to the Ninth Circuit, Napster argued that the notification requirements imposed on the plaintiffs by the Mar. 5 modified injunction were mandated by the Ninth Circuit's opinion in Napster I, and that even if they were not, their imposition was not an abuse of discretion by the district court. However, Napster argued that the policing obligations of the Mar. 5 modified injunction were too indeterminate to meet the requirements of Rule 65 of the Federal Rules of Civil Procedure, because the Mar. 5 order did not specify the extent, and at what cost, Napster was required to discharge its policing obligations. Unless clarified, Napster argued that the policing obligations would potentially authorize massive blocking of noninfringing works. Napster also argued that the Mar. 5 order impermissibly delegated judicial functions to Dr. Nichols.[1522]

With respect to the July 11 oral order, Napster argued that the district court lacked jurisdiction to issue the order because it constituted a modification of the Mar. 5 order, which was on appeal. Napster noted that the Ninth Circuit, in its stay order, had itself characterized the July 11 order as "modifying" the Mar. 5 order.[1523] Napster also argued that, in any event, the July 11 order's "zero tolerance" standard was fundamentally at odds with the Ninth Circuit ruling in Napster I.[1524] The plaintiffs, in turn, challenged the requirements of the preliminary injunctions that they provide to Napster file names found on the Napster index that corresponded to their copyrighted works before Napster had a duty to act on those files.

On appeal, the Ninth Circuit rejected most of the arguments of both Napster and the plaintiffs in a very sparse opinion that will be referred to as "Napster II."[1525] With respect to the plaintiffs' argument that it should not have to supply file names to Napster and that Napster should instead be required to search for and block all files containing any protected copyrighted works, not just works with which plaintiffs had been able to provide a corresponding file name, the Ninth Circuit ruled that the notice requirements of the preliminary injunctions complied with its holding in Napster I that the plaintiffs bore the burden to provide notice to Napster of copyrighted works and files containing such works before Napster had a duty to disable access to the offending content.[1526] The court further held that "Napster's duty to search under the modified preliminary injunction is consistent with our holding that Napster must 'affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed on its search index.' The modified preliminary injunction correctly reflects the legal principles of contributory and vicarious copyright infringement that we previously articulated."[1527] Thus, the Ninth Circuit's Napster II opinion appears to establish a legal rule under which there is a notice requirement both for the imposition of common law contributory liability and vicarious liability

---

[1522] "Napster Asks 9th Circuit to Modify 1 Order, Vacate Another," *Mealey's Cyber Tech & E-Commerce Litigation Reporter* (Aug. 2001) 5-6.

[1523] Id. at 6.

[1524] Id.

[1525] A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

[1526] Id. at 1096.

[1527] Id. at 1096-97 (quoting Napster I, 239 F.3d at 1027).

on an OSP, contrary to the district court's conclusion otherwise in its opinion on Napster's motion to dismiss, discussed in subsection 17 above.[1528]

The Ninth Circuit rejected Napster's challenge to the preliminary injunction as impermissibly vague. The court's very terse response was as follows: "Napster has a duty to police its system in order to avoid vicarious infringement. Napster can police the system by searching its index for files containing a noticed copyrighted work. The modified preliminary injunction directs Napster, in no vague terms, to do exactly that."[1529] The court also rejected Napster's argument that the district court had improperly delegated its judicial authority to Dr. Nichols: "At no time did the technical advisor displace the district court's judicial role. The technical advisor never unilaterally issued findings of fact or conclusions of law regarding Napster's compliance."[1530]

Next, the court turned to Napster's challenge that the shut down order improperly amended the modified preliminary injunction by requiring a non-text-based filtering mechanism and a "zero tolerance" standard for compliance. The Ninth Circuit rejected each of these challenges. The court apparently found that the requirement of a non-text-based filtering mechanism did not violate the court's ruling in Napster I that Napster's duty to policy was "cabined by the system's current architecture,"[1531] because the new filtering mechanism "still requires Napster to search files located on the index to locate infringing material."[1532] Thus, the court appears to have viewed the "architecture" of the Napster system as *index* based, rather than *text* based.[1533] Moreover, the Ninth Circuit noted that a district court has inherent authority to modify a preliminary injunction in consideration of new facts. "The text-based filter proved to be vulnerable to user-defined variations in file names. The new filtering mechanism, on the other hand, does not depend on file names and thus is not similarly susceptible to bypass. It was a proper exercise of the district court's supervisory authority to require use of the new filtering mechanism, which may counter Napster's inability to fully comply with the modified preliminary injunction."[1534] This is a substantial ruling, as it appears to allow a district court to

---

[1528] This rule would not, however, appear to survive the Supreme Court's decision in Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2770 (2005), discussed in Section III.C.4(a) below.

[1529] Napster II, 284 F.3d at 1097.

[1530] Id.

[1531] Napster I, 239 F.3d at 1024.

[1532] Napster II, 284 F.3d at 1098.

[1533] It appears that the Ninth Circuit did not fully understand the non-text-based filtering mechanism that the district court required Napster to use. As discussed in subsection 15, that alternative filtering technology known as "fileID," unlike the old technology, was not based primarily on textual filenames, but rather on a technical analysis of the digital musical content contained in a file, including acoustic waveform recognition, to generate a "fingerprint." Napster *combined* the fileID technology with its textual filename search technology using the index, but the fileID technology required a fundamentally different approach to identifying potentially infringing works. However, the fact that Napster continued to maintain an index appears to have led the Ninth Circuit to conclude rather facilely that requiring the use of fileID technology did not constitute a departure from the original Napster system "architecture," when in fact it required a radically different approach.

[1534] Id. at 1098.

require an OSP to adopt new technologies that may become available in order to keep infringing materials off its system.

With respect to the "zero tolerance" challenge, the Ninth Circuit ruled that the district court's imposition of a "zero tolerance" standard was permissible because that standard did not apply to all potentially infringing works on Napster's system, but only to those works that had been noticed by the plaintiff:

> The district court did not, as Napster argues, premise the shut down order on a requirement that Napster must prevent infringement of all of plaintiffs' copyrighted works, without regard to plaintiffs' duty to provide notice. The tolerance standard announced applies only to copyrighted works which plaintiffs have properly noticed as required by the modified preliminary injunction. That is, Napster must do everything feasible to block files from its system which contain noticed copyrighted works. … The district court determined that more could be done to maximize the effectiveness of the new filtering mechanism. Ordering Napster to keep its file transferring service disabled in these circumstances was not an abuse of discretion.[1535]

Even with this clarification of the "zero tolerance" standard, the Ninth Circuit's allowance of that standard may pose a formidable challenge for many OSPs seeking to avoid liability for copyright infringement. It seems unlikely that any technology for identifying and blocking infringing works on a system will be completely foolproof. And how far must an OSP go to do "everything feasible" to block noticed copyrighted works – must it constantly upgrade its technology to the most leading, perhaps unproven, technology? Where is the line on what is "feasible"?

Finally, the Ninth Circuit rejected Napster's challenge that the district court lacked authority to modify the preliminary injunction pending appeal. The court noted that, although a district court cannot, while a preliminary injunction is on appeal, modify the injunction in such manner as to finally adjudicate substantial rights directly involved in the appeal, it can, under Federal Rule of Civil Procedure 62(c), continue supervision of compliance with the injunction. The Ninth Circuit ruled that the district court had properly exercised its power under this Rule.[1536] Accordingly, the court affirmed both the modified preliminary injunction and the shut down order, noting that the "shut down order was a proper exercise of the district court's power to enforce compliance with the modified preliminary injunction."[1537]

18. Motions for Summary Judgment and for Discovery on Misuse Theory and Ownership Questions. While the second consolidated appeal was pending, the plaintiffs filed motions in the district court for summary judgment of willful contributory and vicarious copyright infringement. Napster requested, pursuant to Rule 56(f) of the Federal Rules of Civil

---

[1535] Id.

[1536] Id. at 1099.

[1537] Id.

Procedure, that the court stay any decision on the merits to allow for additional discovery on the questions of (i) whether the plaintiffs actually owned the rights to the musical works for which they alleged infringement and (ii) whether the plaintiffs had misused their copyrights by attempting to control the market for the digital distribution of music.[1538]

With respect to the ownership issues, the plaintiffs rested on the legal rule that a copyright certificate establishes prima facie evidence of the validity of a copyright and the facts in the certificate.[1539] Napster challenged the presumption of ownership set up by the certificates, arguing that in 133 of the 144 copyright certificates submitted with the complaint, the registered works were incorrectly designated as "works for hire." The plaintiffs, in turn, challenged Napster's standing to challenge the presumption of ownership. The court noted a line of cases holding that a third party does not have standing to challenge the presumption of ownership when a plaintiff claims ownership by assignment, but ruled that the third-party standing doctrine does not apply in instances of ownership by authorship. Accordingly, Napster had standing to challenge whether the works in suit were works for hire.[1540]

The court held that there were substantial questions raised by Napster on which it was entitled to take discovery with respect to whether the plaintiffs could satisfy either of the two prongs of the definition of "work made for hire."[1541] With respect to the "specially commissioned" prong of the definition, the court noted that sound recordings are not one of the nine types of specially commissioned works listed in the definition that can qualify as works made for hire. With respect to the "employment" prong of the definition, the court noted that the plaintiffs had produced no contracts with artists to demonstrate an employment relationship.[1542] The court ordered the plaintiffs to produce all documentation relevant to their ownership of the works listed as works for hire to a Special Master appointed by the court to review them. The court specifically withheld any rulings on the work for hire issue, the scope of the plaintiffs'

[1538] In re Napster Inc. Copyright Litigation, 191 F. Supp. 2d 1087, 1093 (N.D. Cal. 2002). Napster also alleged that there were disputed issues of fact with respect to "plaintiffs' ownership of the copyrighted works at issue, copying of the works, fair use, the application of *Sony*, the extent of Napster's control over its system and its policing obligation, the extent of the Napster system's architecture, the sufficiency of plaintiffs' notices and Napster's removal of those works, application of the Digital Millennium Copyright Act, copyright misuse, and willfulness." Id. at 1095 n.1.

[1539] 17 U.S.C. § 410(c).

[1540] In re Napster Copyright Litigation, 191 F. Supp. 2d at 1097-98.

[1541] 17 U.S.C. § 101 defines a "work made for hire" as "(1) a work prepared by an employee within the scope of his or her employment; or (2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. For the purpose of the foregoing sentence, a 'supplementary work' is a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer material for tests, bibliographies, appendixes, and indexes, and an 'instructional text' is a literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities."

[1542] In re Napster Copyright Litigation, 191 F. Supp. 2d. at 1098.

rights, and the extent to which the plaintiffs were protected by the presumption of ownership until further discovery was completed.[1543]

The court then turned to Napster's need for discovery on its allegations of copyright misuse by the plaintiffs. The court first noted that, although both itself and the Ninth Circuit had dismissed Napster's misuse defense at the preliminary injunction stage, "[s]ince those rulings, the factual and procedural landscape has changed significantly. … The evidence now shows that plaintiffs have licensed their catalogs of works for digital distribution in what could be an overreaching manner. The evidence also suggests that plaintiffs' entry into the digital distribution market may run afoul of the antitrust laws."[1544]

Napster based its allegations of misuse on unduly restrictive licensing requirements of the plaintiffs' online music venture, MusicNet, with which Napster had entered into a license agreement. That agreement prevented Napster from entering into any licensing agreement with any individual plaintiffs until March 1, 2002 and provided that even after March 2002, if Napster entered into any individual license with any of the plaintiffs, MusicNet could terminate the agreement upon 90 days notice. Additionally, the license set up a pricing structure under which Napster would be charged higher fees if it failed to use MusicNet as its exclusive licensor for content.[1545] The court held that these provisions effectively granted MusicNet control over which content Napster licensed. "The result is an expansion of the powers of the three MusicNet plaintiffs' copyrights to cover the catalogs of the two non-MusicNet plaintiffs."[1546] The court noted that further inquiry into the actions of MusicNet, and whether those actions should be imputed to the plaintiffs, was warranted.[1547]

The court also found that Napster had raised substantial issues of whether the plaintiffs' entry into the digital distribution market constituted antitrust violations. "[E]ven a naïf must

---

[1543] Id. at 1100. The court further ruled that, with respect to works listing an author other than the plaintiffs on the registration certificate and works protected under state law, the plaintiffs would be obliged to produce a chain of title from the listed author to themselves. Id. at 1101. Works with pending registrations would be given the benefit of the presumption of ownership. Id. Finally, for those works for which the plaintiffs had not yet filed an application for registration, the court ruled that it lacked subject matter jurisdiction. Id.

[1544] Id. at 1102 (citations omitted).

[1545] Id. at 1105-06.

[1546] Id. at 1106.

[1547] Id. at 1107. The court further noted that, if the plaintiffs were engaged in misuse, they could not bring suit based on their rights until the misuse ended, although the misuse would not ultimately preclude recovery for infringement: "The doctrine [of misuse] does not prevent plaintiffs from ultimately recovering for acts of infringement that occur during the period of misuse. The issue focuses on when plaintiffs can bring or pursue an action for infringement, not for which acts of infringement they can recover." Id. at 1108.

The court also rejected the plaintiffs' argument that Napster should not be allowed to assert a misuse defense because of its own unclean hands. Because the plaintiffs had themselves sought equitable relief from the court, Napster should not be barred from bringing an equitable defense. Id. at 1110-11. In any event, upon a balancing of equities, the court concluded that "the potential for public injury and the fact that Napster has shut its doors to infringement justifies allowing Napster to assert a misuse defense to obtain additional discovery." Id. at 1113.

realize that in forming and operating a joint venture, plaintiffs' representatives must necessarily meet and discuss pricing and licensing, raising the specter of possible antitrust violations. These joint ventures bear the indicia of entities designed to allow plaintiffs to use their copyrights and extensive market power to dominate the market for digital music distribution. Even on the undeveloped record before the court, these joint ventures look bad, sound bad and smell bad."[1548] Accordingly, the court granted Napster's Rule 56(f) motion for further discovery into the antitrust and misuse issues raised by Napster.[1549] Such discovery was subsequently stayed as the result of filing of bankruptcy by Napster in June of 2002. On August 9, 2002, Napster's assets were placed up for auction in the bankruptcy proceeding.[1550]

(2) The Scour.com Lawsuit

Another case challenged the legality of peer-to-peer file sharing through a service similar to the Napster service. On July 20, 2000, several leading motion picture studios, record companies, and music publishers filed a copyright infringement action in federal district court in New York against Scour, Inc., operator of an online file sharing service known as the Scour Exchange. Unlike the Napster service, which was limited to the exchange of music files in MP3 format, the Scour Exchange enabled the peer-to-peer exchange of both music and motion picture files among the hard drives of Scour users. The Scour website featured a banner containing a "Top Five" search list, identifying current hit motion picture titles and music recordings that had been requested most frequently by Scour users.[1551]

Like the Napster service, Scour's website provided users with free copies of its proprietary file sharing software, which users could use to connect to Scour's servers and choose which content files stored on their computer hard drives they wished to make available for other Scour users to download. Scour then inventoried the files each user had so designated and combined them in a database and directory that was made available on Scour's servers to all Scour users currently logged on. Users could search the directory and initiate downloads of desired material from other users' computers.[1552] Unlike Napster, however, Scour also made available through a partnership with a third party a service that provided secure storage space for files on a remote server. The service provided what Scour promoted as "free, secure, online storage space for all the multimedia files that you find on Scour." Through this service, Scour users were able to upload their files onto this remote server for other Scour users to download, regardless of whether the originating user was logged on to Scour's servers.[1553] The plaintiffs

---

[1548] Id. at 1109 (citations omitted).

[1549] Id. at 1113.

[1550] Scarlett Pruitt, "Napster Assets Go Up for Auction" (Aug. 12, 2002), available as of Aug. 12, 2002 at www.infoworld.com/articles/hn/xml/02/08/12/020812hnnapster.xml.

[1551] Complaint, Twentieth Century Fox Film Corp. v. Scour, Inc., No. 00 Civ. 5385 (GBD) (S.D.N.Y., filed July 20, 2000) ¶¶ 1-2, available as of Dec. 16, 2000 at www.mpaa.org/press/scourcomplaint.htm.

[1552] Id. ¶ 58.

[1553] Id. ¶ 60.

alleged that Scour was contributorily and vicariously liable for the infringing downloads of copyrighted material by Scour's users.[1554]

The defense of the lawsuit proved too costly for Scour, and on October 13, 2000, Scour filed for Chapter 11 bankruptcy protection.[1555] On Nov. 14, 2000, Scour announced that it would shut down its exchange service in order facilitate a resolution of the copyright infringement litigation and the sale of its assets, which Listen.com had offered to purchase for $5 million in cash and more than 500,000 shares of stock.[1556]

(3) The Aimster/Madster Lawsuits

On April 30, 2001 a company called Aimster, which was operating a file swapping service very similar to the Scour service, filed suit in federal court in Albany, New York against various members of the RIAA for a declaratory judgment that it was not secondarily liable for copyright infringement by users of its service to swap allegedly infringing material. The Aimster service was based on a peer-to-peer technology, but was different from Napster and Scour in that files were traded in an encrypted format which Aimster claimed prevented it from having knowledge of when its users were exchanging files, the identity of persons exchanging files, or what files were being exchanged through its service.[1557]

The Aimster service was based on instant messaging (IM) technology from AOL. Specifically, Aimster made use of AOL IM's "get file" functionality, which gave AOL IM users the ability to designate certain files or directories on the user's hard drive that would be made available for other IM users to copy. The native "get file" functionality in AOL was limited in two ways. First, a user could retrieve files only from a list of his or her known "buddies" who were logged on at the same time. Second, there was no capability to search the files that were available from a buddy; the user was required to know the particular file that was being sought on the buddy's hard drive before that file could be fetched.[1558]

The Aimster service considerably expanded upon the basic file transferring capability of the AOL IM system by designating every Aimster user as the buddy of every other Aimster user, thereby allowing all Aimster users to communicate and share files with any other Aimster user currently online. The Aimster service also afforded its users the capability to search all the files contained on the hard drives of other users that had been designated for sharing.[1559] Once the

---

[1554] Id. ¶ 71.

[1555] Jim Hu, "Scour Files for Bankruptcy Protection" (Oct. 13, 2000), available as of Dec. 16, 2000 at http://news.cnet.com/news/0-1005-200-3178822.html.

[1556] Steven Musil, "Scour to End File-Swapping Service" (Nov. 14, 2000), available as of Dec. 16, 2000 at http://news.cnet.com/news/0-1005-200-3689821.html.

[1557] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 641 (N.D. Ill. 2002).

[1558] Id. at 640.

[1559] Id. at 642. The parties hotly disputed whether Aimster catalogued all available files for download in a single, centralized database, akin to the Napster system. In issuing its preliminary injunction, the court noted that its

search for a suitable file was complete, an Aimster user needed only to click on the file name title and then click on a "Download" button to obtain a copy of the song. The Aimster system then facilitated the connection of its two users though a private, encrypted network so the file could be transferred. During the copying of a file, the Aimster system provided a constant update about the status of each download or upload.[1560]

The Aimster service contained several additional features that ultimately proved relevant to the analysis of copyright infringement. First, located for a time on Aimster's web site was a utility called "Aimster's Guardian Tutorial," which demonstrated how to transfer and copy copyrighted works over the Aimster system using as illustrative on-screen examples some of the copyrighted works of RIAA members. Second, Aimster's service offered message boards on which Aimster users wishing to download particular copyrighted recordings could seek the assistance of others. In addition, users often posted messages on these boards openly discussing trafficking in copyrighted material and "screwing" the RIAA.[1561] Finally, in November 2001, Aimster launched a service called "Club Aimster," which required a $4.95 monthly service fee, for which users were given access to a list of "The Aimster Top-40," a list of the 40 "hot new releases" most frequently downloaded by Aimster users, virtually all of which were owned by RIAA members. Each Aimster Top 40 selection included a Play button that a user could click to automatically begin the copying and transfer of that particular song to the user's computer without the inconvenience of having to type in an Aimster search request. At one point, Aimster changed it procedures to require all prospective users to join Club Aimster in order to be able to download the Aimster client software.[1562]

On May 24, 2001, various members of the RIAA responded to Aimster's declaratory judgment lawsuit by filing copyright infringement lawsuits against BuddyUSA and AbovePeer, corporate entities that owned the Aimster software and file swapping service, and Johnny Deep, CEO of Aimster, in federal court in Manhattan.[1563] On May 29, 2001, these lawsuits were stayed by the court in Albany,[1564] although the stay was lifted on June 22.[1565] On June 27, seven major motion picture studios also filed suit against Deep, BuddyUSA and AbovePeer alleging copyright infringement based on the ability of the Aimster service to share copyrighted motion pictures.[1566] In July 2001 various music publishers and songwriters joined the fray with their

---

legal analysis of the copyright issues would hold regardless of whether or not Aimster maintained a central database of files available for transfer. Id. at 641 n.6.

[1560] Id. at 642-43

[1561] Id. at 643-44, 650.

[1562] Id. at 644-45.

[1563] Id. at 646.

[1564] Steven Bonisteel, "Aimster in Court Today to Fend Off Music-Industry Suits" (May 30, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/166250.html.

[1565] Michael Bartlett, "Movie Studios Attack File-Swapping Service Aimster" (July 3, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/167549.html.

[1566] Id.

own copyright infringement lawsuit filed in Manhattan.[1567] On Nov. 19, 2001, a multi-jurisdictional panel of judges in San Diego ruled that the bevy of lawsuits against Aimster should be tried in federal district court in Chicago as a convenient, central forum among all the various parties.[1568]

On Mar. 19, 2002, the lawsuits against the Aimster service, which was subsequently renamed "Madster" after a trademark dispute with AOL, were placed on hold after BuddyUSA and AbovePeer filed for bankruptcy. On June 20, 2002, the bankruptcy judge lifted the automatic stay of the lawsuits to the extent necessary to allow the record companies to pursue a preliminary injunction against the service in the federal district court in Chicago.[1569] About three months later, the district court ruled that the plaintiffs were entitled to a preliminary injunction on grounds of contributory and vicarious liability.[1570] Aimster appealed.

The Seventh Circuit, per Judge Posner, affirmed the issuance of the preliminary injunction, finding that Aimster was likely liable as a contributory infringer.[1571] The bulk of the court's opinion was devoted to an analysis of the scope of the Supreme Court's "substantial noninfringing use" doctrine in the Sony case, on which Aimster relied heavily for its defense. Judge Posner seems to have significantly reinterpreted that doctrine using a classic "Chicago school" law and economics analysis. (The viability of Judge Posner's interpretive approach to Sony's "substantial noninfringing use" doctrine, whether or not it led to the correct substantive outcome, is at best dubious after the Supreme Court's Grokster decision discussed in Section III.C.2(c)(5) below.[1572])

[1567] "Aimster: Another Day, Another Lawsuit" (July 5, 2001), available as of Jan. 6, 2002 at www.usatoday.com/life/cyber/tech/2001-07-05-aimster.htm.

[1568] Kevin Featherly, "Judges Consolidate Aimster Suits – Correction" (Nov. 19, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/172294.html.

[1569] "Judge: Record Companies Can Pursue Injunction Against Madster" (June 21, 2002), available as of June 21, 2002 at www.siliconvalley.com/mld/siliconvalley/news/editorial/3511564.htm.

[1570] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 665 (N.D. Ill. 2002). The district court also rejected Aimster's argument of a defense under the AHRA. The court first ruled that Aimster's users were plainly engaged in direct copyright infringement and that the AHRA did not provide an affirmative defense to the users' acts of direct copying. Invoking the Ninth Circuit's Diamond Multimedia decision, discussed extensively in Section III.C.2(c)(1).2 above, Aimster argued that the AHRA immunized all noncommercial copying by consumers of digital and analog musical recordings. The district court rejected this argument, distinguishing Diamond Multimedia on the grounds that in that case users were merely space shifting files from their hard drives to a portable digital device for their own personal use. By contrast, the Aimster service involved the copying of MP3 files from one user's hard drive onto the hard drive of another user, and such massive, unauthorized distribution and copying of the plaintiffs' works was not within the scope of the AHRA. Id. at 648-49.

[1571] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[1572] See Mitchell Zimmerman, "Grokster Seems Unlikely to Prevent File Sharing by Itself," *The Daily Journal* (Aug 15, 2005); earlier version available online in Fenwick & West's *IP Bulletin* (Fall 2005), p. 3, at http://www.fenwick.com/docstore/Publications/IP/IP_bulletins/IP_Bulletin_Fall_2005.pdf#xml=http://www.fenwick.com/publications/indices.asp?cmd=pdfhits&DocId=115&Index=C%3a%5cdtindex%5cwebsite%5cIP&HitCount=4&hits=632+10de+1109+11a3+&hc=143&req=Zimmerman.

He began the analysis by noting that Sony's Betamax video recorder was used for three principal purposes – time shifting (recording a television program for later viewing), library building (making copies of programs to retain permanently), and commercial skipping (taping a program before watching it and then, while watching the tape, using the fast-forward button on the recorder to skip over the commercials).[1573] He noted that the Supreme Court held the first use to be a fair use because it enlarged the audience for the program, but went on to note, in dicta, that the second and third uses were "unquestionably infringing" – the second because "it was the equivalent of borrowing a copyrighted book from a public library, making a copy of it for one's personal library, then returning the original to the public library," and the third because it "amounted to creating an unauthorized derivative work … namely a commercial-free copy that would reduce the copyright owner's income from his original program, since 'free' television programs are financed by the purchase of commercials by advertisers."[1574] Thus, according to Judge Posner, the Supreme Court in Sony was confronted with a situation in which the video recorder "was being used for a mixture of infringing and noninfringing uses and the Court thought that Sony could not demix them because once Sony sold the recorder it lost all control over its use."[1575]

Having characterized the Sony case thusly, Judge Posner turned to an application of its principles to the Aimster service. He first rejected some extreme interpretations of those principles put forward by the parties. Specifically, he rejected the RIAA's argument that Sony is inapplicable to services and that, where services are concerned, "the test is merely whether the provider knows it's being used to infringe copyright."[1576] He noted that although knowledge that a service is being used for infringing purposes is a factor to be considered in contributory infringement, it cannot be dispositive, else services like AOL's instant messaging service would be illegal just because some use it for infringing purposes.[1577] Moreover, he noted that in the Sony case, the Supreme Court acknowledged that 25% of Betamax users were fast forwarding through commercials, which, as noted, Judge Posner believed to constitute an infringing use, yet nevertheless there was no contributory infringement.[1578] Judge Posner thus concluded, "We therefore agree with Professor Goldstein that the Ninth Circuit erred in *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 (9th Cir. 2001), in suggesting that actual knowledge of

---

[1573] Id. at 647.

[1574] Id. at 647-48. The ruling that recording for commercial skipping constitutes the making of an unauthorized derivative work is curious. First, it seems novel to judge the legality of a reproduced work on the *subsequent potential use* that a user may put the work to. Second, the work that was actually fixed in the tangible medium by the video recorder was the entire television program, including the commercials without modification. It is only upon playback that the commercials were skipped by fast forwarding through them, and one would have to argue that the transient display produced on the television screen as the commercials run by at faster speed is itself a derivative work. And even if a derivative work, it is unclear why such work might not be a fair use, at least when done by a private viewer to enhance enjoyment of the program.

[1575] Id. at 648.

[1576] Id.

[1577] Id.

[1578] Id. at 649.

specific infringing uses is a sufficient condition for deeming a facilitator a contributor infringer."[1579]

Conversely, Judge Posner rejected Aimster's argument that any showing that its service *could* be used in noninfringing ways is sufficient to avoid contributory liability. "Were that the law, the seller of a product or service used *solely* to facilitate copyright infringement, though it was capable in principle of noninfringing uses, would be immune from liability for contributory infringement."[1580] In addition, the Supreme Court would not have thought it important to state that the Betamax was used "principally" for time shifting.[1581]

Judge Posner therefore interpreted the Sony doctrine ultimately to require an economic cost/benefit analysis of the infringing and noninfringing uses of a system in determining contributory liability. "What is true is that when a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement. … But the balancing of costs and benefits is necessary only in a case in which substantial noninfringing uses, present or prospective, are demonstrated."[1582]

In the instant case, the court concluded the evidence showed that the Aimster system was principally for use for infringement. The court pointed to the fact that in explaining how to use the Aimster software, the tutorial gave as its only examples of file sharing the sharing of copyrighted music. In addition, membership in Club Aimster enabled the member for a fee of $4.95 a month to download with a single click the 40 songs most often shared by Aimster users, and those were invariably copyrighted by the plaintiffs.[1583] "The evidence that we have summarized does not exclude the *possibility* of substantial noninfringing uses of the Aimster system, but the evidence is sufficient, especially in a preliminary-injunction proceeding, which is summary in character, to shift the burden of production to Aimster to demonstrate that its service has substantial noninfringing uses."[1584]

The court held that Aimster had failed to show that its service had ever been used for a noninfringing use, let alone evidence concerning the frequency of such uses.[1585] "Even when there are noninfringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses."[1586] Not only had Aimster failed to engage in this calculation,

---

[1579] Id. (citing 2 Paul Goldstein, *Copyright* § 6.1.2, p. 6:12-1 (2d ed. 2003)).

[1580] 334 F.3d at 651.

[1581] Id. (emphasis in original).

[1582] Id. at 649-50.

[1583] Id. at 651-52.

[1584] Id. at 652 (emphasis in original).

[1585] Id. at 653.

[1586] Id.

the court ruled that it had willfully blinded itself from evidence of how its service was being used by providing encryption for all transactions on the service.[1587] "This is not to say that the provider of an encrypted instant-messaging service or encryption software is ipso facto[] a contributory infringer should his buyers use the service to infringe copyright …. Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used."[1588]

The court therefore concluded that it was likely Aimster would be found a contributory infringer and affirmed the granting of the preliminary injunction.[1589]

The court also rejected a challenge to the injunction's breadth. The preliminary injunction, which was very broad in sweep, required Aimster to "immediately disable and prevent any and all access" to the plaintiffs' copyrighted works on or through any web site, server, or system owned or controlled by Aimster, "including, if necessary, preventing any and all access to the Aimster System and Service in its entirety, until such time that Aimster implements measures that prevent" unauthorized copying and downloading of the plaintiffs' copyrighted works.[1590] After implementing "measures to ensure that the Aimster System and Service prevents any and all copying, downloading, distributing, uploading, linking to, or transmitting" of the plaintiffs' copyrighted works, Aimster was permitted to provide public access to its system, except that it continued to be enjoined from copying, downloading or distributing the plaintiffs' copyrighted works or facilitating the same.[1591]

Aimster was also required to "affirmatively monitor and patrol for, and preclude access to" the plaintiffs' copyrighted works "by employing such technological tools and measures that are reasonably available to carry out such obligations" without specifying what those might be or what technical effectiveness criteria they would have to satisfy.[1592] Finally, in one of the most onerous parts of the order, Aimster was required to "maintain a complete list of any and all sound recordings and musical compositions made available on, over, through, or via its system, and upon five (5) business days' notice [to] make such lists available to Plaintiffs for inspection and copying. Such lists shall include, without limitation, computer, website, and computer server logs delineating User search requests, download requests and upload attempts for any and

---

[1587] Id.

[1588] Id. at 650-51.

[1589] Id. at 656. For a case post-dating the Supreme Court's Grokster decision that interprets and applies Judge Posner's tests for contributory infringement in a non-service provider context, see Monotype Imaging, Inc. v. Bitstream Inc., 2005 U.S. Dist. LEXIS 7410 (N.D. Ill. Apr. 21, 2005) (opinion on motion for summary judgment) and 2005 U.S. Dist. LEXIS 14278 (N.D. Ill. (July 12, 2005) (opinion after bench trial). The court in Monotype applied the Aimster approach to contributory liability without considering at all the issue of whether any of the rationale or holdings of the Aimster cases were called into question by the Supreme Court's Grokster decision.

[1590] Preliminary Injunction Order, In re Aimster Copyright Litigation, No. 01 c 8933 (N.D. Ill. Oct. 30, 2002) at ¶ 2.

[1591] Id. ¶ 3.

[1592] Id. ¶4.

all sound records and musical compositions."[1593] The Seventh Circuit rejected Aimster's challenge to the breadth of the injunction on the ground that Aimster had failed to suggest alternative language either to the district court or to the Seventh Circuit, and had therefore waived the objection.[1594]

(4) The StreamCast/Kazaa/Grokster Lawsuits

One of the most significant peer-to-peer lawsuits to be filed after the Napster case involved the file sharing services originally known as Music City (later renamed to StreamCast), Kazaa, and Grokster. On Oct. 2, 2001, various recording companies and movie studios sued the operators of these services for copyright infringement in the Central District of California. Shortly thereafter, on Nov. 19, 2001, Jerry Leiber and Mike Stoller filed a class action for copyright infringement on behalf of themselves and all music publishers represented by The Harry Fox Agency against the same defendants, again in the Central District of California. The two lawsuits were eventually consolidated.

These suits presented a potential extension of the legal theories on which the Napster case relied in view of technical differences in the peer-to-peer architecture used by the StreamCast, Kazaa, and Grokster services, as opposed to the Napster service. As discussed in Section III.C.2(c)(1) above, the Napster service relied on a central index of files available for sharing stored on servers maintained and controlled by Napster. This index enabled Napster to block allegedly infringing files by searching the filenames available through the index. By contrast, the StreamCast, Kazaa, and Grokster services did not operate based on such a central index. Rather, the indexes of files available for sharing were distributed across users' computers.

Specifically, according to the complaint filed in the class action case, each of the StreamCast, Kazaa, and Grokster services initially relied on software called FastTrack, originally developed by a group of Scandinavian programmers known as Consumer Empowerment BV, later renamed Kazaa BV.[1595]Kazaa BV launched the first of the three services (the Kazaa service) on July 28, 2000 by publicly releasing its FastTrack software on its web site.[1596] The FastTrack software interacted with Kazaa BV's server side software to enable Kazaa users to connect their computers to one or more central computer servers controlled and maintained by Kazaa BV.[1597] After the central server registered, identified, and logged in the user, the Kazaa service connected the user to a "SuperNode." A SuperNode is a computer with a high-bandwidth connection that is operated by another user already connected to the service. After a user connected to a SuperNode, these "local search hubs" compiled an index of digital files being offered by the user for downloading by other service users. The FastTrack software also enabled users to search for and import preexisting libraries of music files (such as libraries that users built

---

[1593] Id. ¶ 6.

[1594] In re Aimster Copyright Litigation, 334 F.3d 643, 656 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[1595] Class Action Complaint for Copyright Infringement, Leiber v. Consumer Empowerment, Civ. No. 01-09923 (C.D. Cal. Nov. 19, 2001) ¶¶ 25-26.

[1596] Id. ¶ 27.

[1597] Id. ¶ 31.

using Napster) to make them available through the service. In response to a search request, the SuperNode reviewed its own index of files and, if necessary, the indices maintained by other SuperNodes. It then displayed the search results to the user to permit the user to download any files displayed by the search.[1598] Hence the index of files available at any point in time were distributed throughout various SuperNode computers maintained by the users of the network, not Kazaa BV.

Any Kazaa service user could become a SuperNode by choosing that option in the FastTrack software, and users were encouraged to do so. Kazaa BV's central servers maintained communications with all SuperNodes and assisted in administering the Kazaa service.[1599] The role of Kazaa BV's central servers in the operation of the service was a key basis upon which the plaintiffs asserted contributory and vicarious copyright liability. The Kazaa service continuously monitored its thousands of users to keep track of when they logged on and off. As soon as a user logged on, that user's music files were inventoried and added to the distributed database, and when the user logged off, that user's files were eliminated from the database.[1600] Communications on the service between its users' computers and its central servers, between the user and a SuperNode, between SuperNodes and the central servers, and between and among SuperNodes were all encrypted using a scheme controlled by Kazaa BV.[1601] According to the complaint, Kazaa BV created the connection between the user who had selected a music file for copying and the user who was offering the selected file. "Thus, all users need to do is select the file they want and it automatically downloads – *i.e.*, copies and saves – to their individual computer hard drive. [Kazaa BV] makes the entire transaction possible."[1602]

The StreamCast and Grokster services operated in a very similar fashion. Initially, both StreamCast and Grokster used the FastTrack software. After the lawsuits were filed, StreamCast switched to use of the open standard Gnutella technology and developed its own software known as "Morpheus" based on that technology. Also after initiation of the lawsuits, the operation of the Kazaa system passed from Kazaa BV to Sharman Networks.[1603] A news article reported on May 23, 2002 that Kazaa BV was no longer able to afford defending the lawsuit and that it would accept a default judgment, and that the attorney for StreamCast Networks was withdrawing from the case because StreamCast also could not afford the cost of the litigation.[1604]

[1598] Id. ¶ 32.

[1599] Id. ¶ 33.

[1600] Id. ¶ 34.

[1601] Id. ¶ 38.

[1602] Id. ¶ 37. An internal RIAA memorandum, which both outlines the RIAA's legal theories against the Kazaa service and gives further technical detail on how it functions, may be found at www.dotcomscoop.com/article.php?sid=39 (available as of Jan. 6, 2002).

[1603] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1032 & n. 2 (C.D. Cal. 2003).

[1604] John Borland, "Kazaa, Morpheus Legal Case Collapsing" (May 22, 2002), available as of May 23, 2002 at http://news.com.com/2102-1023-920557.html. The article further reported that "squabbling between Streamcast and Kazaa BV has badly weakened the defendants' case."

In July of 2002, the federal district court ruled that the plaintiffs could expand their U.S. lawsuit to include Sharman Networks, which had assumed distribution of the Kazaa file-swapping software.[1605] In January of 2003, the court rejected a jurisdictional challenge brought by Sharman Networks, ruling that Sharman Networks could be sued in California since the Kazaa software had been downloaded and used by millions of Californians.[1606] Approximately one week later, Sharman Networks filed antitrust and copyright misuse counterclaims against the plaintiffs.[1607]

The plaintiffs and defendants StreamCast and Grokster filed cross motions for summary judgment with regard to contributory and vicarious copyright infringement. On April 25, 2003, the court granted summary judgment in favor of StreamCast and Grokster on both theories. The court noted that its order applied only to the then current versions of Grokster's and StreamCast's products and services, and did not reach the question of whether either defendant was liable for damages from prior versions of their software or from other past activities.[1608]

With respect to the issue of contributory liability, the court first noted that it was undisputed that at least some of the individuals using the defendants' software were engaged in direct copyright infringement.[1609] The court then turned to an analysis of the two prongs of contributory liability for such direct infringements, knowledge of the infringing activity and material contribution thereto.

In one of the most significant aspects of the ruling, the court held that mere constructive knowledge is not sufficient for contributory liability, but rather the defendant must have actual knowledge of specific infringing acts at the time the infringement occurs. Citing the Ninth Circuit's decision in the Napster case, the court ruled that "defendants are liable for contributory infringement only if they (1) have specific knowledge of infringement at a time at which they contribute to the infringement, and (2) fail to act upon that information."[1610] This requirement of specific, actual knowledge seems contrary to the courts' rulings in the Aimster case, discussed in Section III.C.2(c)(3) above, and in the Ellison and Perfect 10 v. Cybernet Ventures cases, discussed in Sections III.C.2(e) and (f) below, that constructive knowledge is sufficient for contributory infringement on the part of a service provider. In addition, the Ninth Circuit's ruling in Napster requiring actual knowledge of specific infringing files, invoked by the Ninth Circuit in its ruling on appeal of the district court's decision in this case, was repudiated by the Supreme Court in its Grokster decision, analyzed in detail below in Section III.C.2(c)(5) below.

[1605] John Borland, "Judge OKs Suit Against Kazaa Parent" (July 9, 2002), available as of July 10, 2002 at http://news.com.com/2102-1023-942533.html.

[1606] Declan McCullagh, "Judge: Kazaa Can Be Sued in U.S." (Jan. 10, 2003), available as of Jan. 13, 2003 at http://news.com.com/2102-1023-980274.html.

[1607] John Borland, "Kazaa Strikes Back at Hollywood, Labels" (Jan. 27, 2003), available as of Jan. 28, 2003 at http://news.com.com/2102-1023-982344.html.

[1608] Grokster, 259 F. Supp. 2d at 1033. The defendant Sharman Networks was not a party to the motions.

[1609] Id. at 1034.

[1610] Id. at 1036 (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001)).

The plaintiffs argued that the StreamCast and Grokster defendants had knowledge of the infringing acts because the plaintiffs had sent the defendants thousands of notices regarding alleged infringement. The court held, however, that "notices of infringing conduct are irrelevant if they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement," as was the case here since the infringing activity took place only after the defendants had distributed their software and, as elaborated under the material contribution prong, they were not in a position to stop the infringing activity.[1611]

Citing to the Supreme Court's Sony case, the court further ruled that mere distribution of a device that the defendants had general knowledge could be used to commit infringement was insufficient to impose contributory liability, so long as the device was capable of substantial noninfringing uses. The court noted several substantial noninfringing uses for the defendants' software, including distributing movie trailers, free songs or other non-copyrighted work, sharing the works of Shakespeare, and sharing other content for which distribution is authorized.[1612]

Turning to the material contribution prong, the court ruled that neither StreamCast nor Grokster had materially contributed to the infringing acts of users of their software. The court first noted that the Ninth Circuit found liability in the Napster case because Napster did more than distribute client software – it also hosted a central list of files available on each user's computer and "thus served as the axis of the file-sharing network's wheel."[1613] Here, "the critical question is whether Grokster and StreamCast do anything, aside from distributing software, to actively facilitate – or whether they could do anything to stop – their users' infringing activity."[1614]

With respect to Grokster, the court noted that Grokster did not have access to the source code of the FastTrack client software application, and its primary ability to affect its users' experience was the ability to configure a "start page" in the software and to provide advertising automatically retrieved by the software. An individual node using the FastTrack software automatically self-selected its own supernode status, and utilized a preset list of "root supernodes," each of which functioned principally to connect users to the network by directing them to active supernodes.[1615] "While Grokster may briefly have had some control over a root supernode, Plaintiffs do not dispute that Grokster no longer operates such a supernode. Thus, the technical process of locating and connecting to a supernode – and the FastTrack network – currently occurs essentially independently of Defendant Grokster."[1616] The transfer of files

---

[1611] Grokster, 259 F. Supp. 2d at 1037.

[1612] Id. at 1035.

[1613] Id. at 1039.

[1614] Id.

[1615] Id. at 1040.

[1616] Id.. Primary root supernodes on the FastTrack network were operated by Kazaa BV and Sharman Networks. Id. at 1040 n.6.

among users was accomplished without any information being transmitted to or through any computers owned or controlled by Grokster.[1617]

With respect to StreamCast, the court noted that the Gnutella technology on which StreamCast was based was a "true" peer-to-peer network that was even more decentralized than FastTrack. Users connected to the Gnutella network by contacting another user who was already connected. The initial connection was usually performed automatically after the user's computer contacted one of many publicly available directories of those currently connected to the Gnutella network. Instead of using supernodes, search requests on the Gnutella network were passed from user to user until a match was found or the search request expired.[1618]

Accordingly, the court concluded that, unlike Napster, neither StreamCast nor Grokster provided the "site and facilities" for direct infringement. Users connected to their respective networks, selected files to share, sent searches, and downloaded files, all without material involvement of the defendants.[1619] "If either Defendant closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption."[1620] The defendants therefore did not provide sufficient material contribution to the infringing acts of users to be liable as contributory infringers.[1621]

An analysis of the court's rulings with respect to vicarious liability may be found in Section III.C.3(f) below.[1622]

On appeal, the Ninth Circuit affirmed.[1623] Turning first to the knowledge prong of contributory infringement, the Ninth Circuit noted that any examination of contributory copyright infringement must be guided by the seminal Sony case, under which it is sufficient to defeat a claim of contributory infringement if the defendant shows that its product is capable of substantial or commercially significant noninfringing uses.[1624] The court noted that, based on Sony, it had held in the first appeal in the Napster case that if substantial noninfringing use was

---

[1617] Id. at 1040.

[1618] Id. at 1041.

[1619] Id.

[1620] Id.

[1621] Id. at 1043. Nor did the provision of technical assistance to their users constitute a material contribution to infringement, because the technical assistance was rendered only after the alleged infringements too place, was routine and non-specific in nature. Id. at 1042.

[1622] In January of 2004, the district court ruled that Sharman Networks could pursue claims against the record labels and Hollywood studios for copyright infringement and breach of contract based on allegations that, in their effort to find people sharing files illegally, the labels and studios used unauthorized and unlicensed versions of the Kazaa software to monitor users of the network. Sharman Networks also claimed that the labels breached the software license agreement by sending instant message warnings and bogus files through the network. Jon Healy, "Kazaa Owner Cleared to Sue Record Labels, Movie Studios" (Jan. 23, 2004), available as of Jan. 23, 2004 at www.latimes.com/technology/la-fi-kazaa23jan23,1,2476555.story.

[1623] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004).

[1624] Id. at 1160-61.

shown, the copyright owner would be required to show that the defendant had reasonable knowledge of specific infringing files:

> Thus, in order to analyze the required element of knowledge of infringement, we must first determine what level of knowledge to require. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue *is* capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.[1625]

Thus, the Ninth Circuit in effect read the Sony case as essentially nothing more than a gloss on the knowledge prong of contributory liability (and therefore inapplicable to vicarious liability), rather than an independent defense to any secondary copyright liability based upon the sale and distribution of technology that is capable of substantial noninfringing uses. The Ninth Circuit further noted that Judge Posner had, in the Aimster case discussed in Section III.C.2(c)(3) above, read Sony's substantial noninfringing use standard differently by looking at how "probable" the noninfringing uses of a product are. The Ninth Circuit stated that it simply did not read Sony as narrowly as Judge Posner did.[1626]

Because there was no genuine issue of material fact that there were substantial noninfringing uses of the defendants' software, the court concluded that the "reasonable knowledge of specific infringement" requirement was to be applied, and turned to an analysis of whether the copyright owners had raised sufficient genuine issues of material fact to satisfy that higher standard. The Ninth Circuit agreed with the district court that the plaintiffs' notices of infringement were irrelevant to the knowledge prong because they arrived when the defendants did nothing to facilitate, and could not do anything to stop, the alleged infringement of the specific copyrighted content.[1627] The court emphasized the great import of the software design to its holding. Unlike the Napster case, in which Napster maintained a centralized set of servers with an index of available files, no central index was maintained by the defendants' software. Accordingly, even if the defendants were to close their doors and deactivate all their computers, users of their products could continue sharing files with little interruption.[1628]

Turning to the material contribution prong, the Ninth Circuit agreed with the district court's conclusion that the defendants did not provide the "site and facilities" for infringement because the defendants did not provide file storage or index maintenance on their computers, nor did the defendants have the ability to suspend user accounts.[1629] "Rather, it is the users of the

---

[1625] Id. at 1161.

[1626] Id. at 1162 n.9.

[1627] Id. at 1162.

[1628] Id. at 1163.

[1629] Id.

software who, by connecting to each other over the internet, create the network and provide the access. 'Failure' to alter software located on another's computer is simply not akin to the failure to delete a filename from one's own computer, to the failure to cancel the registration name and password of a particular user from one's user list, or to the failure to make modifications to software on one's own computer."[1630]

The court also found that the defendants had not materially contributed to the infringement in any other manner. StreamCast maintained an XML file from which user software periodically retrieves parameters, including the addresses of web sites where lists of active users were maintained. The owner of the FastTrack software, Sharman, maintained root nodes containing lists of currently active supernodes to which users could connect. Both defendants also communicated with users incidentally, but not to facilitate infringement. The court found all of these activities too incidental to any direct copyright infringement to constitute material contribution. Accordingly, the defendants were not liable for contributory infringement.[1631]

On appeal, the Supreme Court vacated the Ninth Circuit's decision, rejecting much of its analysis, and remanded the case for further proceedings. The Supreme Court's decision is analyzed in detail in the next subsection below. In November of 2005, in view of the Supreme Court's decision, Grokster agreed to shut down its operations entirely to settle the lawsuits against it. The settlement bans Grokster from participating directly or indirectly in the theft of copyrighted files and requires the company to stop giving away its software. Grokster's web site was changed to display a message that said, "There are legal services for downloading music and movies. This service is not one of them."[1632]

Subsequent to the Supreme Court's decision, Grokster settled with the plaintiffs for $50 million and a permanent injunction,[1633] and Sharman Networks settled with the plaintiffs for $115 million and agreed to launch a "legitimate" service.[1634]

International Lawsuits Against the Kazaa Service. Lawsuits were also filed in the Netherlands against the operator of the Kazaa service. On Nov. 29, 2001, an Amsterdam court ordered the service to block customers from trading illegal files by Dec. 13, 2001 or face fines of

---

[1630] Id. at 1163-64.

[1631] Id. at 1164. The court noted that the copyright owners had also sought relief based on previous versions of the defendants' software, which contained significant, and perhaps crucial, differences from the software at issue on appeal. The Ninth Circuit noted that it was expressing no opinion as to those issues. Id. at 1166.

[1632] Ted Bridis, "Grokster Downloading Service Shuts Down" (Nov. 7, 2005), available as of Nov. 7, 2005 at http://news.tmcnet.com/news/2005/nov/1201939.htm.

[1633] "Grokster Settles, Streamcast Fights" (Nov. 8, 2005), available as of July 27, 2006 at www.marketingvox.com/archives/2005/11/08/grokster_settles_streamcast_fights/.

[1634] "Kazaa to Settle File-Share Lawsuits" (July 28, 2006), available as of July 28, 2006 at http://www.mercurynews.com/mld/mercurynews/business/technology/15143252.htm. Kazaa also subsequently settled with the music publishers. "Music Publishers Say Kazaa Deal Reached" (Oct. 31, 2006), available as of Nov. 1, 2006 at www.washingtonpost.com/wp-dyn/content/article/2006/10/31/AR2006103100953.htm.

$45,000 per day.[1635] On Jan. 17, 2002, Kazaa suspended downloads of the FastTrack software pending a further decision from the Dutch court.[1636] In late Jan. 2002, Kazaa BV sold its Kazaa.com web site to an Australian firm, Sharman Networks Limited, which then resumed operation of the file-swapping service.[1637] In December of 2003, the Dutch Supreme Court affirmed a ruling of the Court of Appeals in Amsterdam that reversed the ruling of the lower court, finding that Kazaa could not be liable for the copyright infringements committed by users of its software because the Kazaa service did not require centralized servers, as did the Napster service, and the software was capable of sharing many types of files other than audio files and was in fact being used for noninfringing uses.[1638] In December of 2005, Sharman Networks cut off Australians' access to the web site from which the Kazaa file swapping software could be downloaded in order to comply with orders from Australia's Federal Court. Sharman Networks also warned existing Australian users that use of the software was not permitted in Australia, pending an appeal.[1639]

(5) The Supreme Court's Grokster Decision

In one of the most significant copyright decisions since the Sony case, the Supreme Court vacated the Ninth Circuit's ruling in the Grokster case and remanded it for further proceedings. In its decision, taking inspiration again from the patent law, as it had in the Sony case, the Supreme Court introduced inducement liability for the first time into U.S. copyright law. The Court largely sidestepped, however, the opportunity to clarify a number of open questions about the scope of contributory liability and the Sony defense, with respect to many of which the Ninth Circuit and the Seventh Circuit had issued conflicting rulings in the Grokster and Aimster cases, respectively.

Open Issues Going Into the Appeal. In order to best understand the scope of the Supreme Court's decision – both what it decided and the issues it left open – it is useful to begin by noting the issues of secondary liability with respect to which the Ninth Circuit (in its Napster and Grokster decisions) and the Seventh Circuit (in its Aimster decision) had issued contrary rulings before the appeal to the Supreme Court. From the analyses of these cases in earlier sections[1640] it is apparent that the two Circuits differed in their interpretation of Sony on at least the following dimensions:

[1635] Jasper Koning, "Kazaa Plays On Despite Threat of Fines" (Dec. 20, 2001), available as of Jan. 6, 2002 at http://news.cnet.com/news/0-1005-200-8245314.html.

[1636] Brad King, "Kazaa Halts Download Distribution" (Jan. 18, 2002), available as of Jan. 18, 2002 at www.wired.com/news/mp3/0,1285,49831,00.html.

[1637] Associated Press, "Kazaa Still Up Despite Orders" (Jan. 31, 2002), available as of Feb. 10, 2002 at www.wired.com/news/mp3/0,1285,50165,00.html.

[1638] "Kazaa Software Does Not Violate Dutch Copyright Law, High Court Rules," *BNA's Electronic Commerce & Law Report* (Jan. 7, 2004) at 11.

[1639] Ian Ferguson, "Sharman Cuts Off Kazaa Downloads in Australia" (Dec. 5, 2005), available as of Dec. 6, 2005 at www.news.com.com/2100-1027_3-5983455.html.

[1640] See Sections III.C.2(c)(1) & (4) (Napster and Grokster, respectively) and III.C.2(c)(4) (Aimster).

- What types of secondary liability the Sony defense applies to: contributory liability only (Ninth Circuit) versus both contributory and vicarious liability (Seventh Circuit).

- How the Sony defense should be interpreted: as merely a gloss on the type of knowledge required for contributory liability (Ninth Circuit) versus a cost/benefit analysis of the infringing and noninfringing uses of a system to determine whether contributory liability should be imposed (Seventh Circuit).

- What triggers the Sony defense: mere capability of substantial noninfringing uses of the technology at issue (Ninth Circuit) versus "principal," actual uses (Seventh Circuit).

- Whether Sony imposes a duty to redesign technology to avoid or reduce infringing uses: no (Ninth Circuit) versus yes if not disproportionately costly to do so (Seventh Circuit).

These contrary rulings from the Circuits, together with the petitioners' and respondents' briefs and a host of amicus briefs, presented a number of questions that the Supreme Court could have resolved through this case:

- Does Sony afford an independent, stand-alone immunity to secondary copyright liability based upon the sale and distribution of technology that is capable of substantial noninfringing uses, or is it merely a gloss on the knowledge prong of contributory liability?

- More generally, does the Sony defense apply to both contributory and vicarious liability, or only to contributory liability?

- If the Sony defense is an independent immunity, what is its relationship to the traditional doctrines of secondary liability?

- With respect to noninfringing uses of a technology, do merely potential uses count, or only actual uses?

- Is a cost/benefit analysis required to determine whether the Sony immunity should apply?

- Is there any difference between "substantial" and "commercially significant" noninfringing uses and which is the operative test for triggering the Sony immunity (the Supreme Court used both phrases in its Sony opinion in immediately contiguous sentences without elucidating whether it meant any difference between the two phrases, and if so, which standard should govern)?

- Must the distributor of a technology that can be used for infringing uses redesign its product to reduce or eliminate infringing uses in order to avoid secondary liability for them?

In their briefs on appeal, the petitioners urged the following principal positions with respect to these questions:

- That a court should examine the "primary" actual uses of a technology, not merely the potential or theoretical uses, to determine whether its distribution should qualify for immunity from liability under the Sony doctrine;

- That, by analogy to the inducement doctrine of patent law, the defendant's subjective intent with respect to how the technology would or should be used should be examined to determine liability;

- That a cost/benefit analysis as explicated in the Aimster case should always be required to determine whether the Sony immunity is available for a technology;

- That Sony affords a defense only to contributory liability, and not to vicarious liability;

- That one should examine, under the financial benefit prong of the vicarious liability test, whether the defendant's business model is substantially predicated on infringement; and

- That the control prong of vicarious liability should be deemed satisfied where the defendant has failed to exercise control or refused to implement readily available mechanisms to reduce or prevent infringement.

As explicated below, the Supreme Court did not resolve most of the questions identified above, nor did it directly accept any of the positions advocated by the petitioners, at least in the strong form in which they were urged on the Court. Instead, the Court adjudicated the case on its newly introduced doctrine of copyright inducement liability. The Court articulated a standard for inducement liability, noted the kinds of behavior that might give rise to such liability, and remanded the case for further proceedings under the new standard. In the process, the Court's opinion not only left open most of the questions noted above, but gave rise to a number of new questions about the scope of inducement liability that will have to be resolved by the lower courts in future decisions in which inducement liability is invoked by the plaintiff.

The New Doctrine of Inducement Liability. Justice Souter, writing a 9-0 opinion for a unanimous Court, stated the principal question to be decided as "under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product."[1641] The Court answered this question by formally introducing inducement liability for the first time into U.S. copyright law. To do so, the Court analogized to patent law, as it had in the Sony case:

> For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear

[1641] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2770 (2005).

expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.[1642]

This test of inducement liability examines the intent or objective of the distributor of a product or technology that can be used to infringe. Where the distributor has shown "by clear expression or other affirmative steps" that it has an intent or object to foster infringement, there can be liability for inducement. The Court's rule grew out of its exegesis of Sony as a case about "imputed intent."[1643] Specifically, Justice Souter noted that "*Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement."[1644] Note that Justice Souter used a new phrase ("capable of substantial lawful use") that is different from each of the alternative two phrases used in Sony – "capable of substantial noninfringing uses" and "capable of commercially significant noninfringing uses" – against which a technology or product must be measured for the Sony immunity to apply. He did not state, however, whether the new phrase was intended to have a different meaning from either of the phrases used in Sony, or to subsume those two phrases into a single moniker.

It is unclear from the majority opinion whether the inducement doctrine is meant to form a third basis for secondary liability, in addition to the traditional contributory and vicarious liability doctrines, or whether the Court intended it to be merely one species of contributory liability. At one point in the opinion, Justice Souter stated, "One infringes contributorily by intentionally inducing or encouraging direct infringement … and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it."[1645] This sentence suggests that intentional inducement is but one species of contributory infringement, as distinct from vicarious liability. And Justice Souter's interpretation of Sony as a case "about … imputed intent"[1646] reinforces this notion, since intent is the primary issue for copyright inducement liability as set forth by the Court. Yet Justice Breyer's concurring opinion implies that the inducement doctrine is a new basis for liability distinct from contributory and vicarious liability, for he notes that the Court's opinion should further deter infringement "by adding a weapon to the copyright holder's legal arsenal."[1647] Justice Ginsburg's concurring opinion contains a similar inference in her statement that on the record before the Court, Grokster and StreamCast could be liable "not only for actively inducing copyright infringement," but "alternatively" for contributory infringement.[1648]

[1642] Id. at 2780.

[1643] Id. at 2778.

[1644] Id. Justice Souter noted that inferred intent, based solely on the distribution of a product with knowledge that it would be used for some infringing purposes, was the only intent at issue in Sony because the record contained "no evidence of stated or indicated intent to promote infringing uses" on the part of Sony. Id. at 2777.

[1645] Id. at 2776.

[1646] Id. at 2778.

[1647] Id. at 2791.

[1648] Id. at 2783.

Despite the ambiguity in the opinion, it seems to be the better view that the inducement doctrine should be seen as a separate basis for secondary liability distinct from that of the traditional contributory and vicarious liability doctrines. In addition to the fact that Justice Breyer reads it that way in his concurrence, Justice Souter notes that Sony, although it forbade imputing culpable intent as a matter of law from the characteristics or uses of a distributed product, was never meant to foreclose rules of "fault-based liability derived from the common law."[1649] The traditional doctrine of contributory infringement, as articulated by the courts before the Grokster opinion, was not grounded on a concept of "fault," thereby suggesting that the inducement doctrine and its associated notion of "fault" is something new. That notion of "fault" is to be found under the inducement doctrine in proof of intent to promote unlawful behavior, coupled with concrete steps taken to act out that intent.[1650] In addition, the kinds of evidence the Court notes as relevant to intent and inducement liability is different from the kinds of evidence courts had usually considered for contributory liability before the Grokster decision.[1651]

The Required Threshold of Showing of Unlawful Intent. From the majority opinion, it appears that the threshold of showing required to prove an unlawful intent to induce infringement will be rather high, so as to "leave[] breathing room for innovation and a vigorous commerce" founded on new technological products:[1652]

> [M]ere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.[1653]

[1649] Id. at 2779.

[1650] The Court noted that the staple article of commerce doctrine in general, and the Sony case in particular, "absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one's products will be misused." Id. at 2778.

[1651] The doctrines of contributory and inducement liability are clearly separate doctrines in the patent law, for they are embodied in separate statutory sections. 35 U.S.C. § 271(b) sets forth inducement liability: "Whoever actively induces infringement of a patent shall be liable as an infringer." 35 U.S.C. § 271(c) sets forth contributory liability: "Whoever offers to sell or sells within the United States or imports into the United States a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer." Treating inducement and contributory liability as separate doctrines in the copyright law would therefore afford a natural parallel to the patent law, to which the Court analogized in both Sony and Grokster.

[1652] Grokster, 125 S. Ct. at 2778.

[1653] Id. at 2780 (emphasis added).

On the other hand, inducement liability is not necessarily limited to encouragement of specific consumers to engage in infringing acts. "It is not only that encouraging a particular consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable act is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use."[1654]

The Ninth Circuit's Error. Based on its exegesis of Sony and the rule of inducement liability, the Court noted that the Ninth Circuit had erred in its understanding of secondary liability and the boundaries placed on it by Sony. Specifically, the Ninth Circuit in its Grokster opinion had read Sony's limitation to mean "that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had 'specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information.'"[1655] The Court found that the Ninth Circuit had, by this error, converted the case "from one about liability resting on imputed intent to one about liability on any theory."[1656] The Ninth Circuit's failure to consider an inducement basis for liability, and its affirmance of summary judgment for the defendants, was therefore sufficient grounds for reversal.[1657] Accordingly, the Court found it unnecessary "to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur"[1658] – in other words, to further explicate what "substantial" or "commercially significant" means as applied to the quantum of noninfringing uses required for Sony's immunity against imputed intent to apply.

Types of Evidence Relevant to Unlawful Intent. What kinds of evidence will be sufficient to prove an unlawful intent or object to induce or foster infringement? The Court noted the classic examples of "advertising an infringing use or instructing how to engage in an infringing use."[1659] With respect to the case at bar, the Court noted much in the record that could be used to establish an intent to encourage infringement on the part of the defendants. The Court found three features of this evidence particularly notable:

[1654] Id. at 2782 n.13. Although the Court does not address the issue, this language may suggest that, where a defendant has established a clear purpose to promote infringement through use of a product it distributes, injunctive relief can extend beyond the affirmative inducing acts and encompass distribution of the product itself.

[1655] Id. at 2778 (quoting Grokster, 380 F.3d at 1162 (9th Cir. 2004)).

[1656] Id.

[1657] Id.

[1658] Id.

[1659] Grokster, 125 S. Ct. at 2779.

Targeting Known Demand for Infringing Activity. First, both Grokster and StreamCast showed themselves to be aiming to satisfy a known source of demand for copyright infringement – the market comprising former Napster users.[1660] StreamCast's internal company communications and advertising designs were aimed at Napster users. One ad mockup, for example, stated, "When the lights went off at Napster … where did the users go?"[1661] An internal email from a company executive stated, "We have put this network in place so that when Napster pulls the plug on their free service … or if the Court orders them shut down prior to that … we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative."[1662] Significantly, the Court noted that whether these internal messages or ads were ever communicated to the public did not disqualify them as valid evidence of inducement, because they tended to establish the subjective purpose in the minds of the defendants, particularly when coupled with other evidence of concrete actions taken by the defendants.[1663] StreamCast and Grokster both distributed an "OpenNap" program, which was a Napster-compatible program for file sharing. Grokster distributed an electronic newsletter containing links to articles promoting its software's ability to access popular copyrighted music. The Court also noted that even Grokster's name was an apparent derivative of Napster.[1664] Finally, both companies responded affirmatively to requests for help in locating and playing copyrighted materials.[1665]

Absence of Effort to Reduce Infringing Activity. Second, the evidence of unlawful objective was given added significance by the fact that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software.[1666] In one of the most significant footnotes in the opinion, the Court stated that, absent other evidence of intent, there is no general duty to redesign a product to reduce or avoid infringement: "Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the *Sony* safe harbor."[1667] However, in this case, the Court believed that, given the very strong other evidence of intent to induce infringement, the failure to develop filtering

---

[1660] Id. at 2781.

[1661] Id. Another read, "Napster Inc. has announced that it will soon begin charging you a fee. That's if the courts don't order it shut down first. What will you do to get around it?" Id. at 2773.

[1662] Id. StreamCast delivered a press kit containing press articles about its potential to capture former Napster users, and it introduced itself to some potential advertisers as a company "which is similar to what Napster was." Id. StreamCast also planned to flaunt the illegal uses of its software; its chief technology officer averred that "the goal is to get in trouble with the law and get sued. It's the best way to get in the news."Id.

[1663] Id. at 2781. "Even if these advertisements were not released to the public and do not show encouragement to infringe, they illuminate StreamCast's purposes." Id. at 2773 n.7.

[1664] Id. at 2773, 2780.

[1665] Id. at 2781.

[1666]Id.

[1667] Id. at 2781 n.12.

tools underscored the defendants' intentional facilitation of their users' infringement.[1668] Moreover, the record established that the defendants had responded to questions from their users about how to play infringing movies they had downloaded.[1669]

Gains Proportional to Infringing Activity. Third, StreamCast's and Grokster's monetary gains were proportional to the volume of infringement by their users. Because both companies made money by selling advertising space directed to the screens of users, the more their software was used, the more ads that would be sent out and the greater their advertising revenues. The companies therefore had incentive to encourage high volume use, which the record showed was infringing.[1670] Again, the Court noted that "[t]his evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear."[1671]

Summary of Significant Aspects of the Court's Ruling. Based on the preceding analysis, the following key aspects of the majority opinion can be summarized:

- A defendant can be liable for inducing copyright infringement where the defendant takes acts or other affirmative steps with the subjective intent to promote infringement. The Court has, however, established a high standard of proof for demonstrating the required subjective intent to induce infringement, for its opinion uses language requiring "clear expression or other affirmative steps taken to foster infringement,"[1672] "purposeful, culpable expression and conduct,"[1673] and "a patently illegal objective."[1674] The purpose of this high standard is so as not to "compromise legitimate commerce or discourage innovation having a lawful purpose."[1675]

- Inducement liability cannot be based on the mere "characteristics" of a product, including its functional capability for use for infringing purposes, or on the mere "knowledge that it may be put to infringing uses."[1676] Instead, for inducement liability, "statements or actions directed to promoting infringement" through use of the technology are required.[1677] Thus, the Court's rule for inducement liability focuses on subjective purpose of the defendant rather than the technology itself. Two vendors of the same

---

[1668] Id. at 2781.

[1669] Id. at 2772.

[1670] Id. at 2781-82.

[1671] Id. at 2782. Thus, "the business models employed by Grokster and StreamCast confirm that their principal object was use of their software to download copyrighted works." Id. at 2774.

[1672] Id. at 2780.

[1673] Id.

[1674] Id. at 2782.

[1675] Id. at 2780.

[1676] Id. at 2779.

[1677] Id.

technology could therefore have different liability depending upon their actions and the intent behind them.

- Even where a distributed technology is used by some to commit infringement, the vendor of that technology can engage in ordinary acts incident to product distribution, such as offering customers technical support or product updates, and those acts, in themselves, will not establish inducement liability.[1678]

- The basic immunity of the Sony case remains intact. Sony continues to "bar[] secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement."[1679]

- In judging the subjective intent of a defendant accused of inducing infringement, a court may look at evidence of internal communications (whether or not released to the public or potential users), the business model of the defendant and whether it is predicated on infringement, product naming, advertising and press kits, customer support activities in response to specific questions about how to use the technology for infringing acts, targeting of users who are known to be committing or likely to commit infringing acts using the technology in question, whether the defendant has taken steps to reduce or eliminate use of its technology for infringement, and whether the defendant's gain is proportional to infringing volume.

- In the absence of other evidence of intent, mere failure to design or redesign a technology to avoid or reduce infringing uses, by itself, cannot form the basis of liability, if the technology is otherwise capable of substantial noninfringing uses.[1680] Where there is other evidence of purpose, however, failure to take steps to prevent infringing uses of a technology can reinforce an inference of subjective intent to induce infringement.

- The traditional tests for secondary liability – the contributory and vicarious liability doctrines – as articulated by the courts before the Grokster case remain intact.

The Court left open a host of questions with respect to the issue of product design and infringement avoidance, which the lower courts will be left to work out:

- What threshold showing of intent must be made before the failure to design a product to reduce or avoid infringement becomes relevant to show culpable purpose to encourage infringement? The Court's opinion generally requires "clear expression or other affirmative steps" to promote infringement. Must the plaintiff therefore show a "clear expression" of purpose or "affirmative steps" taken through other evidence before the evidence of failure to design becomes even relevant? Or is a lesser quantum of other

[1678] Id. at 2780.

[1679] Id. at 2778.

[1680] Id. at 2781 n.12.

evidence sufficient to trigger the relevancy of failure to design evidence, which can then be aggregated with such other evidence to make a showing of "clear expression"? If a lesser quantum of other evidence is sufficient, what is that quantum?[1681] And must such other evidence be direct evidence, or may it be circumstantial evidence?

- Once evidence of failure to design to avoid infringement becomes relevant, what substantive standard governs the extent to which the product must be designed to avoid or reduce infringement? Presumably some kind of reasonableness standard will govern that looks to both the state of the art of technology that could be deployed in the design to reduce infringement, as well as the costs and benefits of that technology.

- Does the copyright holder itself have a duty to reduce or prevent infringement of its copyrighted material by deploying technology (such as DRM technology) to protect it at the time of distribution? If so, how is the burden to deploy technological means to reduce infringement to be allocated between the copyright holder and the distributor of the products or services that are ultimately used to commit infringement?

- Can a defendant use evidence of affirmative steps it took to prevent infringement as a defense to inducement liability?

- Monetary gain from infringing activity does not by itself justify an inference of unlawful intent. But where there is other strong evidence of unlawful intent, gain that is proportional to infringing activity can be reinforcing evidence of intent.[1682] Similar questions as those discussed in the preceding bullets arise with respect to the threshold showing of intent through other evidence that must be made before evidence of monetary gain from infringing activity is relevant. Also unknown is the substantive standard governing what kinds of monetary gain will be cognizable as evidence of intent to promote infringement, and how directly tied to the infringing activity such monetary gain must be.

One can expect that the doctrine of inducement will take on a jurisprudential life of its own, with attendant uncertainty as to standards and outcomes as further judicial development takes place. The focus on subjective intent and the business model of the defendant will likely make summary judgment more difficult to obtain in inducement cases than in other secondary liability cases. Finally, one can expect that the written record relating to development and

---

[1681] The inducement rule set up by the Court in Grokster appears to differ a bit from the active inducement rule in patent law. Some patent cases, most notably Oak Industries, Inc. v. Zenith Electronics Corp., 726 F. Supp. 1525 (N.D. Ill. 1989), distinguish between an affirmative act directed toward encouraging or promoting infringement, and the distinct element of intent to induce, which can be proved by evidence not only of affirmative acts but also design omissions. By contrast, the Grokster opinion requires that intent be shown by "clear expression or other affirmative steps taken to foster to infringement." Unlike the patent law, then, intent cannot be established through acts of design omission alone. See Matthew Brown et al., "Secondary Liability for Inducing Copyright Infringement After MGM v. Grokster: Infringement-Prevention and Product Design," *Journal of Internet Law*, Dec. 2005, at 21, 25.

[1682] Grokster, 125 S. Ct. at 2782.

promotion of a technology, including purely internal communications, will be crucial to the issue of intent and therefore the focus of discovery and litigation in inducement cases.

The Concurring Opinions – Disagreement About the Scope of the Sony Safe Harbor. Despite the urging of the petitioners, the majority opinion found it unnecessary to provide "a more quantified description" of what level of noninfringing uses are required to qualify as "substantial" or "commercially significant" within the meaning of Sony. Six of the justices, however, in two concurring opinions, joined this issue and advocated significantly different positions.

The first concurring opinion was authored by Justice Ginsburg and joined by Chief Justice Rehnquist and Justice Kennedy. Justice Ginsburg noted that, in addition to liability under the inducement doctrine articulated by the majority, one could be liable under traditional contributory infringement principles for distributing a product that users use to infringe copyrights, if the product is not capable of "substantial" or "commercially significant" uses.[1683] Without choosing between, or articulating any difference between, the two phrases "substantial" and "commercially significant," she elaborated on her understanding of what those phrases in Sony mean collectively.

Although not stating so explicitly, Justice Ginsburg's opinion seems based on two key interpretations of the Sony safe harbor: (i) that it requires a court to focus more on actual uses of a product, or those that are concretely likely to develop over time, rather than merely potential uses, and (ii) that one should balance the relative numbers of infringing and noninfringing uses, and not merely the absolute number of noninfringing uses.

With respect to the first principle, Justice Ginsburg expressed the belief that, unlike in Sony, there had been no finding of fair use and "little beyond anecdotal evidence of noninfringing uses."[1684] She noted that the district court's conclusion of substantial noninfringing uses rested almost entirely on a collection of declarations submitted by Grokster and StreamCast, and that review of those declarations showed a collection of mostly anecdotal evidence, sometimes obtained second-hand, of authorized copyrighted works or public domain works available online and shared through peer-to-peer networks, and general statements about the benefits of peer-to-peer technology.[1685] She concluded that the declarations did not support summary judgment in the face of evidence proffered by the plaintiffs of "overwhelming use of Grokster's and StreamCast's software for infringement"[1686] – clearly focusing on the current, actual uses of the software. Nor did she see a realistic possibility that concrete noninfringing uses were likely to develop over time. "Fairly appraised, the evidence was insufficient to

---

[1683] Id. at 2783 (Ginsburg, J., concurring).

[1684] Id. at 2785.

[1685] Id.

[1686] Id. at 2786.

demonstrate, beyond genuine debate, a reasonable prospect that substantial or commercially significant noninfringing uses were likely to develop over time."[1687]

Concerning the second principle, Justice Ginsburg stated, "Even if the absolute number of noninfringing files copied using the Grokster and StreamCast software is large, it does not follow that the products are therefore put to substantial noninfringing uses and are thus immune from liability. The number of noninfringing copies may be reflective of, and dwarfed by, the huge total volume of files shared."[1688]

The second concurring opinion, authored by Justice Breyer and joined by Justices Stevens and O'Connor, expressly disagreed with Justice Ginsburg's opinion and articulated a very different understanding of the Sony safe harbor. Justice Breyer began his analysis by noting how low a number of actual authorized uses were required in Sony to qualify as "substantial." Specifically, the record showed that of all the taping actually done by Sony's customers, only around 9% was of the sort the Court referred to as authorized, yet the Court found the magnitude of authorized programming was "significant."[1689] Justice Breyer noted that the Sony Court had concluded from this evidence that rights owners had authorized duplication of their copyrighted programs "in significant enough numbers to create a *substantial* market for a noninfringing use" of the VCR.[1690] By using the key word "substantial," the Sony Court had concluded that 9% authorized uses alone constituted a sufficient basis for rejecting the imposition of secondary liability. Justice Breyer then concluded that, when measured against the evidence of authorized use present in Sony, the evidence before the Court in the Grokster case should be sufficient to pass the test of Sony. Specifically, the plaintiffs' evidence showed 75% of current files available on Grokster as infringing and 15% likely infringing. That left approximately 10% of files that were apparently noninfringing, a figure very similar to the 9% of authorized uses of the VCR the Court faced in Sony.[1691]

In addition, Justice Breyer noted that Sony's standard also incorporates the word "capable" with respect to noninfringing uses, and concluded "that a figure like 10%, if fixed for all time, might well prove insufficient, but that such a figure serves as an adequate foundation where there is a reasonable prospect of expanded legitimate uses over time."[1692] He found that the record revealed a significant future market for noninfringing uses of peer-to-peer software like Grokster's, and the combination of such foreseeable development, together with an estimated 10% of existing noninfringing material, is sufficient to meet Sony's standard.[1693]

[1687] Id.

[1688] Id.

[1689] Id.

[1690] Id. (quoting Sony, 464 U.S. at 447 n.28) (emphasis added by Justice Breyer).

[1691] Grokster, 125 S. Ct. at 2788-89.

[1692] Id. at 2789.

[1693] Id. at 2789-90.

Justice Breyer then reviewed the appellate decisions construing Sony and noted that only one – the Seventh Circuit's Aimster decision – had interpreted Sony more strictly that he would do.[1694] Based on a review of those appellate decisions, he concluded that Sony establishes "that the law will not impose copyright liability upon the distributors of dual-use technologies (who do not themselves engage in unauthorized copying) unless the product in question will be used *almost exclusively* to infringe copyrights (or unless they actively induced infringements as we today describe)."[1695]

Justice Breyer lauded this interpretation of Sony as encouraging technical innovation by providing "entrepreneurs with needed assurance that they will be shielded from copyright liability as they bring valuable new technologies to market."[1696] It does so in the following ways:[1697]

- The Sony rule, as so interpreted, is clear, and allows those who develop new products that are capable of substantial noninfringing uses to know, ex ante, that distribution of their product will not yield massive monetary liability.

- It is strongly technology protecting, sheltering a product unless it will be used almost exclusively to infringe.

- It is forward looking, and does not confine the safe harbor to a static snapshot of a product's current uses, but rather looks to uses of which the product is capable.[1698]

- It is mindful of the limitations facing judges where matters of technology are concerned, since judges have no specialized technical ability to answer questions about present or future technological feasibility or commercial viability where technology professionals, engineers, and venture capitalists may radically disagree and where answers may differ depending upon whether one focuses upon the time of product development or the time of distribution.

Justice Breyer concluded that a modified Sony rule as urged by the petitioners or as interpreted by Justice Ginsburg would significantly chill technological development, as innovators would have no way to predict how courts would weigh the respective values of infringing and noninfringing uses, determine the efficiency and advisability of technological changes or assess a product's potential future markets.[1699]

[1694] Id. at 2790-91.

[1695] Id. 2791.

[1696] Id.

[1697] See id. at 2791-92.

[1698] Justice Breyer interpreted the word "capable" as used in Sony to refer "to a plausible, not simply a theoretical, likelihood that such uses will come to pass, and that fact anchors Sony in practical reality." Id. at 2792.

[1699] Id. at 2792-93.

Justice Breyer concluded his opinion with the question of whether a modified Sony rule would yield a positive copyright impact that would outweigh any technology-related loss. Although he acknowledged that a more intrusive Sony test would generally provide greater revenue security for copyright holders, he found it harder to conclude that the gains to copyright holders would exceed the losses to innovation. "For one thing, the law disfavors equating the two different kinds of gain and loss; rather, it leans in favor of protecting technology."[1700] In addition, since Sony has been the law for quite some time, there should be a serious burden on copyright holders to show a need for a more strict interpretation of the current rules. Justice Breyer concluded that a strong demonstrated need for interpreting the Sony standard more strictly had not been shown and that the Court should maintain Sony, reading it as he had interpreted it.[1701]

Issues Left Open by the Supreme Court. The Supreme Court's opinion left open a host of unanswered questions concerning secondary liability and the scope of the Sony immunity. Among them are the following:

- Whether there is any substantive difference between the phrases "capable of substantial noninfringing uses" and "capable of commercially significant noninfringing uses" as used in Sony. None of the majority opinion or the two concurrences expressly analyzes a difference, and all seem to treat the phrases as interchangeable. However, given that all justices agreed that the Sony standard need not be revisited as part of the Court's disposition of the case, and given that Justice Souter introduced yet a third phrase in the majority opinion – "capable of substantial lawful use" – the issue was not definitively resolved by the case.

- Whether Sony requires consideration of the relative balance of the infringing uses against the noninfringing uses of a technology. Justice Ginsburg's concurrence seems to require such a balance, whereas Justice Breyer's concurrence does not. The majority opinion does not reach the issue.

- Whether Sony requires some minimal threshold of noninfringing uses, and if so, what that threshold is. The wide split in conclusions from the record in the Grokster case expressed in the concurring opinions illustrate how unsettled this question was among the members of the Court that decided Grokster. Moreover, three justices did not express an opinion of any kind on the issue.

- What "capable of" means in the Sony test. Both concurrences seem to reject a meaning of purely theoretical uses. However, Justice Ginsburg's concurrence focuses much more on the actual uses of a product, whereas Justice Breyer's concurrence evidences more of a willingness to look to future legitimate uses that might be precluded by a strict interpretation of the Sony safe harbor. Stated differently, Justice Ginsburg's concurrence

[1700] Id. at 2793.

[1701] Id. at 2793-96.

appears predisposed to favor the copyright holders rights, whereas Justice Breyer's concurrence is predisposed to favor technological innovation.

- Whether the Sony immunity applies to both contributory and vicarious liability, or only to contributory liability. Justice Souter's majority opinion does not address vicarious liability at all: "Because we resolve the case based on an inducement theory, there is no need to analyze separately MGM's vicarious liability theory."[1702]

- What level of active encouragement will be sufficient to find inducement in less egregious cases. Related questions include (i) the meaning of "clear expression" of intent and "purposeful, culpable expression and conduct," and (ii) if there is little "expressive" evidence of purpose, what kinds of acts or omissions will qualify as "other affirmative steps taken to foster infringement."

- At what point in time the defendant's "intent" is to be measured – at the time of original design of the technology, at the time of distribution, at some other time?

- Whether the defendant must merely intend to induce the acts that give rise to infringement, or intend to cause infringement itself. For example, what happens if the defendant had a good faith belief at the time of product design or promotion that the intended acts were fair use, but they are later judged infringing? Must the belief be objectively reasonable?

- Under what circumstances failure to design or redesign a product to avoid or reduce infringement can be used as proof of intent to induce infringement, and when a vendor of technology has an obligation to redesign in order to avoid inducement liability. As analyzed above, there are a host of questions left unanswered by the Court's opinion with respect to the issue of design to avoid infringement.

- Whether the Seventh Circuit's approach to the Sony safe harbor in the Aimster case is correct or not. None of the three opinions in Grokster expressly address whether the Aimster approach erred in various aspects. The majority opinion cites the Aimster case only for the factual proposition that it may be impossible to enforce rights in a protected work effectively against all direct infringers, making the only practical alternative going against the distributor of the copying device for secondary liability.[1703] Justice Ginsburg's concurring opinion merely notes the conflict between the Aimster and Napster decisions and states only that all members of the Court agree that the Ninth Circuit misapplied Sony, at least to the extent it read that decision to limit secondary liability to a "hardly-ever category."[1704] Justice Breyer's concurring opinion cites Aimster only for the proposition that there is but a single appellate decision to date

[1702] Id. at 2776 n.9 (Souter, J.).

[1703] Id. at 2776.

[1704] Id. at 2784 n.1 (Ginsburg, J., concurring).

interpreting Sony more strictly than Justice Breyer would.[1705] Nevertheless, it seems that, to the extent the Aimster decision suggests that failure to affirmatively prevent infringing uses could by itself, without other evidence of unlawful intent, subject a defendant to liability, it is plainly inconsistent with the Grokster majority opinion.[1706] In addition, Aimster's general cost/benefit balancing approach to the Sony safe harbor may not survive the majority opinion either.[1707]

Although the Grokster case is one of the most important copyright decisions to come out of the Supreme Court, it clearly left much work to be done by the lower courts, and perhaps the Supreme Court itself in future copyright decisions, to work out the boundaries of the copyright inducement doctrine and the Sony safe harbor.

(6) The Grokster Decision on Remand

(i) The Ruling on Liability

Defendant Grokster settled with the plaintiffs shortly after the Supreme Court's decision. On remand from the Supreme Court, the district court granted the plaintiffs' motion for summary judgment as to liability of defendants StreamCast and Sharman for inducing copyright infringement.[1708] Not surprisingly, the district court's ruling essentially tracked the Supreme Court's analysis, which had strongly presaged the ultimate outcome of the case.[1709] By and large, the district court's opinion did little more than elaborate factually on the various bases the Supreme Court had identified in its opinion upon which the defendants could be held liable under the inducement doctrine.

The district court may, however, have put one important gloss on the Supreme Court's legal rulings that may represent an extension of the scope of inducement liability. Specifically, StreamCast argued that a defendant could be found liable under the inducement doctrine only if it: (1) for the purpose of inducing infringement, (2) took actions beyond distributing infringement enabling technology, and (3) which actually resulted in specific instances of

---

[1705] Id. at 2790 (Breyer, J., concurring).

[1706] "Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the Sony safe harbor." Id. at 2781 n.12 (Souter, J.).

[1707] See Mitchell Zimmerman, "Does *Aimster* Survive *Grokster,*" *Cyberspace Lawyer*, Dec. 2005, at 1 (noting that Aimster insisted that "balancing of costs and benefits is necessary," even in cases "in which substantial noninfringing uses, present or prospective, are demonstrated, whereas Grokster says instead that "the [Sony] doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses …"). Mr. Zimmerman's article notes several other ways in which the Grokster majority opinion may *sub silentio* disapprove of Aimster.

[1708] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 454 F. Supp. 2d 966 (C.D. Cal. 2006).

[1709] Indeed, the district court noted in its opinion after reviewing all the evidence that "in Grokster the Supreme Court had hinted that summary judgment should be granted for Plaintiffs after reviewing much of the same evidence." Id. at 992.

infringement. In StreamCast's view, even if it distributed peer-to-peer software with the intent for it to be used for infringement, liability would not attach unless it took further actions, such as offering instructions on infringing use, that actually caused specific acts of infringement. StreamCast devoted much energy to arguing that the plaintiffs had failed to prove the second and third elements of its proposed test.[1710]

The district court rejected StreamCast's argument, finding it contrary to the following language from the Supreme Court's decision:

> It is not only that encouraging a particular consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable conduct is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use.[1711]

From this passage, the district court went on to conclude, "Thus, Plaintiffs need not prove that StreamCast undertook specific actions, beyond product distribution, that caused specific acts of infringement. Instead, Plaintiffs need prove only that StreamCast distributed the product with the intent to encourage infringement."[1712] Although not entirely clear, it appears that in the district court's view, as long as a defendant has a subjective intent to encourage infringement, the mere distribution of a product that is used by others to commit infringement is sufficient to make the distributor of the product secondarily liable. Such a rule, however, appears to be inconsistent with the Supreme Court's ruling. In the passage quoted by the district court, the Supreme Court stated that "distribution of a product can itself give rise to liability where evidence shows that the distributor intended *and encouraged the product to be used to infringe*."[1713] The use of the conjunctive "and" followed by a requirement of encouraging a product to be used to infringe suggests that the Supreme Court did not view distribution of a product alone, coupled with a subjective intent on the part of the distributor to encourage infringement, would be sufficient for inducement liability. Rather, the distributor must in addition take actions that encourage the product to be used to infringe. Although the facts of the case, as elaborated below, seem sufficient to establish StreamCast's liability under either rule, the district court's articulation of the rule seems broader than, and therefore contrary to, the Supreme Court's Grokster ruling.

In any event, following the outline of the Supreme Court's analysis, the district court found a sufficient basis for inducement liability on the part of StreamCast based upon the following facts:

[1710] Id. at 984.

[1711] Id. at 984-85 (quoting Grokster, 125 S. Ct. at 2782 n.13).

[1712] 454 F. Supp. 2d at 985.

[1713] Grokster, 125 S. Ct. at 2782 n.13 (emphasis added).

-- StreamCast's software was used overwhelmingly for infringement: A study by the plaintiffs' experts showed that 87.33% of the files offered for distribution on the Morpheus network, and that almost 97% of the files actually requested for downloading, were infringing or highly likely to be infringing. The district court noted that, while infringing use by third parties was not by itself evidence of StreamCast's intent, the staggering scale of infringement made it more likely that StreamCast condoned illegal use and provided a backdrop against which all of StreamCast's actions had to be assessed.[1714]

-- StreamCast targeted Napster users: The district court found uncontroverted evidence, including internal communications, promotional efforts, advertising designs, and actual advertisements, establishing that StreamCast purposefully targeted Napster users, not merely to market to them, but to convert them into StreamCast users by offering them the same file-sharing service that Napster had itself offered.[1715]

-- StreamCast assisted infringing uses: StreamCast provided users with technical assistance for playback of copyrighted content, in one instance suggesting to a user who complained about the paucity of music from Elvis and Muddy Waters that he upload copyrighted content for sharing.[1716]

-- StreamCast ensured its technology had infringing capabilities: Among other things, the district court cited to evidence that, before deciding to license FastTrack technology for Morpheus, StreamCast's chairman evaluated FastTrack by searching for Garth Brooks songs on the FastTrack network. While Morpheus was in beta testing, StreamCast employees identified the insufficient quantity of popular copyrighted content on the network as an important problem, and many StreamCast employees tested the software's infringing capabilities by downloading copyrighted tracks. The Morpheus interface contained a search category for "Top 40" songs that were almost invariably copyrighted. And the court noted that StreamCast took active steps to protect illegal file trading from the enforcement efforts of copyright holders and deployed encryption technology so that the plaintiffs could not see what files were being transferred through Morpheus.[1717]

-- StreamCast's business model depended on massive infringing use: The record established that StreamCast knew its business model depended on massive infringing use, and acted to grow its business accordingly. StreamCast's CTO testified that StreamCast's objective in advertising to Napster users was to increase the number of users by increasing the amount of file sharing, since the more files that were physically available, the more users would come. The company tracked its progress after launch by tracking the number of files that were available for sharing, particularly as against those available for sharing through Napster.[1718]

[1714] 454 F. Supp. 2d at 985.

[1715] Id. at 985-86.

[1716] Id. at 986-87.

[1717] Id. at 987-88.

[1718] Id. at 988-89.

-- StreamCast took no meaningful affirmative steps to prevent infringement: Although noting that secondary liability could not be premised on failure to prevent infringing use alone, the district court noted the Supreme Court's holding that a defendant's failure to do so can indicate an intent to facilitate infringement.[1719] Based on this, the district court ruled, "By implication, although StreamCast is not required to prevent all the harm that is facilitated by the technology, it must at least make a good faith attempt to mitigate the massive infringement facilitated by its technology."[1720] The district court noted at least two technologies that StreamCast could have used to implement a system to filter out copyrighted content from the Morpheus network – acoustic fingerprinting using unique digital signatures for each music file for identification and metadata that describes the properties of a file, such as song title and artist name. With respect to the latter, the court noted that Morpheus executed file searches on the basis of metadata such as song names, and contained a feature that, if activated by the user, would filter out pornographic content on the basis of file name. The plaintiffs argued that the technology behind the pornographic filter could easily have been reconfigured to filter out copyrighted content.[1721]

StreamCast countered that metadata filtering would be burdensome and overbroad, as it would block all files that shared common words in metadata, even if the file was not copyrighted. StreamCast also argued that, with regard to FastTrack-based versions of Morpheus, it did not have the ability to directly modify the FastTrack source code, which the licensor controlled, to implement filtering.[1722] The court noted that, based on the foregoing, a jury could reasonably agree with StreamCast that copyright filtering would not work perfectly and implementing it would negatively impact usability.[1723] However, the court ruled that "the ultimate question … is to examine StreamCast's intent. Even if filtering technology does not work perfectly and contains negative side effects on usability, the fact that a defendant fails to make some effort to mitigate abusive use of its technology may still support an inference of intent to encourage infringement."[1724]

The court further noted that StreamCast saw its resistance to filtering as a competitive advantage, citing testimony of StreamCast's chairman that if Napster were forced to filter, StreamCast would take all of Napster's users. StreamCast was unreceptive when it was approached by GraceNote, a company that had worked with Napster on a way to use acoustic fingerprinting technology to identify copyrighted music and pay copyright holders.[1725]

[1719] Id. at 989.

[1720] Id.

[1721] Id. at 989-90.

[1722] Id. at 990.

[1723] Id.

[1724] Id.

[1725] Id. at 991.

Finally, the court ruled, although not in the context of a DMCA safe harbor defense asserted by StreamCast, that StreamCast's blocking of users from its network in response to requests from copyright holders was insufficient to absolve it from liability:

> This Court recognizes that StreamCast blocked certain users from its network when asked to do so by copyright holders. However, its effort was half-hearted at best. As described above, StreamCast used encryption technology to defeat Plaintiffs' monitoring efforts. Moreover, blocking users was not very effective because a user could simply create a new username to re-enter the network under a different identity. StreamCast had the capability of automatically blocking these users on a rolling basis, but expressly decided not to do so.[1726]

Based on these factual findings, the court concluded that "evidence of StreamCast's objective of promoting infringement is overwhelming" and granted summary judgment of liability for inducement on the part of StreamCast.[1727]

(ii) The Permanent Injunction

In a subsequent opinion, the district court considered the plaintiffs' proposal for a very broad permanent injunction against StreamCast.[1728] The court noted that, under the Supreme Court's decision in the eBay case,[1729] to be entitled to a permanent injunction on their copyrights, the plaintiffs were required to satisfy the traditional four part test for injunctive relief of irreparable harm, inadequate remedies at law, a balance of hardships in their favor, and that the public interest would not be disserved by an injunction.[1730] The court first turned to whether, having established infringement, the plaintiffs were entitled to a presumption of irreparable harm, and concluded that a presumption of irreparable harm no longer inures to a plaintiff after eBay in a permanent injunction case.[1731] Nevertheless, the court found that irreparable harm had been established for two reasons. First, Streamcast had and would continue to induce far more infringement than it could ever possibly redress with damages. Second, absent an injunction, a substantial number of the plaintiffs' copyrighted works would continue to be made available for

---

[1726] Id. at 992. The court did not elaborate on how StreamCast could have automatically blocked users on a "rolling basis."

[1727] Id. at 992, 999.

[1728] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 2007 U.S. Dist. LEXIS 79726 (C.D. Cal. Oct. 16, 2007).

[1729] eBay, Inc. v. MercExchange, L.L.C., 126 S. Ct. 1837 (2006).

[1730] Grokster, 2007 U.S. Dist. LEXIS at *30.

[1731] Id. at *38-40. The court noted significant division among the existing post eBay decisions concerning whether the traditional presumption of irreparable harm in a preliminary injunction context flowing from a showing of likelihood of success on the merits also failed to survive eBay. The court noted that, although the law was muddled and the Ninth Circuit had not yet spoken on the point post eBay, the better view is that the presumption probably did not survive eBay in a preliminary injunction context. Id. at *43-49.

unending infringement outside of the Morpheus system and software, effectively eviscerating the plaintiffs' ability to protect their property rights.[1732]

The court found that the plaintiffs had no adequate remedy at law because a statutory recovery for those infringements induced through the Morpheus system would not compensate the plaintiffs when those same files were subsequently shared outside the Morpheus system. The balance of hardships tipped in the plaintiffs' favor because StreamCast would likely engage in further inducement in the absence of a permanent injunction. Finally, an injunction would serve the public interest since it would protect the plaintiffs' copyrights against increased infringement.[1733]

Turning to the scope of the injunction, the court first ruled that the scope should not extend beyond inducement activities, because inducement was the only form of infringement that StreamCast had been found liable for. Accordingly, the court rejected the plaintiffs' proposed broad wording for the injunction to the extent it would reach activities giving rise to liability solely under contributory or vicarious liability doctrines, although the court noted that the injunction could properly extend to copyrighted works of the plaintiffs whether then in existence or later created.[1734]

The court then turned to the most interesting and significant issue relating to the injunction – whether it should require StreamCast to implement filtering of the plaintiffs' copyrighted works on its system, and if so, to what extent. StreamCast argued that, under Sony, its continued distribution of the Morpheus system and software was legal, even without filtering technology, so long as StreamCast did not engage in any additional actions or statements promoting infringement, because the system and software were capable of substantial non-infringing uses.[1735] The court rejected this argument, reasoning that under the Supreme Court's Grokster opinion, once acts of encouragement or promotion of infringement through a product or system have taken place, the further distribution of that product or system can be restricted as further acts of inducement:

> It is important to recognize that the Supreme Court did not impose any strict timing relationship between specific acts promoting infringements, distribution, and the direct infringements themselves. For a party to be liable for inducement, distribution may begin prior to any promotion of infringement, distribution and promotion can occur at the same time, and most critically, distribution can follow past promotion. … As a matter of common sense, a successful inducer will sometimes have no need to repeat the infringing message ad infinitum. This is

---

[1732] Id. at *57-62. The court ruled it would make no difference to the irreparable harm analysis if Streamcast's inducement was demonstrated to increase the plaintiffs' sales because, as copyright owners, plaintiffs "have the exclusive right to decide when and how their material should be reproduced and/or distributed, regardless of whether their decisions make good business sense." Id. at *63.

[1733] Id. at *66-73.

[1734] Id. at *88,-94.

[1735] Id. at *100.

> especially likely to be the case where the product in question is overwhelmingly used for infringing purposes, and requires little or no specialized training to operate. At a certain point, the inducer can simply continue to distribute the product without any additional active encouragement, recognizing that the marketplace will respond in turn.
>
> Thus, once the market has internalized the inducer's promotion of infringement, the resulting infringements should be attributable to that defendant even though he/she no longer chooses to actively promote that message. … Thus, distribution of a product capable of substantial noninfringing uses, even after the promotion/encouragement of infringement ceases, can by itself constitute inducement.[1736]

In view of these principles, the court concluded that the injunction must impose a filtering obligation on StreamCast because an unfiltered Morpheus system and software would necessarily capitalize on and remain inexorably linked to StreamCast's historical efforts to promote infringement.[1737] The court rejected, however, the plaintiffs proposal that StreamCast be enjoined from distributing Morpheus or another peer-to-peer network unless and until it had demonstrated to the court's satisfaction that it contained "robust and secure means exhaustively to prevent users from using" the system to infringe.[1738] The court noted that there is no filtering system that could "exhaustively" stop every single potential infringement on a peer-to-peer network, and plaintiffs should not, through a standard that stringent, be effectively given the right to prohibit entirely the distribution of a product having substantial noninfringing uses.[1739]

Instead, the court concluded that it would issue a permanent injunction requiring StreamCast to reduce Morpheus' infringing capabilities, while preserving its core noninfringing functionality, as effectively as possible.[1740] "Streamcast's duties will include, but not necessarily be limited to: (1) a filter as part of future Morpheus software distributed to the public; and (2) steps to encourage end-user upgrades from non-filtered software."[1741] The court noted that cost of such filtering, while a relevant criterion if all else were equal, "is not likely a controlling factor, as the injunction will be designed primarily to protect Plaintiffs' copyrights. The mere fact that an adjudicated infringer may have to expend substantial resources to prevent the consummation of further induced infringements is not a central concern."[1742]

Lastly, the court turned to the issue of whether, and to what extent, the injunction should require notice from the plaintiffs of their copyrighted works in order to trigger StreamCast's duty

---

[1736] Id. at *106-08.

[1737] Id. at *110-11.

[1738] Id. at *112.

[1739] Id. at *113-14.

[1740] Id. at *115.

[1741] Id. at *115-16.

[1742] Id. at *117.

to filter those works. The court noted that in the Napster case the Ninth Circuit had imposed notice obligations on the plaintiffs before Napster had a duty to disable access to the offending content on its system.[1743] The court reflected that, although Sony's knowledge prong is completely irrelevant to whether one can be held liable as a vicarious infringer, the Ninth Circuit had nevertheless, by imposing a notice requirement on the plaintiffs, essentially allowed Sony notice concerns "to creep back into the vicarious infringement analysis for purposes of an injunction."[1744] Accordingly, although actual notice of specific infringing files and the failure to remove them is not a prerequisite to inducement liability in the first instance, the Ninth Circuit's Napster ruling informed the court that, like vicarious infringement, notice should be relevant to the injunction against StreamCast.[1745] The court ruled that StreamCast's duty to filter any particular copyrighted work would commence upon the plaintiffs' provision of notice in the form of artist-title pair, a certification of ownership, and some evidence that one or more files containing each work was available on the Morpheus system.[1746]

By order dated Nov. 29, 2007, the court appointed a special master, Andy Johnson-Laird, to assist the court. The court ordered the special master to report on the type of filtering system that should be used (e.g., artist and title matching, hash value digital fingerprinting, and/or acoustical fingerprinting) for the most effectiveness at eliminating the greatest number of infringing works while allowing the core noninfringing uses to continue, and on the most effective way by which StreamCast could encourage current users of legacy software versions to upgrade to a version that possessed the requisite filtering technology.[1747] "The final Report shall include a comprehensive regimen of the actions StreamCast needs to undertake, the forms of filtering necessary, and the methods for implementation of these tools. Such a Report is to include any details of the filtering, such as how StreamCast can adopt keyword filters, common misspellings, and file extensions into filtering technology."[1748]

(7) The Audiogalaxy Case

On May 24, 2002, various record companies, music publishers and songwriters filed a class action lawsuit against the peer-to-peer filing sharing service Audiogalaxy, alleging liability

---

[1743] Id. at *118-19.

[1744] Id. at *120.

[1745] Id. at *121. The court amplified as follows: "One might argue that Napster's notice requirement should not be followed in light of the Supreme Court's Grokster opinion. At one point, the Supreme Court stated that 'Sony did not displace other theories of secondary liability,' and is confined to cases involving 'imputed intent.' It could reasonably be argued, as a result, that Sony occupies a much less central position in the copyright field than was previously understood. Since Sony cannot preclude vicarious and inducement liability, the doctrine could now be viewed as irrelevant to injunctions aimed at preventing such violations. However, this Court will not read this implication into the Supreme Court's ruling, nor hold that Napster has been overruled sub silentio on this question." Id. at *121-22 (citations omitted).

[1746] Id. at *123.

[1747] Order re Appointment of Special Master, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., CV 01-8541 SVW (C.D. Cal. Nov. 29, 2007) at pp. 5-7.

[1748] Id. at p. 7.

for contributory and vicarious copyright infringement for facilitating the copying of digital music files over the Internet. The plaintiffs alleged that the Audiogalaxy service was even worse than the Napster system in facilitating infringement, because the Audiogalaxy service allowed users to download entire record albums, cover art, and software.[1749] Less than one month later, on June 17, 2002, the plaintiffs announced a settlement with Audiogalaxy that required the file sharing service to halt the infringement of copyrighted works on its network and allowed, but did not require, the service to employ a "filter-in" system that would not make music available without the consent of the copyright holder. Audiogalaxy also agreed to pay the plaintiffs a substantial sum in settlement.[1750]

(8) The Hummer Winblad/Bertelsmann Litigation

After Napster filed for bankruptcy, several of the plaintiffs in the Napster litigation brought suit against the venture capital firm Hummer Winblad and the media company Bertelsmann AG, each of which had funded Napster, seeking to hold those defendants secondarily liable for the infringement of the plaintiffs' works committed through the Napster system. The plaintiffs alleged that by investing in Napster and assuming control of the operation of Napster,[1751] the defendants contributorily and vicariously infringed the plaintiffs' rights. In July of 2004, Judge Patel denied summary judgment motions filed by the defendants, ruling that the plaintiffs' allegations that Bertelsmann and Hummer Winblad "exercised essentially full operational control over Napster during periods in which Napster remained a conduit for infringing activity" would, if proved, give rise to liability for contributory and vicarious infringement.[1752]

The defendants subsequently filed motions for summary judgment seeking to limit their liability for copyright infringement to those works that were the subject of notice to Napster, and more narrowly, those works of which Bertelsmann had actual notice, in view of the Ninth Circuit's rulings in Napster I and Napster II, discussed extensively in Section III.C.2(c)(1) above. Judge Patel's opinion of May 2006 denying such motions[1753] afforded her an interesting and detailed opportunity to construe some of the more confusing aspects of the Napster I and Napster II cases, as well as to explicate the effect of the Supreme Court's Grokster decision on the Ninth Circuit's rulings and their applicability to Hummer Winblad's and Bertelsmann's secondary liability.

In moving for summary judgment, the defendants argued that the Ninth Circuit's rulings in Napster I and Napster II limited Napster's liability to those works of which Napster had actual

---

[1749] "Record Labels, Music Publishers, Songwriters Sue Audiogalaxy; Allege It Is Same as Napster," *BNA's Electronic Commerce & Law Report* (June 5, 2002) at 561-62.

[1750] "RIAA, NMPA Reach Settlement With Audiogalaxy," *BNA's Electronic Commerce & Law Report* (June 26, 2002) at 655.

[1751] Hank Berry, a partner at the Hummer Winblad firm, was installed by Hummer Winblad as Napster's CEO shortly after Hummer Winblad made a substantial venture capital investment in Napster.

[1752] UMG Recordings, Inc. v. Bertelsmann AG, 222 F.R.D. 408 (N.D. Cal. 2004).

[1753] In re Napster, Inc. Copyright Litigation, 2006 U.S. Dist. LEXIS 30338 (N.D. Cal. May 17, 2006).

notice and which Napster failed to remove from its system. The Plaintiffs disputed the defendants' reading of Napster I, and also argued that Judge Patel's holding in Fonovisa, Inc. v. Napster, Inc.[1754] and the Supreme Court's Grokster decision firmly established that actual notice is not required. The defendants argued that the ultimate holding of Napster I, however it might have been called into question by the Grokster case, with respect to the degree of Napster's liability was binding in the instant litigation.[1755] To adjudicate the contentions of the plaintiffs and the defendants, Judge Patel revisited the Napster I, Fonovisa v. Napster, and Grokster decisions in detail.

Turning first to the Napster I decision, the court noted that the Ninth Circuit's rulings with respect to the standard of knowledge required – actual versus constructive – were confusing. The Ninth Circuit began its opinion by noting that Napster had both actual and constructive knowledge of direct infringements committed through the Napster system. But then the Ninth Circuit's opinion abruptly shifted when it quoted language from the court's opinion in the Netcom case to the effect that evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement.[1756]

Judge Patel noted that the Ninth Circuit's discussion of the Netcom case was confusing in several respects. First, the Ninth Circuit's opinion stated at least two formulations of the level of knowledge required for infringement, suggesting alternately that actual knowledge was *required* and that it was *sufficient*. Second, the Ninth Circuit's opinion did not explicitly discuss constructive knowledge as an alternate basis for liability. Judge Patel noted, however, that focusing on the Ninth Circuit's own formulations of the legal standard, and not on the quote from the Netcom decision, it would be possible to read the first half of Napster I as upholding Judge Patel's findings on both actual and constructive knowledge and affirming liability on both bases.[1757]

However, Judge Patel noted that the portion of the Ninth Circuit's opinion modifying the scope of her preliminary injunction presented a second discontinuity in reasoning. The Ninth Circuit set forth a three factor test defining the boundary of Napster's contributory liability: Napster could be liable to the extent it (1) received reasonable knowledge of specific infringing files with copyrighted works, (2) knew or should have known that such files were available on the Napster system, and (3) failed to act to prevent viral distribution of the works. The references to "reasonable" knowledge and "should have known" of the availability of infringing files again suggested a constructive knowledge standard.[1758]

Nevertheless, the Ninth Circuit went on to formulate guidelines for the narrowing of the injunction. First, the Ninth Circuit placed the burden on the plaintiffs to provide notice to

---

[1754] 2002 U.S. Dist. LEXIS 4270 (N.D. Cal. Jan. 28, 2002).

[1755] In re Napster, Inc. Copyright Litigation, 2002 U.S. Dist. LEXIS 4270 at *13.

[1756] Id. at *14-16.

[1757] Id. at *19.

[1758] Id. at *19-20.

Napster of copyrighted works and files containing such works available on the Napster system. Second, after plaintiffs provided notice, Napster had the duty to disable access to the offending content, as well as the additional burden of policing the system within the limits of the system (i.e., searching the system for similarly named files). Judge Patel found this section of the Ninth Circuit's opinion to demonstrate the inconsistency in its reasoning. Despite finding that Napster had constructive knowledge based on facts unrelated to specific infringing files, the Ninth Circuit nonetheless in effect limited Napster's liability to those files of which Napster had actual knowledge.[1759]

Judge Patel then summarized her conclusions from the Napster I case as follows:

> Whether or not it is supported by clear reasoning, the Ninth Circuit explicitly stated that Napster must have "reasonable knowledge" of specific infringing works before it could be found liable. Plaintiffs attempt to avoid the consequences of the Ninth Circuit's holding by arguing that the rules used in crafting an injunction are distinct from those used in determining damages. The Ninth Circuit, however, expressly limited Napster's "liability," (i.e., the extent of its infringing conduct), according to the "reasonable knowledge" standard before embarking on a discussion of how the injunction should be modified. Although the actual proposed mechanics of the injunction – notice followed by a duty to remove the files – may be narrower than the outer limits of Napster's liability, there is no doubt that Napster I significantly reduced the scope of Napster's exposure.[1760]

Judge Patel then turned to a discussion of her ruling in the Fonovisa decision, in which Napster, moving to dismiss Fonovisa's complaint, had argued that Napster I added a "notice" requirement for claims of secondary copyright infringement by on-line systems. Judge Patel rejected Napster's arguments in her 2004 decision in Fonovisa, finding that although Napster I set fairly narrow limits on Napster's liability, it studiously avoided any clear reshaping of the doctrine of contributory infringement.[1761]

Judge Patel then observed that her Fonovisa opinion had set forth four points relevant to Hummer Winblad's and Bertelsmann's instant motions for summary judgment. First, liability is not necessarily coextensive with injunctive relief or damages, and the required mental state for Napster's liability remained "reasonable knowledge." Second, the conduct identified by the Napster I court as infringing use – actual notice followed by a failure to correct – was exemplary and not intended to be an exhaustive list. Under the "reasonable knowledge" standard, other methods of proving actual and constructive knowledge were possible, although Napster I admittedly set the bar for reasonable knowledge quite high. Third, it was significant that Fonovisa considered only a motion to dismiss and not the precise scope of liability. To survive a motion to dismiss, a plaintiff need identify only a specific instance of infringement, whereas the

---

[1759] Id. at *20-22.

[1760] Id. at *22-23.

[1761] Id. at *24.

same facts would be inadequate in proving the precise amount of damages. And fourth, Judge Patel had acknowledged in Fonovisa that broader readings of Napster I were possible, but absent a compelling reason to do so, she was unwilling to read more into it than it stated.[1762]

Judge Patel then turned to an analysis of the Grokster decision. She noted that the Ninth Circuit's opinion in Grokster had read Napster I more expansively than she had anticipated in Fonovisa, reading Napster I to mean that if a defendant could show that its product was capable of substantial or commercially significant noninfringing uses, then constructive knowledge of the infringement could not be imputed. Judge Patel noted that the Supreme Court rejected the Ninth Circuit's ruling, and that taken as a whole, the Supreme Court's decision provided for liability under broader circumstances than those permitted under Napster I. She noted that the evidence stressed by the Supreme Court, particularly the defendants' advertising and marketing strategies – was strikingly similar to the evidence supporting her finding of constructive knowledge in shaping her original, more sweeping injunction in the Napster case.[1763]

The defendants argued that the Grokster ruling could not be applied retroactively to the current case to render actionable conduct that conformed to the modified preliminary injunction entered following Napster I, a closed case that was no longer on direct review. Judge Patel rejected this argument, noting that Bertelsmann was a different party than Napster, and the instant action was not the same as the now-closed original Napster lawsuit. Bertelsmann was alleged to be separately liable based on its own control over the operation of the Napster system, even if its liability were factually derivative of the same alleged acts of illegal copying by Napster. Accordingly, the court ruled that the plaintiffs were entitled to pursue recovery under the Grokster theory of liability, which did not require actual or even reasonable knowledge of specific infringing files, as well as under the "reasonable knowledge" standard articulated in Napster I.[1764] Accordingly, she denied the defendants' motion for summary judgment.[1765]

(9) Arista Records v. Lime Group

(For a discussion of contributory liability in this case, see Section III.C.4(d) below.)

(d) The CoStar Case

In CoStar v. Loopnet,[1766] discussed in detail in Section III.C.6(b)(1)(iii) below, the court addressed in some detail the knowledge an OSP must have of infringing activity in order to be liable for contributory infringement. In brief summary, the plaintiff argued that once it gave the OSP notice of specific infringements on its system, the OSP was on notice that ongoing infringements were occurring and had a duty to prevent repeat infringements in the future. The court ruled that the amount of policing for future infringements the OSP would be required to do

---

[1762] Id. at *24-27.

[1763] Id. at *27-30.

[1764] Id. at *31-32.

[1765] Id. at *33.

[1766] 164 F. Supp. 2d 688 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

would depend upon the level of knowledge it possessed and the specificity of that knowledge. The court further held that, to prove its claim for contributory infringement, the plaintiff would have to establish that the notice it gave to the OSP comprised at least constructive knowledge of specific infringing activity which the OSP materially contributed to or induced by its alleged failure to halt the activity. There remained too many material factual disputes for the court to decide on summary judgment either that such a level of knowledge did or did not exist or that the OSP's actions in trying to stop the infringement were or were not insufficient to the point of comprising inducement as a matter of law.

(e) Ellison v. Robertson

In Ellison v. Robertson,[1767] discussed in detail in Section III.C.6(b)(1)(i)b. below, the district court addressed the "reason to know" prong of the knowledge requirement of contributory liability. In that case an individual named Robertson scanned several fictional works written by the plaintiff and posted them onto the Usenet group "alt.binaries.e-book," a group that was used primarily to exchange pirated and unauthorized digital copies of text material, principally works of fiction by famous authors. AOL, acting as a Usenet peer, hosted the infringing materials on its Usenet server for a period of fourteen days. The plaintiff sought to hold AOL liable for direct, vicarious and contributory copyright infringement.[1768]

With respect to contributory infringement, the court found that AOL did not have actual knowledge of the infringement until the lawsuit was filed. Although the plaintiff had attempted to notify AOL of the presence of the infringing works via email to AOL's designated copyright agent as listed in the Copyright Office's records, AOL never received the email because AOL had changed its contact email address from "copyright@aol.com" to "aolcopyright@aol.com" in Fall 1999, but waited until April 2000 to notify the Copyright Office of this change. The district court held that, in view of AOL's failure to explain why it delayed in notifying the Copyright Office of its email address change, as well as why it did not make provision for forwarding to the new address emails sent to the old address, a reasonable trier of fact could find that AOL had reason to know that infringing copies of the plaintiff's works were stored on its Usenet servers.[1769] The Ninth Circuit affirmed this ruling on appeal.[1770]

[1767] 189 F. Supp. 2d 1051 (C.D. Cal. 2002).

[1768] Id. at 1053-54.

[1769] Id. at 1057-58. The court also noted that a trier of fact might conclude that AOL had reason to know of infringement on its system from the fact that another AOL user had called AOL to report a number of infringing books posted on Usenet. The user spoke only to a low-level customer service representative, who advised him to send an email setting forth the details of his complaint. The court stated, "a reasonable trier of fact might conclude that AOL should have transferred Miller to speak with an employee with knowledge of AOL's copyright infringement policies instead of directing him to an email address." Id. at 1058.

[1770] Ellison v. Robertson, 357 F.3d 1072, 1077 (9th Cir. 2004) ("Because there is evidence indicating that AOL changed its e-mail address in an unreasonable manner and that AOL should have been on notice of infringing activity we conclude that a reasonable trier of fact could find that AOL had reason to know of potentially infringing activity occurring within its USENET network.").

With respect to the material contribution prong of contributory infringement, AOL argued that as a matter of law, the mere provision of Usenet access was too attenuated from the infringing activity to constitute a material contribution, citing for support by analogy the provisions of Section 512(m) of the DMCA that an OSP need not monitor its system for infringing activity to qualify for the DMCA safe harbors. The district court rejected this argument, citing the Netcom court's holding that providing a service that allows for the automatic distribution of all Usenet postings can constitute a material contribution when the OSP knows or should know of infringing activity on its system and yet continues to aid in the distribution of the infringing material. Accordingly, the district court ruled that the plaintiff had demonstrated triable issues of fact on contributory infringement by AOL.[1771] The Ninth Circuit also affirmed this ruling on appeal.[1772]

(f) Perfect 10 v. Cybernet Ventures

In Perfect 10, Inc. v. Cybernet Ventures, Inc.,[1773] the defendant Cybernet was the operator of an "age verification service" that enrolled subscribers, after verifying their age as an adult, to a service that would enable them to gain access for a single monthly fee to a large number of member sites displaying pornographic pictures. All fees paid by subscribers went directly to Cybernet, which on a semi-monthly basis then paid each individual member site a commission based on the site where the subscriber originally signed up for his or her membership in Cybernet's service.[1774] Cybernet exercised some control over the content of each of its member sites, requiring that each site contain unique and adequate content, which generally meant at least 30 pictures of sufficient quality to provide value to Cybernet's customers. Cybernet also imposed a zero tolerance child pornography policy on its member sites.[1775] The court found that Cybernet actively reviewed and directed its affiliated webmasters on the appearance and content of their sites.[1776]

The plaintiff, Perfect 10, was the holder of copyright in various photographs of nude women. Perfect 10 claimed to have found more than 10,000 copies of its photographs on approximately 900 websites affiliated with Cybernet.[1777] Perfect 10 sought to hold Cybernet liable for the unauthorized presence of its photographs on Cybernet's member sites.

On a motion for a preliminary injunction, the court ruled that Perfect 10 had established a strong likelihood of success on its claim of contributory copyright infringement. The court found that Cybernet had knowledge of the infringements because a member for the Association for the Protection of Internet Copyright had contacted Cybernet with approximately 2,000 emails

---

[1771] Ellison v. Robertson, 189 F. Supp. 2d 1051, 1058-60 (C.D. Cal. 2002).

[1772] Ellison v. Robertson, 357 F.3d 1072, 1078 (9th Cir. 2004).

[1773] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[1774] Id. at 1159.

[1775] Id. at 1160-61.

[1776] Id. at 1164.

[1777] Id. at 1162.

over the course of three or four years, notifying Cybernet of alleged copyright infringement on its system. In addition, Cybernet's site reviewers reviewed every site before allowing the sites to become members of Cybernet's service, and the court found that there was evidence that many sites contained disclaimers to the effect that the site did not hold copyrights for the works on the site.[1778] Accordingly, the court ruled that there was "a strong likelihood of success in proving general knowledge of copyright infringement prior to Perfect 10's filing of the complaint" as well as "serious questions as to Cybernet's constructive knowledge of infringement of Perfect 10's copyrights prior to the complaint raised by this general knowledge, Cybernet's review of sites containing Perfect 10 images and the likelihood of those sites containing copyright disclaimers. Further, there appears to be little question that Cybernet has been provided with actual notice of a large number of alleged infringements since June 2001."[1779]

Citing the Fonovisa case,[1780] the court also concluded that Cybernet had materially contributed to the infringements by providing technical and content advice to its member sites, reviewing those sites, and attempting to control the quality of the product it presented to subscribers as a unified brand.[1781]

(g) Perfect 10 v. Visa International

In Perfect 10, Inc. v. Visa International Service Ass'n,[1782] Perfect 10, owner of the copyrights in pornographic materials, sought to hold various credit card and banking institutions liable for contributory and vicarious infringement for providing financial services to various web sites that Perfect 10 alleged contained infringing copies of its copyrighted materials. The district court granted the defendants' motion to dismiss.

With respect to contributory liability, the defendants did not contest the issue of their knowledge of infringement, but denied that they materially contributed to the infringement. The district court agreed. Unlike the defendant age verification service in Perfect 10, Inc. v. Cybernet Ventures, Inc.,[1783] which advertised the infringing web sites and paid a commission to a web site whenever someone registered for its services through that particular web site, the court noted that the defendants in the instant case did not promote the web sites that used their services, nor have any content-specific regulations with which merchants must comply before using their services.[1784]

[1778] Id. at 1169.

[1779] Id. at 1170 (emphasis in original).

[1780] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

[1781] Perfect 10, 213 F. Supp. 2d at 1170.

[1782] 71 U.S.P.Q.2d 1914 (N.D. Cal. 2004), aff'd, 494 F.3d 788 (9th Cir. 2007), cert. denied, 2008 U.S. LEXIS 4523 (June 2, 2008).

[1783] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[1784] Perfect 10, Inc. v. Visa International, 71 U.S.P.Q.2d at 1917.

The court rejected Perfect 10's argument that because the defendants provided essential financial services to alleged infringers, they were materially contributing to the infringement. The court noted that the financial services were not essential to the functioning of the allegedly infringing web sites because they could employ intermediate payment services if the defendants terminated their merchant accounts. Furthermore, even if the defendants provided services that materially contributed to the functioning of the web site businesses, there was no factual basis for the allegation that they materially contributed to the alleged *infringing activities* of the web sites. The defendants' ability to process credit cards did not directly assist the allegedly infringing web sites in copying the plaintiffs' works. Accordingly, the court ruled that Perfect 10 had not adequately pled a claim for contributory infringement, although the court granted Perfect 10 leave to amend its complaint to establish a relationship between the financial services provided by the defendants and the alleged infringing activity.[1785]

On appeal, the Ninth Circuit affirmed.[1786] With respect to contributory infringement, the court noted that it need not address the knowledge prong because it found that Perfect 10 had not pled facts sufficient to establish that the defendants induced or materially contributed to the infringing activity.[1787] With respect to material contribution, the court held that merely continuing to process credit card payments to the infringing web sites despite knowledge of ongoing infringement was insufficient contribution for contributory liability because such payment services had no direct connection to the actual infringing activities of reproduction or distribution of the plaintiff's copyrighted material. The defendants' services did not assist users in searching for infringing images, nor provide links to them, nor did infringing materials pass through the defendants' payment systems. Although the payment services made it easier for web sites to profit from the infringing activities, this fact was insufficient for contributory liability because the services did not directly assist in the *distribution* of infringing content to Internet users. The court noted that even if users couldn't pay for images with credit cards, infringement could still continue on a large scale because other viable funding mechanisms were available.[1788]

The court rejected Perfect 10' argument that the defendants' payment services were akin to provision of the site and facilities for infringement analogous to the Fonovisa case. The court noted that the web sites on which the infringing photographs resided were the "site" of the infringement, not the defendants' payment networks. If mere provision of a method of payment could be considered a "facility" of infringement, so too could the provision of computers, of software, and of electricity to the infringing web sites, and such a rule would simply reach too far.[1789]

[1785] Id.

[1786] Perfect 10, Inc. v. Visa International, 2007 U.S. App. LEXIS 15824 (9th Cir. July 3, 2007), cert. denied, 2008 U.S. LEXIS 4523 (June 2, 2008).

[1787] Id. at *10-11.

[1788] Id. at *13-16.

[1789] Id. at *21-24.

With respect to inducement, Perfect 10 argued that the Grokster decision was analogous because the defendants induced customers to use their cards to purchase goods and services, and should therefore be held guilty of specifically inducing infringement if the cards were used to purchase images from sites that had stolen content from Perfect 10. The court rejected this argument as insufficient, noting that Perfect 10 had pled no facts suggesting that the defendants had promoted their payment system as a means to infringe, nor had they promoted the purchase of specific infringing goods. Accordingly, the facts as pled evidenced no clear expression of a specific intent to foster infringement, and thus there could be no liability for inducement.[1790]

The court's rulings with respect to vicarious liability are set forth in Section III.C.3.(g) below.

(h) Parker v. Google

In Parker v. Google,[1791] pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled "29 Reasons Not To Be A Nice Guy." He posted Reason # 6 on USENET. Parker asserted that Google's automatic archiving of this USENET content made Google contributorily liable for copyright infringement because it facilitated users to make unauthorized distributions and copies of his copyrighted material through the "author search" feature on Google's web site. The district court rejected this argument for two reasons. First, Parker failed to allege infringement of a specific copyrighted work in his claim for contributory infringement. And second, he had failed to allege that Google had requisite knowledge of a third party's infringing activity.[1792] On appeal, the Third Circuit affirmed in an unpublished opinion on the ground that Parker had failed to allege that Google had the requisite knowledge of a third party's infringing activity.[1793]

(i) MDY Industries v. Blizzard Entertainment

In MDY Industries v. Blizzard Entertainment,[1794] the defendant distributed bot software called "Glider" that was able to play Blizzard Entertainment's multiplayer online role-playing game known as World of Warcraft (WoW) for its owner while the owner was away from his or her computer, thereby enabling the owner to advance more quickly within WoW than would otherwise be possible. Glider also enabled its user to acquire an inordinate number of game assets, with some users even selling those assets for money in online auction sites. Both the use of bot software to play WoW and the resale of game assets were prohibited by the Terms of Use (TOU) that governed the play of WoW, together with an End User License Agreement (EULA). The EULA and TOU were displayed on a player's computer screen when the game client software was loaded and the player sought online access to Blizzard's game servers. Players

---

[1790] Id. at *26-31.

[1791] 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS 16370 (9th Cir. July 10, 2007).

[1792] Id. at 498-99.

[1793] Parker v. Google, 2007 U.S. App. LEXIS 16370 at *9 (3d Cir. July 10, 2007).

[1794] 2008 U.S. Dist. LEXIS 53988 (D. Ariz. July 14, 2008).

were required to agree to the terms of the EULA and TOU before proceeding to play the game. Blizzard alleged that users of WoW were licensees who were permitted to copy the copyrighted game client software only in conformance with the EULA and TOU, and that when users launched WoW using Glider, they exceeded the license in the EULA and TOU and created infringing copies of the game client software. Blizzard sought to hold the defendant contributorily liable for those infringing copies.[1795]

The district court agreed and granted Blizzard summary judgment against the defendant. Citing the Ninth Circuit's decision in MAI Sys. v. Peak Computer, Inc.,[1796] the court ruled that copying of software to RAM constitutes "copying" for purposes of Section 106 of the Copyright Act, and thus if a person is not authorized by the copyright holder through a license or by law (e.g. Section 117) to copy the software to RAM, the person commits copyright infringement by using the software in an unauthorized way.[1797] The court ruled that the provisions in the EULA and the TOU prohibiting the use of bots and resale of game assets were limitations on the scope of the license, not merely separate contractual covenants. The EULA stated the game client software was distributed solely for use by authorized end users according to the terms of the EULA, and the grant clause in the license was expressly conditioned as being subject to the end user's continuing compliance with the EULA. The license also made clear that, although users were licensed to play WoW and to use the game client software while playing, they were not licensed to exercise other rights of the copyright holder, such as distributing or modifying the software, thus establishing that the provisions of the license were designed to protect Blizzard's copyright interests. Thus, when end users used bot software such as Glider to operate the WoW game client software in violation of the EULA and TOU, they were making unauthorized copies of the game client software, which infringed Blizzard's copyright, and for which the defendant was liable as a copyright infringer.[1798]

The district court rejected the defendant's argument that the copies of the game client software made by end users while operating the Glider software were authorized by Section 117 of the copyright statute. The court noted that MAI and at least two other rulings by the Ninth Circuit had held that licensees of a computer program do not "own" their copy and are therefore not entitled to a Section 117 defense.[1799] In October of 2008, the court awarded Blizzard over $6 million in damages for copyright infringement.[1800]

On appeal, the Ninth Circuit confirmed the district court's ruling that WoW players were licensees, not owners, of their copy of WoW's game client software. Citing the standards for

---

[1795] Id. at *1-11.

[1796] 991 F.2d 511, 518-19 (9th Cir. 1993).

[1797] MDY Industries, 2008 U.S. Dist. LEXIS at *10-11.

[1798] Id. at *12-18

[1799] Id. at *24-28.

[1800] Liz McKenzie, "Warcraft Creator Wins $6M Over Software 'Bot'" (Oct. 1, 2008), available as of Oct. 2, 2008 at http://ip.law360.com/articles/71118.

determining status as a licensee versus an owner in its decision in Vernor v. Autodesk,[1801] the Ninth Circuit noted that Blizzard reserved title in the software, granted players a non-exclusive, limited license, and also imposed transfer restrictions if a player sought to transfer the license and a variety of use restrictions (e.g., for non-commercial entertainment purposes only and no use in cyber cafes and computer gaming centers). Accordingly, WoW players were licensees, not owners, of their copy of the software and therefore did not have rights under Section 117.[1802]

The Ninth Circuit then turned to whether the prohibition on the use of bots and cheats was a contractual covenant or a condition on the license. Section 4(B) of the TOU provided:

> You agree that you will not … (ii) create or use cheats, bots, "mods," and/or hacks, or any other third-party software designed to modify the World of Warcraft experience; or (iii) use any third-part software that intercepts, "mines," or otherwise collects information from or through the Program or Service.[1803]

The court noted that, wherever possible, equity construes ambiguous contract provisions as covenants rather than conditions. The court found that TOU sections 4(B)(ii) and (iii)'s prohibitions against bots and unauthorized third-party software were covenants rather than copyright-enforceable conditions. Nothing in those provisions conditioned Blizzard's grant of a limited license on players' compliance with the restrictions in TOU Section 4(B).[1804]

The court further noted that, although one can be liable for copyright infringement by exceeding the scope of a granted license, the potential for infringement exists only where the licensee's action exceeds the license's scope in a manner that implicates one of the licensor's exclusive statutory copyright rights, such as unlawful reproduction or distribution. Although a Glider user violated the anti-bot covenants with Blizzard, the user did not thereby commit copyright infringement because Glider did not infringe any of Blizzard's exclusive rights. For instance, the use did not alter or copy WoW software.[1805]

> Were we to hold otherwise, Blizzard – or any software copyright holder – could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software

---

[1801] 621 F.3d 1102, 1108-09 (9th Cir. 2010).

[1802] MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 at *12-14 (9th Cir. Feb. 17, 2011).

[1803] Id. at *11.

[1804] Id. at *16-17.

[1805] Id. at *

copyright owners far greater rights than Congress has generally conferred on copyright owners.[1806]

Accordingly, the Ninth Circuit held "that for a licensee's violation of a contract to constitute copyright infringement, there must be a nexus between the condition and the licensor's exclusive rights of copyright."[1807] Here, the WoW players did not commit copyright infringement by using Glider in violation of the TOU. MDY was thus not liable for secondary copyright infringement, because there was no direct infringement on the part of the players.[1808]

(j) Louis Vuitton v. Akanoc Solutions, Inc.

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,[1809] the defendants provided OSP services that hosted websites through which the plaintiff alleged goods were being sold that infringed its trademarks and copyrights. The plaintiff sought to hold the defendants contributorily and vicariously liable for hosting such websites and the defendants moved for summary judgment. The court denied the motion as to contributory infringement, but granted it as to vicarious infringement.[1810] With respect to contributory infringement, the court found issues of material fact concerning whether direct infringements were taking place on websites hosted by the defendants, citing internal emails in which defendants discussed attempts to take down websites selling counterfeit Louis Vuitton products.[1811] The court also found issues of material fact with respect to the defendants' knowledge of infringing activity, rejecting the defendants' argument that they did not have such knowledge because they did not log on to sites to investigate complaints of infringing activity, but rather simply took such sites down. The court found this testimony merely served to highlight that there were issues of material fact concerning actual knowledge on the part of defendants, and in any event, the defendants had not submitted any testimony with respect to whether they should have known of infringing activity in view of numerous letters from the plaintiff alleging such activity.[1812]

Finally, citing the Ninth Circuit's decision in Perfect 10 v. Amazon allowing a finding of material contribution where an OSP fails to take "simple measures" to limit infringement on its site, the court found material issues of fact with respect to whether the defendants could have taken such simple measures based on evidence submitted by the plaintiff that the defendants had

---

[1806] Id. at *20.

[1807] Id. at *21. The court noted, however, special treatment in the case of failure to pay: "A licensee arguably may commit copyright infringement by continuing to use the licensed work while failing to make required payments, even though a failure to make payments otherwise lacks a nexus to the licensor's exclusive statutory rights. We view payment as *sui generis*, however, because of the distinct nexus between payment and all commercial copyright licenses, not just those concerning software." Id. at *22 n.4.

[1808] Id. at *21-22.

[1809] 591 F. Supp. 2d 1098 (N.D. Cal. 2008).

[1810] Id. at 1113. The court's rulings with respect to vicarious infringement are set forth in Section III.C.3(i) below.

[1811] Id. at 1106.

[1812] Id. at 1107-08.

the ability to remove single websites by disabling IP addresses without taking down an entire server. The court noted that the defendants had not submitted any evidence indicating that removing a web site in this fashion would not be a "simple measure" by which they could purge infringing activity using their services.[1813]

A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with respect to the claims and the DMCA defense.[1814] The court denied the defendants' motion as to the contributory copyright claim. With respect to the knowledge requirement, the evidence established that the defendants had ample actual notice of directly infringing activity on dozens of web sites hosted on the defendants' servers in the form of many notice letters from the plaintiff identifying specific web sites that were selling counterfeit goods infringing the plaintiff's copyrights.[1815] With respect to the material contribution requirement, the defendants provided and operated the servers through which the web sites offering the counterfeit goods were hosted, and continued to do so despite receiving notices from the plaintiff of particular web sites engaged in infringing conduct. One of the defendants testified that he rarely used several of the tools at his disposal to punish or deter the operation of the counterfeiting web sites. Thus, there was sufficient evidence to support a finding by the jury of material contribution. [1816]

Accordingly, the court issued a permanent injunction against 'knowingly" hosting infringing web sites in the United States. The order specifically spelled out that the defendants would be deemed to be acting "knowingly" upon proof that (i) they had been served be email or regular mail by the plaintiff with a notice of infringement of specific copyrights on an Internet hosting or routing service operated by the defendants, and (ii) the notice contained screen shot(s) depicting the infringing activity, and (iii) 72 hours after service of the notice the infringing activity was still taking place. The order further stated that the defendants would not be deemed to be acting "knowingly" upon proof that (i) the defendants condition their use of their Internet hosting or routing services, and notify each subscriber and customer accordingly, that their use of such services is subject to immediate termination upon receipt of a notice of infringement that the subscriber or customer is infringing the copyright of Louis Vuitton, and (ii) the defendants publish on their web site complete and accurate contact information for receiving notices of infringement, and (iii) upon receipt of a notice the defendants mailed to the plaintiff an acknowledgment of receipt, and (iv) the defendants assigned a tracking number to the notice, and (v) within 24 hours of receipt of the notice the defendants sent to the subscribe or customer a notice to immediately cease and desist from the activity that is the subject of the notice and failure to do so would result in immediate terminate of services, and (vi) the defendants investigated whether activity did or did not cease within the time period required by the notice

---

[1813] Id. at 1108-09.

[1814] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2010 U.S. Dist. LEXIS 85266 at *1-2 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part, 658 F.3d 936 (9th Cir. 2011).

[1815] Id. at 17.

[1816] Id. at *20.

and upon verifying that it did not cease, the defendants immediately terminated services to the infringing subscriber or customer.[1817]

On appeal, the defendants challenged the jury instructions on contributory infringement as erroneous because they "omitted both the elements of intent and material contribution."[1818] Although the court agreed with the defendants that the jury instructions departed from the Ninth Circuit Model Jury Instructions, it rejected the defendants' challenge, noting that the court had never held that an express finding of intent is necessary to support liability for contributory infringement. Thus, the district court was not required to instruct the jury to make a separate finding that the defendants' knowing action evidenced intent to contribute to copyright infringement. In addition, the court rejected the defendants' argument that the jury instructions should have required an express finding of material contribution. The court noted that material contribution turns on whether the activity in question substantially assists direct infringement, and here, there was no question that providing direct infringers with server space satisfied that standard. Thus, the district court had not erred by narrowing the instruction on material contribution to the only genuine question as to that element – whether the defendants provided the3ir services to direct infringers.[1819]

The court also rejected the defendants' challenge to the court's instructions on willful infringement, on the ground that the instructions erroneously allowed the jury to find that the defendants engaged in willful infringement based solely on a finding of knowing contribution to direct infringement. The defendants claimed that under this formulation, a finding of willfulness required proof of no element beyond those of contributory copyright infringement. The court rejected this argument, noting that a finding of willfulness in the copyright context can be based on either intentional behavior or merely reckless behavior or willful blindness to the copyright holder's rights. The jury instructions were adequate under this standard.[1820]

Finally, the court determined that the jury's award of statutory damages was erroneous. The jury awarded statutory damages of $300,000 per defendant for willful contributory infringement of two of Louis Vuitton's copyrights. The court held that the jury verdict form erroneously invited the jury to specify a separate statutory damages award against *each* defendant.[1821] "Statutory damages reach a maximum based on the number of protected works, not the number of defendants."[1822] Accordingly, the court reversed the statutory damages award

---

[1817] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2010 U.S. Dist. LEXIS 34021 at *4-6 (N.D. Cal. Mar. 19, 2010).

[1818] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936, 943 (9th Cir. 2011).

[1819] Id. at 943-44.

[1820] Id. at 944.

[1821] Id. at 946.

[1822] Id. at 947.

and remanded with instructions that the district court award statutory damages in the total amount of $300,000, for which the defendants would be jointly and severally liable.[1823]

(k) Arista Records v. Usenet.com

In Arista Records LLC. V. Usenet.com, Inc.,[1824] the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on "spool" news servers operated by the defendants.[1825] The court granted the plaintiff record companies' motion for summary judgment on their claim for contributory infringement. With respect to the knowledge prong of contributory liability, unlike the Ninth Circuit in the Napster cases, the court ruled that knowledge of specific infringements on the defendants' service was not required to support a finding of contributory infringement. Rather, it was sufficient that the record established the defendants' employees were clearly aware that their service was used primarily to obtain copyrighted material, users of the service told defendants' technical support employees that they were engaged in copyrighted infringement, and the defendants had targeted the service to former users of Napster and Kazaa.[1826]

The material contribution prong was satisfied because the defendants' servers were the sole instrumentality of their subscribers' infringement. The servers physically stored the content that subscribers requested for download, and the defendants had created designated servers for newsgroups containing MP3 or music binary files so as to maximize the average retention time of those files as compared to other Usenet groups with non-music content. The court rejected the defendants' assertion that they could not be contributorily liable under the Supreme Court's Sony doctrine because their product had substantial noninfringing uses. The court distinguished Sony on the ground that Sony's last meaningful contact with the product or the purchaser was at the point of purchase, after which it had no ongoing relationship with the product or its end user. By contrast, the defendants maintained an ongoing relationship with their infringing users in the course of offering their service, thereby rendering the noninfringing uses immaterial to insulate the defendants from liability. Accordingly, the court granted the plaintiffs' motion for summary judgment on their contributory copyright infringement claim.[1827]

(l) Hermeris v. Brandenburg

In Hermeris v. Brandenburg,[1828] the court issued a ruling that may impliedly broaden an online service provider's duty to police its site for other similar infringing material, at least in a situation where no DMCA safe harbor has been asserted and the material is all owned by related

---

[1823] Id.

[1824] 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

[1825] Id. at 130-31.

[1826] Id. at 154-55.

[1827] Id. at 155-56.

[1828] 2011 U.S. Dist. LEXIS 6682 (D. Kan. Jan. 23, 2011).

defendants. The plaintiff operated an online document preparation web site. The plaintiff sought to hold the defendant OSP contributorily and vicariously liable for hosting three web sites, all of which were owned by apparently related defendants, that were allegedly infringing of the plaintiff's copyrights in its own web site. The plaintiff gave the OSP direct notice that the first of the three web sites was infringing, then sought to hold the OSP secondarily liable for failure to take down the second and third web sites, which the plaintiff alleged were substantially similar to the first web site. The OSP filed a motion to dismiss.[1829]

The court denied the motion with respect to contributory liability because, assuming the facts pled in the complaint were true, the OSP had constructive knowledge of infringement by virtue of the fact that it had received actual knowledge of infringement by the first web site and the fact that the second and third web sites were substantially similar to the first web site.[1830] "Given these factual allegations and viewing the facts in the light most favorable to plaintiff, it is reasonable to infer that [the OSP] should have known that the Second and Third Websites directly infringed upon plaintiff's copyright."[1831] Although the court does not say, its ruling that the actual notice of infringement by the first web site gave the OSP constructive knowledge of infringement by the second and third web sites may have been influenced by the fact that all three web sites were owned by the same defendants and were all substantially similar to each other. If so, then the court's ruling may not necessarily imply a more general holding that actual notice of one infringement gives a defendant OSP constructive notice as to all other substantially similar material on its site for purposes of contributory liability. In any event, having found sufficient knowledge for purposes of contributory liability, the court found an adequate allegation of material contribution to infringement in the form of failure to purge the web sites from the OSP's system.[1832]

The court also ruled that the plaintiff had adequately pled a claim for vicarious infringement because it had pled that the OSP hosted the infringing web sites, and the court found it reasonable to assume that, as the host, the OSP had the right and ability to stop or limited the defendants from displaying or distributing the allegedly infringing materials. The court rejected the OSP's argument that it did not have control over the second and third web sites because it did not have actual knowledge of them. The court found it sufficient for purposes of the control prong that the plaintiff had pled the OSP had constructive knowledge of the second and third web sites.[1833] This ruling seems to imply that, at least in an Internet context (as opposed to a dance hall, for example), some form of knowledge of infringing activity is required before a defendant can be said to have control over it.

The court's opinion makes no mention of the OSP asserting any safe harbor defense under Section 512.

[1829] Id. at *4-6.

[1830] Id. at *10.

[1831] Id.

[1832] Id. at *11.

[1833] Id. at *12-13.

(m) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b). The court denied the defendants' motion to dismiss the plaintiff's claim for contributory infringement. With respect to the knowledge requirement, the court assumed for its discussion that to allege knowledge for common law liability, a plaintiff must allege something more than the defendants' receipt of its seven DMCA notices. Here the DMCA notices identified both specific infringing files and specific repeat infringers. In addition, although the plaintiff did not allege that the defendants failed to remove the infringing material from myVidster, it did allege that the defendants failed to take any action to stop, reprimand, or ban the repeat infringers listed in the DMCA notices and that the defendants failed to implement filters or identifiers to prevent repeated infringing conduct.[1834] "Because plaintiff alleges not just the receipt of DMCA notices but also that after having received the notices defendants failed to act to prevent future similar infringing conduct, it has sufficiently alleged the knowledge element of contributory copyright infringement."[1835] The court found a sufficient material contribution alleged in the allegations that defendants provided a web site that stored infringing material, allowed backup copies to be made, encouraged sharing, had no filters or identifiers in place to prevent repeat infringers, and took no action to stop or ban the repeat infringers who allegedly posted the plaintiff's copyrighted works.[1836]

In a subsequent opinion, the court ruled that the plaintiff was entitled to a preliminary injunction, finding the defendant liable for contributory infringement for essentially the same reasons articulated in the first opinion.[1837] In its opinion, the court commented on the provisions of a proposed injunction submitted by the plaintiff. The plaintiff had proposed that myVidster be required to implement digital fingerprinting on its site, but the court noted that the plaintiff had presented no evidence of what constituted "digital fingerprinting" or whether its implementation would be reasonably feasible or affordable. Accordingly, the court said it would decline to order that the defendants implement that technology. However, the court agreed that it would include in the injunction an obligation to filter based on a list of keywords and tags to prevent the upload or download of, posting of links to videos, and the posting of embedded videos containing the plaintiff's copyrighted content, including intentional or inadvertent misspellings of the keywords and tags. The injunction would also require the defendants to disable the accounts of users who on two or more occasions had posted content that infringed one or more of the plaintiff's copyrights.[1838]

On appeal, the Seventh Circuit (per Judge Posner) vacated the preliminary injunction in a rather confusing opinion. The court first adopted the Second Circuit's succinct definition of

---

[1834] Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *11-12 (N.D. Ill. May 10, 2011).

[1835] Id. at *12.

[1836] Id. at *12-13.

[1837] Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 82955 at *20-29 (N.D. Ill. July 27, 2011). The court also ruled that the defendants were not entitled to a DMCA safe harbor. See Section III.C.6(b)(iii).r below.

[1838] Id. at *34-35.

contributory infringement as "personal conduct that encourages or assists the infringement."[1839] The court then considered two potential infringing acts of myVidster users to which myVidster might be a contributory infringer – the uploading of infringing copies of Flava's videos and the public performance of those videos when viewed by myVidster users. The court held that myVidster could not be a contributory infringer to any unauthorized acts of uploading of infringing copies of Flava's videos because there was no evidence that myVidster was encouraging such acts, and merely providing a connection to websites that contained illegal copies of Flava's copyrighted videos was insufficient encouragement for contributory liability.[1840] "myVidster displays names and addresses (that's what the thumbnails are, in effect) of videos hosted elsewhere on the Internet that may or may not be copyrighted. Someone who uses one of those addresses to bypass Flava's pay wall and watch a copyrighted video for free is no more a copyright infringer than if he had snuck into a movie theater and watched a copyrighted movie without buying a ticket. The facilitator of conduct that doesn't infringe copyright is not a contributory infringer."[1841]

The court then turned to whether myVidster could be a contributory infringer to unauthorized public performances of Flava's videos. With no direct analysis of the statutory definition of "public performance," Judge Posner posited two different interpretations of what constitutes a public performance under the transmit clause of the definition. The first interpretation, which he labeled "performance by uploading," is that "uploading plus bookmarking a video is a public performance because it enables a visitor to the website to receive (watch) the performance at will, and the fact that he will be watching it at a different time or in a different place from the other viewers does not affect its 'publicness,' as the statute makes clear."[1842] myVidster could have no contributory liability under this interpretation because there was no evidence that myVidster was contributing to the decision of users to upload a Flava video to the Internet where it then became available to be bookmarked on myVidster's web site.[1843]

The second interpretation, which Judge Posner labeled "performance by receiving," is that "the performance occurs only when the work (Flava's video) is transmitted to the viewer's computer – in other words when it is 'communicated to the public in a form in which the public can visually or aurally comprehend the work.'"[1844] The court noted that under this interpretation, there was an argument that even though the video uploader was responsible for the transmitting, not myVidster, myVidster was assisting the transmission by providing the link between the uploader and the viewer, and was thus facilitating public performance. However, Judge Posner ultimately rejected such an argument by virtue of distinctions from previous Seventh Circuit authority in the Fonovisa and Aimster cases.

[1839] Flava Works, Inc. v. Gunter, 2012 U.S. App. LEXIS 15977 at *10 (7th Cir. Aug. 2, 2012) (quoting Matthew Bender & Co. v. West Publishing Co., 158 F.3d 693, 706 (2d Cir. 1998).

[1840] Flava Works, 2012 U.S. App. LEXIS 15977 at *10-13.

[1841] Id. at *11.

[1842] Id. at *19.

[1843] Id. at *20-21.

[1844] Id. at *19 (quoting William F. Patry, Patry on Copyright § 14:21, p. 14-41 (2012)).

Specifically, Judge Posner distinguished the present case from the "swap meet" operated by the defendant in the Fonovisa case,[1845] in which pirated copies of musical recordings were being bought and sold. The court noted that Flava's pirated videos were not sold, and there wasn't even admissible evidence that they were actually being accessed via myVidster, rather than via other websites. myVidster was not encouraging the uploading of Flava videos because it had some financial incentive to encourage performance of those works, as the swap meet did.[1846] Judge Posner also distinguished the Aimster case,[1847] in which Aimster created the online equivalent of a swap meet by supplying the software that enabled the file-sharing of copyrighted recordings over the Internet. Unlike Aimster, myVidster was not encouraging swapping, which in turn would encourage infringement.[1848]

Accordingly, the court concluded that on the record compiled to that point there was no basis for the grant of a preliminary injunction on the grounds of secondary infringement. Judge Posner noted, however, that Flava should be entitled to an injunction against myVidster's backup service, in which it made copies of videos that some of its subscribers had posted, including videos copyrighted by Flava (although myVidster had stopped offering that service), because the service constituted direct infringement on myVidster's part. But the preliminary injunction issued by the district court did not enjoin the backup service because Flava didn't make a claim for direct infringement a basis for its motion for preliminary relief. Judge Posner noted that such an injunction might be something for consideration on remand.[1849]

(n) Summary

An OSP, BBS operator or other operator of an online service can be liable for contributory infringement where the operator has sufficient knowledge of infringing activity. The level of knowledge required is not consistent among the cases and is confusingly explicated in some of them, particularly the Ninth Circuit's rulings in the Napster cases. The Ellison and Perfect 10 v. Cybernet Ventures cases seem to hold that constructive knowledge, or reason to know of infringement, may be sufficient for contributory liability. However, the Ninth Circuit's Napster cases seem to adopt a standard of "reasonable knowledge," as Judge Patel's extensive analysis of those cases concludes in her opinion in the Hummer Winblad case, discussed in Section III.C.2(c)(7) above. As Judge Patel concluded, the precise scope of this standard of "reasonable knowledge" is not clear, but it seems to be narrower than the "reason to know" standard of constructive knowledge used in the Ellison and Perfect 10 v. Cybernet Ventures cases.

To add to the confusion, under the Ninth Circuit's Grokster decision, where contributory liability is alleged based on the distribution of a product or service used to infringe, the level of

---

[1845] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

[1846] Flava Works, 2012 U.S. App. LEXIS at *22-23.

[1847] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[1848] Flava Works, 2012 U.S. App. LEXIS at *23-24.

[1849] Id. at *24-26.

knowledge required for contributory liability varies with whether the product or service of the defendant has substantial noninfringing uses. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue is capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement. The Ninth Circuit's Grokster decision interpreted the Napster I decision as requiring actual knowledge of specific infringing acts at a time during which the OSP materially contributes to the infringement in order for there to be contributory liability for such acts. However, the Supreme Court's Grokster decision found that the Ninth Circuit erred in the latter ruling, so it is unclear how much of the Ninth Circuit's adjudication of the knowledge requirement for contributory liability survives the Supreme Court's Grokster ruling. In her analysis of this issue in her opinion in the Hummer Winblad case, Judge Patel was able to conclude only that the Supreme Court's rejection of the Ninth Circuit's ruling suggests that, taken as a whole, the Supreme Court's decision provided for liability under broader circumstances than those permitted under Napster I, but the precise scope of that liability remains unclear.

Beyond knowledge, how much the operator must contribute to the infringing activity after gaining such knowledge beyond the mere provision of the facilities used to accomplish the infringement is also unclear. The Ninth Circuit's interpretation in the Napster I case of its Fonovisa decision seems to require little more than continuing to provide such facilities after knowledge that infringing activity is taking place. The MAPHIA, CoStar and Ellison courts interpreted the Netcom decision to require more (note that, although the Netcom case was decided before both Fonovisa and Napster I, the CoStar and Ellison cases were decided after Fonovisa and Napster I).

As discussed in detail above, the Ninth Circuit's Napster I decision contains a number of ambiguities with respect to the scope of the duty to police for occurrences of infringing material upon receipt of such knowledge. However, the cases seem to require at least that a service provider actively attempt to verify a claim of infringement after receiving notice of the same and to take appropriate action in response. In addition, several decisions have imposed contributory liability on the part of a BBS where the BBS operator actively encouraged the acts leading to the infringements. See the discussions of the Sabella case[1850] and the Hardenburgh case[1851] above.

As discussed in Section III.C.6(b) below, the DMCA defines certain safe harbors against liability for OSPs who act as merely passive conduits for infringing information and without knowledge of the infringement. These safe harbors may provide a defense against liability in certain instances to claims of contributory liability.

[1850] Sega Enterprises Ltd. v. Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

[1851] Playboy Enterprises, Inc. v. Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997).

3. Vicarious Liability

A party may be vicariously liable for the infringing acts of another if it (1) has the right and ability to control the infringer's acts and (2) receives a direct financial benefit from the infringement.[1852] Unlike contributory infringement, knowledge is not an element of vicarious liability.[1853]

(a) The Netcom Case and its Progeny

In the Netcom case, the court refused to impose liability on Netcom under a theory of vicarious liability. The court found that there was a genuine issue of material fact as to whether Netcom had the right and ability to control the activities of its subscribers, in view of the fact that Netcom's expert testified that with an easy software modification Netcom could identify postings containing particular words or from particular individuals, and Netcom had acted to suspend subscribers' accounts on over one thousand occasions.[1854]

However, the court held that the second prong of the test was not satisfied, because there was no evidence that Netcom received a direct financial benefit from the infringing postings, or that such postings enhanced the value of Netcom's services to subscribers or attracted new subscribers.[1855]

In refusing to impose vicarious liability because it found Netcom received no direct financial benefit from the infringing postings, the court in Netcom relied on the district court's decision in Fonovisa, Inc. v. Cherry Auction, Inc.,[1856] which found no direct financial benefit despite an argument that lessees at a swap meet included many vendors selling counterfeit goods and that clientele sought "bargain basement prices."[1857] It should be noted that the Ninth Circuit subsequently reversed Fonovisa, and appears to have adopted a less demanding standard for financial benefit for purposes of vicarious liability, which may undermine the strength of the Netcom decision as precedent on this point. The Ninth Circuit held that adequate financial benefit was alleged by virtue of the fact that the operator of the swap meet received financial benefits through admission fees, parking fees, and sales at concession stands.[1858] A copyright

---

[1852] E.g., Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963).

[1853] Religious Technology Center v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995); R. Nimmer, Information Law ¶ 4.11, at 4-40 (2001).

[1854] Religious Technology Center v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1376 (N.D. Cal. 1995).

[1855] Id. at 1377. The plaintiffs argued that the financial benefit prong was satisfied based on "Netcom's advertisements that, compared to competitors like CompuServe and America Online, Netcom provides easy, regulation-free Internet access. Plaintiffs assert that Netcom's policy attracts copyright infringers to its system, resulting in a direct financial benefit. The court is not convinced that such an argument, if true, would constitute a direct financial benefit to Netcom from *Erlich's* infringing activities." Id. (emphasis in original).

[1856] 847 F. Supp. 1492 (E.D. Cal. 1994).

[1857] Id. at 1496.

[1858] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

holder seeking to hold an OSP or BBS operator vicariously liable might argue under Fonovisa that the subscription fees paid by the infringers should be sufficient financial benefit, just as were the admission fees, parking fees, and concession stand sales in Fonovisa. In addition, as discussed above, in the Napster case, the Ninth Circuit ruled that Napster had received a financial benefit because the presence of infringing material on the Napster system acted as a draw for users.

The Ninth Circuit's holdings in both Fonovisa and Napster suggest a standard that does not require direct financial benefit from the infringing activity itself, but rather that the infringing activity contributes to an overall commercial design and benefit for the operator.[1859]

In one decision handed down after both the Netcom and Fonovisa decisions, Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,[1860] the court, citing the Netcom case, refused to hold vicariously liable an OSP supplying Internet service to a website that contained infringing material because the infringements that occurred through the website did not directly financially benefit the OSP. The website owner paid the OSP a flat quarterly subscription fee that did not change based upon how many people visited the website or what was accessed on such site.[1861]

(b) The Napster Cases

(For a discussion of vicarious liability in the Napster cases, see Section III.C.2.(c)(1) above.)

(c) Ellison v. Robertson

(For a discussion of vicarious liability in the case of Ellison v. Robertson, see Section III.C.6(b)(1)(i) below.)

(d) Perfect 10 v. Cybernet Ventures

The facts of the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.[1862] are set forth in Section III.C.2(f) above. In that case, the court found, on a motion for a preliminary injunction, that the plaintiff had established a strong likelihood of success on its claim of vicarious liability. The court ruled that the defendant Cybernet had a direct financial interest in the infringing activities of its member sites because Cybernet benefited from such sites to the extent they acted as a draw for new subscribers to Cybernet's service. The court further noted that the relationship between Cybernet and its member sites was so close that it appeared to Cybernet's subscribers as if the Cybernet service constituted a single brand. In addition, subscribers paid all the money for

---

[1859] R. Nimmer, Information Law ¶ 4.13[2], at 4-49 (2001).

[1860] 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

[1861] Id. at 1245.

[1862] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

their subscription fees directly to Cybernet, which then apportioned it to the member sites as commissions.[1863]

With respect to the control prong, the court found that Cybernet had the ability to control its member sites. Cybernet had a monitoring program in place under which its member sites received detailed instructions regarding issues of layout, appearance and content. Cybernet monitored images on the sites to make sure that celebrity images did not over-saturate the content found within the sites making up Cybernet's service. Cybernet also forbade its members sites to display certain types of images. Accordingly, the court concluded that Cybernet had sufficient control over the infringing activity to be vicariously liable.[1864]

(e) The Aimster/Madster Lawsuits

The facts of the case of Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, the district court found, on a motion for a preliminary injunction, that the plaintiffs had established a reasonable likelihood of success on their claim of vicarious liability. The court ruled that Aimster had the right and ability to supervise its users merely because it retained the right under its Terms of Service to terminate service to individual users who were repeat violators of copyright law – as required by the DMCA safe harbors, thereby raising the Catch 22 discussed in Section III.C.2(c)(1).10 above in connection with the Napster case, which Catch 22 led the courts in the Hendrickson v. eBay, CoStar, and Perfect 10 v. Cybernet Ventures cases to reject this interpretation (see Sections III.C.6(b)(1)(iii).b, c & d below). In addition, Aimster controlled access of its users by requiring them to log on after paying their monthly fee to join Club Aimster. The court rejected the argument that the encryption on the Aimster system effectively prevented Aimster from controlling the activity of its users, ruling that Aimster need not, as a matter of law, have the physical Internet address of its users in order to be deemed to have sufficient right and ability to control them.[1865] "The fact that users must log in to the system in order to use it demonstrates that Defendants know full well who their users are."[1866]

The district court also concluded that the defendants had a direct financial interest in the infringing activities of Aimster users, because each Club Aimster user was required to pay $4.95 per month to use the service, and there was evidence that every Aimster was now required to pay the fee. In addition, citing Napster II, the court ruled that the financial benefit element was satisfied because the existence of infringing activities acted as a draw for potential customers to the system.[1867]

On appeal, the Seventh Circuit stated that it was "less confident" than the district judge was that the plaintiffs were likely to prevail on the vicarious infringement theory.[1868] Judge

---

[1863] Id. at 1171-72.

[1864] Id. at 1173.

[1865] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 654-55 (N.D. Ill. 2002).

[1866] Id. at 655.

[1867] Id.

[1868] In re Aimster Copyright Litigation, 334 F.3d 643, 654 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

Posner noted that vicarious liability could conceivably have been applied in the Sony case given that the Court treated vicarious and contributory infringement interchangeably, and Sony could have made a design change in its product that would have controlled its users' ability to fast forward through commercials, which Judge Posner found to be the creation of infringing derivative works.[1869] However, he concluded that the court need not reach the issue because Aimster's "ostrich-like refusal" to eliminate the encryption feature in its system and "discover the extent to which its system was being used to infringe copyright" made it a contributory infringer, and that was a sufficient basis to affirm the grant of the preliminary injunction without reaching the vicarious liability issue.[1870]

(f) The StreamCast/Kazaa/Grokster Lawsuits

The facts of the case of StreamCast/Kazaa/Grokster lawsuits are set forth in Section III.C.2(c)(4) above. In that case, the court granted summary judgment to the defendants StreamCast and Grokster on the plaintiff's claim for vicarious liability. With respect to the financial benefit prong, the court ruled that both defendants derived a financial benefit from the infringing conduct of the users of their software, since the ability to trade copyrighted songs and other copyrighted works acted as a "draw" for many users of the software. The defendants also derived substantial revenue from advertising displayed through the software.[1871]

With respect to the control prong, the court distinguished the Napster system, in which centralized search indices and mandatory registration system gave Napster both knowledge of what was being exchanged and the ability to police those exchanges. By contrast, the court found no evidence before it that the defendants had the ability to supervise and control the infringing conduct, all of which occurred after the product had passed to end-users.[1872]

The plaintiffs argued that the defendants' software could have been altered to prevent users from sharing copyrighted files and the court should require such alterations, as the Ninth Circuit required Napster to do. The plaintiffs noted that the defendants' software already included optional screens for pornographic/obscene file names and that it could just as easily screen out copyrighted song titles. The plaintiffs also argued that an effective "meta data" screen could be implemented, as well as emerging "digital fingerprinting" technology.[1873] In a significant holding, the court rejected these arguments, stating that "whether these safeguards are practicable is immaterial to this analysis, as the obligation to 'police' arises only where a defendant has the 'right and ability' to supervise the infringing conduct."[1874] Unlike Napster, whose client software was an essential component of the integrated Napster system, the defendants provided software that communicated across networks entirely outside defendants'

[1869] Id. at 647, 654.

[1870] Id. at 654-55.

[1871] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1043-44 (C.D. Cal. 2003).

[1872] Id. at 1044-45.

[1873] Id. at 1045.

[1874] Id. (emphasis in original).

control.[1875] "The doctrine of vicarious infringement does not contemplate liability based upon the fact that a product could be made such that it is less susceptible to unlawful use, where no control over the user of the product exists."[1876] Accordingly, the court granted the defendants summary judgment on the issue of vicarious liability.

On appeal, the Ninth Circuit affirmed.[1877] The Ninth Circuit began by observing that it had held in the first appeal of the Napster case that the Sony doctrine has no application to vicarious infringement because vicarious liability was not before the Supreme Court in that case. Noting further that the issue of direct financial benefit, via advertising revenue, was undisputed, the court turned its analysis to the prong of right and ability to supervise the infringers.[1878]

Noting that the Napster case had found especially important the fact that Napster had an express policy reserving the right to block infringers' access to its system, the court contrasted the instant case in which there was no evidence in the record to establish that either of the defendants had the ability to block access to individual users. Although Grokster nominally reserved the right to terminate access, StreamCast did not maintain a licensing agreement with persons who downloaded Morpheus. Given the lack of a registration and log-in process, however, even Grokster had no ability to actually terminate access to filesharing functions, absent a mandatory software upgrade to all users that the particular user refused, or IP address-blocking attempts (which would not be effective against most users who were utilizing dynamic IP addresses). The court also noted that none of the communication between the defendants and users provided a point of access for filtering or searching for infringing files, since infringing material and index information did not pass through the defendants' computers.[1879]

In the case of StreamCast, shutting down its XML file altogether would not prevent anyone from using the Gnutella network. In the case of Grokster, its licensing agreement with Kazaa/Sharman did not give it the ability to mandate that root nodes be shut down. In any event, the court noted that any alleged ability to shut down operations altogether would be more akin to the ability to close down an entire swap meet than the ability to exclude individual participants or to police aisles. The Ninth Circuit noted that the district court had correctly characterized the copyright owners' evidence of the right and ability to supervise as little more than a contention that the software itself could be altered to prevent users from sharing copyrighted files.[1880]

> In arguing that this ability constitutes evidence of the right and ability to supervise, the Copyright Owners confuse the right and ability to supervise with the strong duty imposed on entities that have already been determined to be liable for vicarious copyright infringement; such entities have an obligation to exercise

---

[1875] Id.

[1876] Id. at 1045-46.

[1877] Metro-Goldwyn-Mayer v. Grokster, 380 F.3d 1154 (9th 2004).

[1878] Id. at 1164.

[1879] Id. at 1165.

[1880] Id. at 1165-66.

> their policing powers to the fullest extent, which in Napster's case included implementation of new filtering mechanisms. … But the potential duty a district court may place on a vicariously liable defendant is not the same as the "ability" contemplated by the "right and ability to supervise" test. … We agree with the district court that possibilities for upgrading software located on another person's computer are irrelevant to determining whether vicarious liability exists.[1881]

Accordingly, the court affirmed summary judgment for the defendants on the vicarious liability claim.[1882]

(g) Perfect 10 v. Visa International

In Perfect 10, Inc. v. Visa International Service Ass'n,[1883] Perfect 10, owner of the copyrights in pornographic materials, sought to hold various credit card and banking institutions liable for contributory and vicarious infringement for providing financial services to various web sites that Perfect 10 alleged contained infringing copies of its copyrighted materials. The district court granted the defendants' motion to dismiss.

Perfect 10 argued that the defendants had the right and ability to control the infringing activities because (i) provision of financial services was essential to the survival of the allegedly infringing web sites, and the defendants could therefore dictate content by threatening to revoke their services if the web sites did not comply with their standards, and (ii) the defendants had in place internal regulations governing the provision of service to high-risk merchants, including adult entertainment web sites. The district court rejected both arguments. As to the first, the court noted that the record established the allegedly infringing web sites would be able to continue their alleged infringing conduct regardless of whether the defendants blacklisted them. As to the second, even if the defendants had internal regulations requiring monitoring of web sites, the web sites were not bound by such regulations and the defendants had no contractual right to dictate the web sites' content or to take action against them in the event of infringing activity. And unlike the Fonovisa swap meet case, the defendants could not "eject" the web sites from the Internet. Accordingly, the district court ruled that the defendants had no way to control the infringing conduct of the web sites.[1884]

The court noted that the complaint included facts that might indicate a financial benefit to the defendants as a result of the draw from the alleged infringing images, but because of the absence of a right or ability to exercise control over the alleged infringing activity, the existence

---

[1881] Id. at 1166. The plaintiffs also argued that Grokster and StreamCast should not be able to escape vicarious liability by turning a "blind eye" to the detectable infringement of their users. The Ninth Circuit rejected this argument, stating that there is no separate "blind eye" theory or element of vicarious liability that exists independently of the traditional elements of liability. Id.

[1882] Id. at 1167. On appeal, the Supreme Court did not reach the issue of vicarious liability in view of its resolution of the case under the doctrine of inducement.

[1883] 71 U.S.P.Q.2d 1914 (N.D. Cal. 2004), aff'd, 2007 U.S. App. LEXIS 15824 (9th Cir. July 3, 2007), cert. denied, 2008 U.S. LEXIS 4523 (June 2, 2008).

[1884] Id. at 1918.

of a financial benefit would not be sufficient to establish vicarious liability. Accordingly, the district court granted the defendants' motion to dismiss the claim with leave to Perfect 10 to amend.[1885]

On appeal, the Ninth Circuit affirmed.[1886] The Ninth Circuit agreed with the district court that the rules and regulations of the defendants prohibiting member banks from providing services to merchants engaging in certain illegal activities and requiring member banks to investigate merchants suspected of engaging in such illegal activities were insufficient to establish the right and ability to control infringing activity for purposes of vicarious liability. The court noted that the defendants did not have any ability to directly control the infringing activity occurring on the web sites at issue, and the court held that the mere ability to withdraw a financial carrot did not constitute the right and ability to control infringing activity that vicarious infringement requires.[1887]

The court rejected Perfect 10's analogy to the Napster case on the ground that the defendants, like Napster, had the ability to policy their systems and failed to exercise that right to prevent the exchange of copyrighted material. The court noted that Napster's policing power was much more intimate and directly intertwined with the infringing activity than the defendants' payment systems. Napster could block users' access to its system and thereby deprive particular users of use of its location and distribution tools. By contrast, although the defendants could block access to their payment system, they could not themselves block access to the Internet, to any particular web sites, or to search engines enabling the location of such web sites. Nor could the defendants take away the tools the offending web sites used to reproduce, alter, and distribute the infringing images over the Internet.[1888]

Finally, the court rejected Perfect 10's argument that the defendants' rules and regulations imposed on merchant banks gave them contractual control over the content of their merchants' web sites sufficient for vicarious liability. The court held that the ability to exert financial pressure did not give the defendants the right or ability to control the actual infringing activity taking place on the web sites. The court found the defendants analogous to Google, which was held not liable in the Perfect 10 v. Amazon case for vicarious infringement even though search engines could effectively cause a web site to disappear by removing it from their search results, and reserved the right to do so.[1889] In sum, although the infringing activities at issue might not be profitable without access to the defendants' credit card payment systems, the court held that the "alleged infringement does not turn on the payment; it turns on the reproduction, alteration and distribution of the images, which Defendants do not do, and which occurs over networks Defendants do not control."[1890] Accordingly, because Perfect 10 had failed

---

[1885] Id.

[1886] Perfect 10, Inc. v. Visa International, 2007 U.S. App. LEXIS 15824 (9th Cir. July 3, 2007), cert. denied, 2008 U.S. LEXIS 4523 (June 2, 2008).

[1887] Id. at *33-35.

[1888] Id. at *35-37.

[1889] Id. at *38-39.

[1890] Id. at *43.

to establish the control prong, it had not pled a viable claim of vicarious liability, and the court ruled that it need not reach the issue of direct financial interest.[1891]

The Ninth Circuit's rulings were clearly heavily influenced by policy considerations and a belief that to hold tertiary financial service providers secondarily liable for infringing activities on web sites for which they processed payments would simply go too far. Indeed, the court began its analysis of the secondary liability issues with the following:

> We evaluate Perfect 10's claims with an awareness that credit cards serve as the primary engine of electronic commerce and that Congress has determined it to be the "policy of the United States – (1) to promote the continued development of the Internet and other interactive computer services and other interactive media [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[1892]

(h) Parker v. Google

In Parker v. Google,[1893] pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled "29 Reasons Not To Be A Nice Guy." He posted Reason # 6 on USENET. Parker asserted that Google's automatic archiving of this USENET content made Google vicariously liable for copyright infringement because it facilitated users to make unauthorized distributions and copies of his copyrighted material through Google's web site, and Google had the right and ability to supervise or control such user activity and received a substantial financial benefit from it in the form of advertising revenue and goodwill. The district court rejected this argument for two reasons. First, Parker had failed to allege infringement of any specific registered works that were infringed, nor had he alleged specific conduct by a third party that Google may have had the right and ability to supervise. Second, his broad allegations that Google's advertising revenue was directly related to the number of Google users was insufficient to maintain a claim of vicarious liability, as it did not allege any actual relationship between infringing activity and the number of users that would demonstrate an obvious and direct financial interest in infringing activity.[1894] On appeal, the Third Circuit affirmed in an unpublished decision for the reasons articulated by the district court.[1895]

(i) Louis Vuitton v. Akanoc Solutions

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,[1896] the defendants provided OSP services that hosted websites through which the plaintiff alleged goods were being sold that

---

[1891] Id. at *45.

[1892] Id. at *7 (quoting 47 U.S.C §§ 230(b)(1), (2)).

[1893] 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

[1894] Id. at 499-500.

[1895] Parker v. Google, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

[1896] 591 F. Supp. 2d 109 (N.D. Cal. 2008).

infringed its trademarks and copyrights. The plaintiff sought to hold the defendants contributorily and vicariously liable for hosting such websites and the defendants moved for summary judgment. The court denied the motion as to contributory infringement, but granted it as to vicarious infringement.[1897] With respect to vicarious liability, the plaintiff argued that the ability to infringe without strict policing by the defendants acted as a draw to the site, in conjunction with the defendants' Chinese language skills and competitive technology. The court rejected this argument, noting that the plaintiff had provided no evidence that any of the defendants' customers used their services because of the ability to infringe.[1898] The court also found that the plaintiff had not established a showing of direct financial benefit from infringing activity. "Plaintiff does not offer any evidence showing that Defendants made more money when they allowed infringement to continue or less money when they did not. Nor does Plaintiff offer any evidence showing that customers sought or abandoned Defendants' services based on their ability to infringe. Furthermore, Plaintiff concedes that Defendants have 'unplugged' infringers in the past. By doing so, Plaintiff undermines its own contention that Defendants turn a blind eye to the infringing activity occurring on their servers."[1899]

(j) Live Face on Web v. Howard Stern Productions

In Live Face on Web, LLC v. Howard Stern Productions, Inc.,[1900] the plaintiff alleged that the defendant had infringed its copyright in proprietary software that allowed a company to display a "live" salesperson or spokesperson superimposed on the company's web site. The plaintiff's allegations that the unauthorized presentations on the defendant's web site were designed to and did draw and prolong visitors' attention to the web site and to other Howard Stern media promoted on the web site, that the presentations increased the amount of time users would spend on the web site, and that the presentations enhanced visitors' online experience, thus reinforcing and advancing the brand and image of the Howard Stern Show and the defendant's products and services, were sufficient allegations of direct financial interest to avoid a motion to dismiss the plaintiff's claim for vicarious liability.[1901]

(k) Arista Records v. Usenet.com

In Arista Records LLC. V. Usenet.com, Inc.,[1902] the court applied both prongs of the vicarious liability doctrine in a rather broad fashion, in a factual context that was admittedly ripe for imposing liability.. In that case, the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing

---

[1897] Id. at 1113. The court's rulings with respect to contributory infringement are set forth in Section III.C.2(j) above.

[1898] Id. at 1109-10.

[1899] Id. at 1110-11 (citations omitted). For subsequent proceedings in this case, see Sections III.C.1(a) and III.C.2(j) above.

[1900] 2009 U.S. Dist. LEXIS 21373 (E.D. Pa. 2009).

[1901] Id. at *11-12.

[1902] 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

sharing networks, the files were stored on "spool" news servers operated by the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.[1903] The court granted the plaintiffs' motion for summary judgment on their claim for vicarious liability. Citing the Supreme Court's Grokster decision, the court noted that one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities. The court found that the defendants earned a direct financial benefit from the infringement because their revenues increased depending on their users' volume of downloads, the majority of which had been shown to be infringing. The court noted also that the infringing content on the service acted as a draw for users to subscribe to the service. The court rejected the defendants' argument that they lacked direct financial benefit from infringement because they were paid on a per-volume, not per-download, basis and because infringing music accounted for less than 1% of the newsgroups available on their service. The court noted that under the law, the draw of infringement need not be the primary, or even a significant, draw – rather it need only be "a" draw.[1904]

The court ruled that the defendants had also failed to exercise their right and ability to stop or limit infringement on their service. The defendants had in the past exercised their right and ability to control their subscribers' actions by terminating or limiting access of subscribers who posted spam, restricted download speeds for subscribers who downloaded a disproportionate volume of content, and taken measures to restrict users from posting or downloading files containing pornography.[1905] "Defendants likewise have the right and ability to block access to articles stored on their own servers that contain infringing content, but the record does not show any instance of Defendants exercising that right and ability to limit infringement by its users. More generally, Defendants have the right and ability to control which newsgroups to accept and maintain on their servers and which to reject, an ability they chose to exercise when they disabled access to approximately 900 music-related newsgroups in 2008."[1906] Accordingly, the court found the defendants vicariously liable.[1907]

(l) Corbis v. Starr

In Corbis Corp. v. Starr,[1908] the defendant Master, a janitorial maintenance company, hired defendant West Central, an Internet services company, to redesign and host its web site. The redesigned site contained four unauthorized images owned by the plaintiff Corbis. Corbis sent a letter to Master notifying it of the infringing images, and Master responded by directing West Central to remove the images, which West Central did. Corbis then filed suit against the defendants for copyright infringement and moved for summary judgment. The court found West

---

[1903] Id. at 130-31.

[1904] Id. at 156-57.

[1905] Id. at 157.

[1906] Id.

[1907] Id.

[1908] 2009 U.S. Dist. LEXIS 79626 (N.D. Ohio Sept. 2, 2009).

Central directly liable as a matter of law for copying the images onto Master's web site. It also found Master vicariously liable as a matter of law. The control prong of vicarious liability was satisfied because Master had the power to approve changes that West Central made to its corporate web site, including whether photos were used, and also had the ability to stop or limit infringing uses. West Central received a financial benefit from the infringement because the use of the copyrighted images (three of which depicted janitorial and cleaning services) helped draw customers.[1909]

(m) Arista Records v. Lime Group

(For a discussion of vicarious liability in this case, see Section III.C.4(d) below.)

(n) Hermeris v. Brandenburg

(For a discussion of vicarious liability in this case, see Section III.C.2(l) above.)

(o) Luvdarts v. AT&T Mobility

In Luvdarts LLC v. AT&T Mobility, LLC,[1910] the court ruled on a motion to dismiss that the defendant wireless carriers had no vicarious liability for operation of a system that enabled sharing of mobile multimedia messaging (MMS) content between devices, including the plaintiffs' copyrighted electronic greeting messages, because the plaintiffs had not plausibly alleged that the defendants had the right or ability to filter the content transmitted on their wireless networks. In addition, the court noted that the plaintiffs had designed their "Luvdarts" mobile multimedia messaging content several years after the defendants designed their mobile multimedia messaging system.[1911] "The court is not aware of any authority that would require Defendants to retrofit their general purpose network to accommodate technology later developed by a third-party for the purpose of being transmitted with that very technology."[1912] The court also dismissed the plaintiffs' claims for inducement and contributory infringement because the plaintiffs had not alleged that the defendants' networks were designed with the object of promoting infringement or that the defendants had taken affirmative steps to actively encourage or induce infringement, and the defendants' wireless networks were capable of noninfringing uses.[1913]

(p) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b) above. The court granted the defendants' motion to dismiss the plaintiff's claim for vicarious liability. With respect to the control requirement, the court noted that all the plaintiff had alleged as the basis that the

---

[1909] Id. at *2 & *7-9.

[1910] 2011 U.S. Dist. LEXIS 28369 (C.D. Cal. Mar. 17, 2011).

[1911] Id. at *9, 11.

[1912] Id. at *10-11.

[1913] Id. at *7.

defendants had the right and ability to control the infringing activity was that it had ownership of and operated the myVidster site. Mere ownership and control of the site was insufficient to establish the right and ability to control infringing activity on the site. With respect to the financial benefit requirement, the court noted that all the plaintiff needed to allege was that the availability of infringing material on myVidster was a draw for customers. However, the plaintiff had failed to do so. Although the complaint alleged that inexpensive storage space and the ability to share videos attracted customers to myVidster, it did not allege that the presence of the infringing material on the site enhanced the site's attractiveness or drew customers. Accordingly, the court dismissed the claim for vicarious infringement.[1914]

4. Inducement Liability

(a) The Supreme Court's Grokster Decision

For a detailed discussion of the Supreme Court's Grokster decision, which formally introduced inducement liability into the copyright law for the first time, see Section III.C.2(c)(5) above.

(b) Arista Records v. Usenet.com

In Arista Records LLC. V. Usenet.com, Inc.,[1915] the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on "spool" news servers operated by the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.[1916] The court, although noting several courts that had expressed doubt as to whether inducement of infringement states a separate claim for relief, or whether it is a species of contributory infringement, granted the plaintiffs' motion for summary judgment on their claim for inducement of infringement as a separate theory.[1917]

The court found the facts in the instant case very similar, and equally compelling, to those that led the Supreme Court to find inducement liability in Grokster. Specifically, a statistical survey based on random sampling concluded that over 94% of all content files offered in the defendants' music-related binary newsgroups were infringing or highly likely to be infringing.[1918] The defendants openly and affirmatively sought to attract former users of other notorious file-sharing services such as Napster and Kazaa, and boasted that as those file sharing services were scrutinized and shut down for copyright infringement, it would make the way for Usenet to "get back in the game."[1919] The defendants also used meta-tags such as "warez" and

---

[1914] Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *13-16 (N.D. Ill. May 10, 2011).

[1915] 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

[1916] Id. at 130-31.

[1917] Id. at 150 n.17 & 154.

[1918] Id. at 151-52.

[1919] Id. at 152.

"Kazaa" in the source code of their website to ensure that a search on a search engine for illegal content would return their website as a result. The record was replete with evidence of the defendants' own employees overtly acknowledging the infringing purpose for which their service was used and advertising such uses on their web site.[1920] The defendants' employees specifically provided technical assistance to users in obtaining copyrighted content and provided web site tutorials on how to download content, using infringing works as examples. Other evidence showed that, although the defendants had in place various tools and mechanisms that could be used to block access to infringing articles or newsgroups, they never used them to limit copyright infringement on their servers. Finally, the defendants' graded subscription payment plan caused users to pay more the more they downloaded. Accordingly, the court concluded that the defendants' intent to induce or foster infringement by its users on their services was unmistakable.[1921]

(c) Columbia Pictures v. Fung

In Columbia Pictures v. Fung,[1922] the defendants were operators of various sites that facilitated file sharing using the BitTorrent protocol. In a BitTorrent network, rather than downloading content files from an individual host, users of the network selected the content file they wished to download and then downloaded it in pieces through an automated process from a number of host computers (called a "swarm") possessing the content (or portions of it) simultaneously. Servers called "trackers" managed the download process from the multiple hosts. The defendants' sites (known as "torrent sites") maintained indexes of files called "dot-torrent files" that contained information identifying the various hosts where pieces of the desired content were stored. Users could also upload dot-torrent files for use by others to locate desired content. The dot-torrent files did not contain the actual content users were searching for (such as a move), but rather contained the data used by the BitTorrent client software on the user's computer to retrieve the content through a simultaneous peer-to-peer transfer from the multiple hosts of the content.[1923]

The plaintiffs were the owners of copyrighted movies that could be searched for through the index of dot-torrent files on the defendants' sites, then downloaded by users using the BitTorrent client software on their computers. They sought to hold the defendants secondarily liable for the downloading of infringing copies of their copyrighted content by users of the

---

[1920] Id. For example, an employee commented that the tag line for the service should be "piracy, porno and pictures – Usenet," and another commented that "Usenet is full of Music and Movies so get your pirate on!"Id.

[1921] Id. at 153-54.

[1922] 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009).

[1923] Id. at *8-11. "The dot-torrent file contains 'hash' values that are used to identify the various pieces of the content file and the location of those pieces in the network. The BitTorrent client application then simultaneously downloads the pieces of the content file from as many users as are available at the time of the request, and then reassembles the content file on the requesting computer when the download is complete." Id. at *11-12.

defendants' sites. The court granted the plaintiffs summary judgment on the issue of liability based on a theory of inducement.[1924]

Because BitTorrent users could be scattered throughout the world, to establish liability for inducement, the plaintiffs needed to establish that instances of direct infringement by BitTorrent users had taken place in the United States. The court rejected the defendants' argument the plaintiffs were required to provide evidence that both the transferor and the transferee of infringing content were located in the United States.[1925] "[T]he acts of uploading and downloading are each independent grounds of copyright infringement liability. Uploading a copyrighted content file to other users (regardless of where those users are located) violates the copyright holder's § 106(3) distribution right. Downloading a copyrighted content file from other users (regardless of where those users are located) violates the copyright holder's § 106(1) reproduction right. Plaintiffs need only show that United States users either uploaded or downloaded copyrighted works; Plaintiffs need not show that a particular file was both uploaded and downloaded entirely within the United States."[1926] Plaintiffs had adequately provided sufficient evidence to establish acts of direct infringement in the United States through IP address data that located defendants' users and showed that particular infringing downloads took place in the United States.[1927]

Turning to the facts of the case, the court granted the plaintiffs' motion for summary judgment on the issue of inducement liability based on the following acts by the defendants:

– Defendants' messages to users had stimulated others to commit infringement: The defendants web site had a "Box Office Movies" feature that periodically posted a list of the top 20 highest-grossing films then playing in the United States, which linked to detailed web pages concerning each film. Each of these pages contained "upload torrent" links allowing users to upload dot-torrent files for the films. The defendants' web sites presented available torrent files, the vast majority of which pointed to infringing content, in browseable categories and provided further information about the content. The defendants also generated lists of the most popular files in categories like "Top 20 Movies." The sites' operator, Fung, made statements on the site encouraging or assisting infringement, such as posting a message telling the site's users that they should try a particular software application could be used to frustrate copyright enforcement against file sharers. He also provided a link to a torrent file for the recent film *Lord of the Rings: Return of the King* and stated, "if you are curious, download this." Fung also created a promotional page inviting users to upload torrent files for *Matrix Reloaded*, another recent film. Also "warez" metatags were embedded in the sites for reference by search engines.[1928]

[1924] Id. at *3.

[1925] Id. at *28-29.

[1926] Id. at *29-30.

[1927] Id. at *32.

[1928] Id. at *39-43.

– Defendants and their moderators gave assistance to users engaged in infringement: Fung had personally posted messages in his site's discussion forum in which he provided technical assistance to users seeking copyrighted works. The sites were also full of statements by moderators who assisted users seeking to download files or provided links to other sites containing the requested infringing items. The court ruled that these moderators, who were under the control of the defendants and had been given authority to moderate the forums and user discussions, were agents of the defendants, and the defendants were therefore responsible for their acts.[1929]

– Defendants implemented technical features promoting copyright infringement: Defendants' sites allowed users to locate dot-torrent files for desired content, the vast majority of which was infringing. Fung implemented a spider program that located and obtained copies of dot-torrent files from other sites, including well known infringing sites such as "The Pirate Bay."[1930]

– Defendants' business model depended on massive infringing use: The court found there no factual dispute that the availability of copyrighted material was a major draw for users of Fung's web sites, and there was no dispute that defendants derived revenue from the web site and that this revenue increased along with the number of users.[1931]

The court rejected the defendants' assertions of the safe harbors under Sections 512(a) and 512(d). The court ruled that, as a general proposition, "inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business. Here … Defendants are liable for inducement. There is no safe harbor for such conduct."[1932]

Five months later, the court entered a permanent injunction against the defendants, enjoining them from, among other things, knowingly hosting, indexing, linking to, or otherwise providing access to any Dot-torrent or similar files that correspond, point to or lead to any copyrighted works owned by the plaintiffs and for which the plaintiffs had provided the title to the defendants, on or through any web site, system or software using BitTorrent or any peer-to-peer or other file-sharing or content delivery technology. The defendants were also enjoined from providing technical assistance or support services to users engaged in infringement; maintaining lists of "top" downloads that include the plaintiff's copyrighted works; including in metadata for any web pages, or maintaining browseable web site categories of Dot-torrent or similar files using, titles of the plaintiffs' copyrighted works or terms widely known to be associated with copyright infringement (such as "warez," "Axxo," "Jaybo," "DVD Rips," and the like); or soliciting or targeting a user base generally understood, in substantial part, to be

---

[1929] Id. at *44-47.

[1930] Id. at *51.

[1931] Id. at *55.

[1932] Id. at *67-68.

engaging in infringement of or seeking to infringe the plaintiffs' copyrighted works.[1933] The injunction also provided that, "In the event a commercial vendor or other third party becomes able to provide Defendants with a reliable list of Plaintiffs' Copyrighted Works, Plaintiffs may apply to the Court for an order modifying this Permanent Injunction to relieve them of the obligation of providing Defendants with lists of titles, even if there is a cost to Defendants of securing the lists of titles from the commercial vendor or third party."[1934]

(d) Arista Records v. Lime Group

In Arista Records LLC v. Lime Group LLC,[1935] the defendants distributed the peer-to-peer software client known as LimeWire that enabled users to share digital files across the Gnutella network. The LimeWire client contained a search function in its user interface that enabled the entry of search criteria. LimeWire would then scan the computers of other LimeWire users to locate files matching the search criteria, which could then be downloaded to the searching user's computer. The plaintiffs, owners of copyrights in various sound recordings that were shared without authorization by LimeWire users, brought claims of inducement, contributory infringement, and vicarious infringement against the defendants.[1936]

With respect to the claim of inducement, the court granted summary judgment to the plaintiffs. The court noted that under the Supreme Court's Grokster case, inducement constitutes a distinct cause of action from contributory infringement, and requires a showing that the defendant engaged in purposeful conduct that encouraged copyright infringement with the intent to encourage such infringement. The court found purposeful conduct to encourage infringement in the form of distribution of the LimeWire client, which users employed to commit a substantial amount of infringement.[1937]

The court found intent on the part of the defendants to encourage infringement from a combination of five factors taken together:

[1933] Columbia Pictures Industries, Inc. v. Fung, 2010 U.S. Dist. LEXIS 91169 at *20-23 (C.D. Cal. May 20, 2010).

[1934] Id. at *25.

[1935] 784 F. Supp. 2d 298 (S.D.N.Y. 2011). This opinion amended and replaced a prior opinion issued by the court, reported at 715 F. Supp. 2d 481 (S.D.N.Y. 2010).

[1936] 784 F. Supp. 2d at 409, 410-11.

[1937] Id. at 424-26. The court found the evidence clearly established direct infringement on the part of LimeWire users, since it demonstrated through documentation and electronic storage media that LimeWire users employed LimeWire to share and download the plaintiffs' copyrighted recordings without authorization. In one interesting side ruling, the court held that a genuine issue of material fact existed as to whether hash-based analysis could independently support a finding of direct infringement. The plaintiffs' expert argued that if two files have the same hash, they are identical, and if two users possess a file with identical hashes, one user's file is a copy of the other. The defendants' expert disputed this conclusion. He agreed that the fact that two users have a file with the same hash implies that the two users possess a file with likely the same content, but it does not imply that those two users shared the file with each other, or that one copied the file from the other. He argued that there are many different ways that the two users could have ended up with the same, identical file, such as by obtaining the file from the same, non-peer-to-peer source such as a web site, or from some non-gnutella-peer-to-peer network, or from some non-LimeWire Gnutella peer. Id. at 424 n.21.

– The defendants' awareness of substantial infringement by LimeWire users: The plaintiffs submitted an expert report showing that LimeWire was overwhelming used for infringement. In particular, the expert estimated that 98.8% of the files requested for download through LimeWire were copyright protected or highly likely copyright protected, which made it nearly certain that most actual downloads involved unauthorized content. Internal memoranda at LimeWire regularly discussed the fact that LimeWire users downloaded copyrighted recordings.[1938] For example, a 2001 draft of an offering memorandum in connection with a financing stated that LimeWire "allows people to exchange copyrighted mp3 files" and a 2002 statement of the company's goals acknowledged that, "Currently, the most common use of the Gnutella Network is the sharing of music files, many of them copyrighted."[1939] In 2006, LimeWire developed a strategic plan to "convert" LimeWire users who were sharing unauthorized digital recordings into customers of LimeWire's online music store, which would sell authorized music. In the conversion plan, LimeWire openly acknowledged that the majority of LimeWire's users were infringers. In addition, LimeWire employees maintained a file of articles labeled "Knowledge of Infringement."[1940]

– The defendants' efforts to attract infringing users: Following Napster's demise, LimeWire announced that it expected 30% to 100% of Napster users to switch to using LimeWire and similar programs such as Kazaa and Morpheus. LimeWire developed plans to attract Napster users to LimeWire, including conducting a marketing campaign through Google AdWords that would direct searches for "Napster" and similar terms to LimeWire. LimeWire also marketed LimeWire as similar to the popular Napster service.[1941]

– The defendants' efforts to enable and assist users to commit infringement: The LimeWire client user interface allowed searching for specific artists or albums, and a number of LimeWire's genre categories, such as "Classic Rock," "SoundTrack," and "Top 40," inevitably guided users to copyrighted recordings. LimeWire employees specifically tested and sought to improve LimeWire's ability to search for and download unauthorized copies of popular copyrighted songs and recordings. And several online communications between LimeWire employees and users specifically assisted LimeWire users in committing infringement.[1942]

– The defendants' dependence on infringement for success of its business: LimeWire's sources of revenue (selling advertising space on the LimeWire client and website, and distribution of software bundled with LimeWire) depended on LimeWire attracting the massive user population generated by its infringement-enabling features, and those revenues increased in proportion to the expansion of its user base. Thus, LimeWire's commercial success was derived largely from the high-volume use of LimeWire, most of which was infringing.[1943]

[1938] Id. at 411-12, 426.

[1939] Id. at 426.

[1940] Id. at 426-27.

[1941] Id. at 427-28.

[1942] Id. at 428-29.

[1943] Id. at 429.

– LimeWire's failure to mitigate infringing activities: "The evidence reveals that [the defendants have] not implemented in a meaningful way any of the technological barriers and design choices that are available to diminish infringement through file-sharing programs, such as hash-based filtering, acoustic fingerprinting, filtering based on other digital metadata, and aggressive user education."[1944] The court noted that in May 2006, LimeWire had implemented an optional hash-based content filter but that the default setting in the client for the filter was "off." The court noted that LimeWire could have made the hash-based content filter mandatory for all LimeWire users or made the default setting "on." The court further noted that LimeWire had considered, but failed to implement, several other plans to block the availability of infringing content through LimeWire, including a hybrid filtering system that would have combined hash-based filtering and acoustic fingerprinting. The company also developed, but did not implement, its conversion plan, which would have included a user education campaign designed to inform users about the legal consequences of copyright infringement and to promote the purchase of authorized music through the LimeWire online store. Under the conversion plan, LimeWire eventually would have implemented hash-based filtering and acoustic fingerprinting to prevent users from downloading unauthorized files. In addition, LimeWire used keyword-based filtering to allow users to limit their receipt of adult content and active filtering technology to prevent LimeWire users from sharing digital recordings purchased from the LimeWire online store, but did not use any of the filtering technology to screen out copyrighted content from the file-sharing activities of its users. The court found that this selective filtering further demonstrated LimeWire's knowledge of infringement-mitigating technologies and its intentional decision not to employ them in a way that meaningfully deterred its users' infringing activities.[1945] "Failure to utilize existing technology to create meaningful barriers against infringement is a strong indicator of intent to foster infringement."[1946]

Accordingly, the court granted the plaintiffs summary judgment on their claim of inducement of infringement.[1947]

The court, however, denied the plaintiffs' request for summary judgment with respect to their contributory infringement claim. Although the court found that LimeWire was aware of the prevalence of its users' infringing activities and made a material contribution to that infringement by designing, distributing, supporting, and maintaining the software, the court found material issues of fact as to whether the software was capable of substantial non-infringing uses under the Sony case. In particular, LimeWire had presented evidence of some types of non-

---

[1944] Id. at 429.

[1945] Id. at 429-31. The court discounted LimeWire's only step to address infringement – the posting of an electronic notice that appeared when a user first downloaded the LimeWire client, stating that the software was for sharing authorized files only and that downloading the software did not constitute a license for obtaining or distributing unauthorized content. Id. at 431. The user was also required to choose, prior to download, from the following statements: (1) "I will not use LimeWire for copyright infringement." Or (2) I might use LimeWire for copyright infringement." Id. If the user selected the second option, LimeWire would not be downloaded. The court ruled that the notice and statement of intent requirements did not, on their own, constitute meaningful efforts to mitigate infringement. Id.

[1946] Id.

[1947] Id.

infringing content that users share and download through LimeWire in the form of electronic copies of books in the public domain or authorize for distribution, historical documents, archival films and other public domain works, and digital music recordings produced by musicians seeking to promote their work through free online distribution. The court found the record before it insufficient to permit it to assess the technological feasibility or commercial viability of LimeWire's potential non-infringing uses.[1948]

The court granted the plaintiffs' request for summary judgment with respect to their vicarious liability infringement claim. The court found substantial evidence that LimeWire had the right and ability to limit the use of its product for infringing purposes, including by implementing filtering, denying access and supervising regulating users. The court found that LimeWire possessed a direct financial interest in the infringing activity of its users because LimeWire profited from its ability to attract infringing users, including through increased advertising revenue and increased sales of authorized music and an upgraded version of the LimeWire client that users paid for. The court rejected LimeWire's contention that because LimeWire was capable of substantial non-infringing uses, LimeWire could not be liable for vicarious infringement. The court found no case in which the Sony defense had been applied to a claim of vicarious infringement liability.[1949]

On Oct. 27, 2010, the court entered a stipulated permanent injunction that, among other things, enjoined LimeWire from copying, reproducing, downloading, distributing, or making available for distribution (by placing in a computer file or folder accessible by others for downloading) any of the plaintiffs' copyrighted works, and from displaying the source code for the LimeWire client. LimeWire was required to use its best efforts to use all reasonable technological means to prevent and inhibit future infringement of the plaintiff's copyrighted works by disabling the searching, downloading, uploading, file trading and file distribution functionality of legacy versions of the LimeWire client software, establishing default settings in the legacy versions that blocked the sharing of unauthorized media titles, and providing all users with a tool to uninstall the legacy versions. Before distributing any new version of the LimeWire client, LimeWire was required to obtain the approval to do so from the plaintiffs and the court.[1950] New versions of the client were required to incorporate a "Copyright Filter," which was defined as a "robust and secure means to exhaustively prevent" users from copying, downloading, distributing or communicating to the public the plaintiff's copyrighted works.[1951] The Copyright Filter was required to include the ability to filter both by text (i.e. artist and song title) and by the use of "Fingerprinting Technology," defined to mean "the most effective available means of content-recognition filtering based on recognizing the unique content of an underlying audio-visual work and detecting and preventing copying of that content no matter how the file containing the content was created (e.g. whether the file was ripped from a CD,

---

[1948] Id. at 433-34.

[1949] Id. at 435-36.

[1950] Arista Records LLC v. Lime Wire LLC, 2010 U.S. Dist. LEXIS 115675 (S.D.N.Y. Oct. 27, 2010) at *21-24.

[1951] Id. at *20, 23.

DVD, or recorded from a radio or television, etc.), and which is available from commercial vendors such as Audible Magic."[1952]

On Mar. 10, 2011, the court issued a ruling with respect to statutory damages to which the plaintiffs were entitled.[1953] The plaintiffs argued that, because the defendants had been found liable for inducing individuals to infringe their copyrights, they should be entitled to recover a separate statutory award for each individual's infringement of a work as to which they were jointly and severally liable. The court rejected this argument and ruled that the plaintiffs were entitled to only one statutory damage award per work from the defendants, regardless of the number of direct infringers of that work with whom the defendants were jointly and severally liable.[1954]

Section 504(c)(1) allows the recovery of a statutory damages award "for all infringements involved in the action, with respect to any one work, for which any one infringer is liable individually, or for which any two or more infringers are liable jointly and severally." The plaintiffs argued that the defendants and each direct infringer represented one unit of infringers who were jointly and severally liable, and they should therefore get an award for each such unit. The plaintiffs pointed to a similar hypothetical in Professor Nimmer's treatise arguing for such an outcome. The court, after a review of relevant precedent, rejected the Nimmer hypothetical and concluded that Congress intended for the copyright statute to treat jointly and severally liable infringers the same way that the statute treats individually liable infringers – just as a plaintiff is entitled to one statutory damage award per work for any individually liable infringer, a plaintiff is entitled to one statutory damage award per work for any two or more jointly and severally liable infringers. The court found that, in situations involving mass infringements, plaintiffs' position would lead to an absurd result of statutory damages exceeding a billion dollars. And the court noted that the number of direct infringers the defendants induced to infringe could be taken into account in setting the dollar amount of each statutory damage award per work infringed.[1955]

On April 4, 2011, the court issued a ruling that both an album and a sound recording that the plaintiffs issued as an individual track could constitute a "work" infringed for purposes of computing statutory damages. Specifically, the plaintiffs could recover a statutory damages award for each sound recording that (1) plaintiffs made available as an individual track and (2) that was infringed on the Lime Wire system during the time period in which it was issued as an individual track. However, for those sound recordings that plaintiffs issued only as part of an album, the plaintiffs could recover only one statutory damage award for that album, not for each individual sound recording.[1956]

[1952] Id. at *20-21.

[1953] Arista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 313 (S.D.N.Y. 2011).

[1954] Id. at 315, 321.

[1955] Id. at 316-320.

[1956] Arista Records LLS v. Lime Group LLC, 2011 U.S. Dist. LEXIS 36536 at *7, *18 (S.D.N.Y. Apr. 4, 2011). "Thus, for sound recordings that, like those of the Beatles, we4re apparently not available as individual tracks

In additional follow-up rulings on damages, the court rejected the plaintiffs' attempt to convert their election from statutory damages to actual damages with respect to untimely registered recordings, as the defendants would be unduly prejudiced by that change one month before trial, particularly in view of the fact that the defendants had been denied certain discovery on the ground that the plaintiffs were seeking only statutory damages.[1957] The court also precluded expert testimony showing that other illegal services would have induced infringement of the plaintiffs' copyrights if the defendants had not done so. The court held that the defendants could not argue they were not responsible for the infringement that took place through the Lime Wire system because that same infringement could have taken place through another system.[1958]

(e) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b) above. The court dismissed the plaintiff's claim for inducement of copyright infringement because it found that the plaintiff had failed to plead the requirements for an inducement claim as set forth in the Supreme Court's Grokster case. "Plaintiff pleads merely a formulaic recitation of inducement but not facts that plausibly suggest that it is entitled to relief on this theory. It is not enough to allege that myVidster provides storage for video files and encourages sharing (or even that it also knew that the website could be used to infringe). No clear expression of an infringing purpose is alleged, and no active steps taken to foster infringement, such as advertising an infringing use or instructing how to engage in an infringing use, are alleged."[1959]

5. Adequacy of Pleadings of Secondary Liability Against Service Providers

A number of cases have addressed the adequacy of pleadings of secondary liability on the part of service providers in view of the principles of liability articulated in the cases in the preceding three subsections.

(a) Miller v. Facebook

In Miller v. Facebook, Inc.,[1960] the plaintiff, owner of copyright in a video game called "Boomshine" sought to hold Yeo, the developer of another game called "ChainRxn," directly liable for infringing the look and feel of Boomshine, and to hold Facebook indirectly liable for

---

from iTunes or other services during the time period relevant to this action, Plaintiffs can recover only one award per album infringed." Id. at *18 n.7.

[1957] Arista Records LLC v. Lime Group LLC, 2011 U.S. Dist. LEXIS 38949 at *8, *10-11 (S.D.N.Y. Apr. 11, 2011).

[1958] Arista Records LLC v. Lime Group LLC, 785 F. Supp. 2d 423, 425 & 4272 (S.D.N.Y. 2011). "The Court emphasizes that this Order does not preclude the admission of evidence regarding other illegal services for all purposes. Such evidence may be admissible to show (1) that a diminution in Plaintiffs' profits over time is only partially attributable to Defendants (because others caused some of Plaintiffs' actual losses), and (2) the extent to which a large award in this case is likely to deter other infringers." Id. at 426.

[1959] Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *17-18 (N.D. Ill. May 20, 2011).

[1960] 2010 U.S. Dist. LEXIS 61715 (N.D. Cal. May 28, 2010).

listing ChainRXn in the Facebook Application Directory and providing the platform through which ChainRXn was distributed. Facebook sought to deny the plaintiff leave to file a second amended complaint. The court granted leave, finding that the proposed second amended complaint adequately pled claims of direct infringement against Yeo and contributory infringement against Facebook.[1961]

With respect to Yeo, the complaint adequately alleged direct infringement of the distribution right by alleging that Yeo published ChainRxn to a publicly accessible web site where it was then distributed to members of the public. It was reasonable to infer that ChainRxn was downloaded from the computer where it was hosted to the local cache memory of any Facebook user who played the video game. The plaintiff had also adequately pled a violation of the public performance right by Yeo because the video displays of Boomshine could be seen as being publicly performed when users played Yeo's allegedly infringing game.[1962]

Given adequate allegations of direct infringement by Yeo, the court ruled that the plaintiff had also adequately pled contributory infringement against Facebook. Noting that under the Ninth Circuit's decision in Perfect 10 v. Amazon, a computer system operator can be contributorily liable if it has actual knowledge that specific infringing material is available using its system and it could take simple measures to prevent further damage to the copyrighted works, the court ruled that the plaintiff had adequately pled "simple measures" that Facebook could have taken in the form of either disabling Yeo's Facebook account or removing ChainRxn from the Facebook Applications Directory.[1963]

(b) Williams v. Scribd

In Williams v. Scribd, Inc.,[1964] the court rejected Scribd's arguments why the plaintiff's amended complaint failed to state a claim for contributory and vicarious liability. The plaintiff alleged that a Scribd member uploaded onto the Scribd web site hundreds of pages of his copyrighted material. Noting that under the Ninth Circuit's decision in Napster,[1965] in the online context a plaintiff must allege and show actual knowledge on the part of a service provider for contributory liability, the court found that the plaintiff had adequately pled actual knowledge on the part of Scribd by pleading that he had notified Scribd of the infringement and asked that his materials be removed from the web site. And the plaintiff had adequately pled a material

---

[1961] Id. at *1-3.

[1962] Id. at *13-15. However, in a confusing aspect of the opinion, the court ruled that the plaintiff had not adequately pled a direct violation of the public display right because the plaintiff's copyright appears to be limited to the source code rather than the audiovisual aspects of the Boomshine, and the source code had not been publicly displayed. Id. at *13.

[1963] Id. at *20-21.

[1964] 2010 U.S. Dist. LEXIS 90496 (S.D. Cal. June 23, 2010).

[1965] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).

contribution to the infringement both by pleading the mere failure to remove and that the web site provided the site and facilities for direct infringement.[1966]

The court also rejected Scribd's argument that the plaintiff could not state a claim for vicarious copyright liability because he could not plausibly claim that Scribd benefited financially from the alleged infringement. The court noted that financial benefit exists where the availability of infringing materials acts as a draw for customers, and that the draw need not be substantial. Scribd argued that it had too many works on the site for the copyrighted materials of Williams to be a draw.[1967] Citing the Ellison case, the court held "that if the presence of infringing material on Scribd's website compels more people to visit the website than otherwise would, thereby making it more attractive to advertisers, Scribd can be said to benefit from the infringement."[1968] The court found that the plaintiff had alleged that the misuse of his copyrighted works attracted more users to Scribd's web site, and that was adequate at the pleading stage – although the court noted that during discovery, Scribd might be able to show that it didn't in fact generate ad revenues directly or even tangentially from the works of the plaintiff that were uploaded to its site.[1969]

6. Limitations of Liability of Online Service Providers in the DMCA

From late 1995 through May 1996, OSPs, telecommunications carriers and other distributors of online information, content providers and software companies negotiated intensively to reach a consensus on proposed legislation that would provide various statutory safe harbors with respect to the liability of online providers.[1970] The parties were unable to reach agreement for legislation in the 103rd Congress. The debate among the various industry segments was ignited again in connection with the WIPO copyright treaties in Geneva in December of 1996.

(a) History of the Various Legislative Efforts

A number of bills were then introduced in Congress that would limit the liability of OSPs. The first to be introduced was by Rep. Coble on July 17, 1997 (H.R. 2180). This bill would have exempted OSPs from direct or vicarious copyright liability solely based on the transmission or providing of access to online material, and eliminate any damage remedy for contributory liability, limiting plaintiffs to injunctive relief. The criteria for exemption were that the OSP: (a) not initially place the material online; (b) not generate, select, or alter the content of the material; (c) not determine the recipients of the material; (d) not receive a financial benefit directly attributable to a particular act of infringement; (e) not sponsor, endorse, or advertise the

---

[1966] Scribd, 2010 U.S. Dist. LEXIS 90496 at *19-20.

[1967] Id. at *23-24.

[1968] Id. at *24.

[1969] Id. at *24-25.

[1970] A summary of the issues and proposed legislative provisions may be found in K. Stuckey, Internet and Online Law § 6.10[5], at 6-96 to 6-98 (2008).

material; and (f) either not know or be aware by notice or other information indicating that the material is infringing, or be prohibited by law from accessing the material.

The second bill to be introduced was S. 1146, which, in addition to the WIPO treaty implementation provisions discussed above, also contained provisions limiting liability of OSPs. S. 1146 adopted a different approach to OSP liability than H.R. 2180. It contained three major provisions. First, it provided blanket exemptions from direct, vicarious or contributory liability for OSPs based on the mere provision of defined electronic communications network services or facilities, or on the transmission of private electronic communications, including voice messaging or electronic mail services or real-time communication formats, including chat rooms, streamed data, or other virtually simultaneous transmissions. Second, it provided exemptions from direct, vicarious or contributory liability for the provision of the following information location tools: a site-linking aid or directly, including a hyperlink or index; a navigational aid, including a search engine or browser; and the tools for the creation of a site-linking aid. Third, it provided immunity from direct, vicarious or contributory liability to OSPs for stored third party content, unless upon receiving notice of infringing material that complied with certain defined standards, the OSP failed expeditiously to remove, disable, or block access to the material to the extent technologically feasible and economically reasonable for the lesser of a period of ten days or receipt of a court order concerning the material.

Hearings were held in Sept. of 1997 on both H.R. 2180 and S. 1146. These hearings revealed lingering conflict between service providers and copyright owners on liability issues. Rep. Goodlatte led continuing negotiations between the content providers and OSPs, and to further a comprise, he and Rep. Coble introduced on Feb. 12, 1998 a substitute for H.R. 2180, entitled the "On-Line Copyright Infringement Liability Limitation Act" (H.R. 3209).

On April 1, 1998, the House Judiciary Committee approved the substance of H.R. 3209, but folded it into the pending WIPO implementation legislation, H.R. 2281. Subsequently, based on continuing negotiations, an agreement was finally reached between service providers and copyright owners with respect to the proper scope of liability for online infringements of copyright. H.R. 2281 was then amended to include this compromise agreement.

Meanwhile, similar actions were taking place in the Senate. The provisions of S. 1121, implementing the WIPO treaty, were combined with a new title embodying the compromise agreement between service providers and copyright owners with respect to liability.[1971] The combined Senate bill was denominated S. 2037, and was unanimously approved by the Senate Judiciary Committee in April of 1998 and adopted by the full Senate in May of 1998.

Both H.R. 2281 and S. 2037 contained the same substantive provisions with respect to OSP liability, which were ultimately adopted in the DMCA.

[1971] Sen. Patrick Leahy and Sen. John Ashcroft drafted the compromise agreement for incorporation into pending legislation.

(b) The OSP Liability Provisions of the DMCA

The liability provisions are contained in Title II of the DMCA. Title II seeks to clearly define the conditions under which an OSP's liability for infringements that occur on the OSP's systems or networks will be limited. Specifically, Title II defines four safe harbors that are codified in a new Section 512 of Title 17. If the OSP falls within these safe harbors, the OSP is exempt from monetary damages and is subject only to carefully prescribed injunctive remedies. As the legislative history states, "New Section 512's limitations on liability are based on functions, and each limitation is intended to describe a separate and distinct function. … [T]he determination of whether a service provider qualifies for one liability limitation has no effect on the determination of whether it qualifies for a separate and distinct liability limitation under another new subsection of new Section 512."[1972] This principle was codified in Section 512(n) of the DMCA, which provides: "Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection."[1973]

(1) Safe Harbors – Definition of a "Service Provider"

The four safe harbors are described below and are applicable to a "Service Provider." Under Section 512(k), for purposes of the first safe harbor, a "Service Provider" is defined as "an entity offering the transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." For purposes of the other three safe harbors, a "Service Provider" is defined more broadly to be "a provider of online services or network access, or the operator of facilities therefor." The latter definition would seem to cover a broad array of OSPs, BBS operators, system operators, search engines, portals, and the like. It is also probably broad enough to cover the owners and operators of corporate intranets, university networks and interactive websites.[1974]

In Marvel Enterprises, Inc. v. NCSoft Corp.,[1975] the court dismissed the plaintiffs' claim in their complaint for declaratory judgment that the defendants did not qualify as a "service provider" under the DMCA safe harbors and thus would not be protected from liability thereunder. The court noted the rule that a plaintiff may not seek declaratory relief as an advance ruling on a potential affirmative defense. From their allegations, it was clear that the plaintiffs were seeking a determination of the defendants' ability to use the DMCA as a defense. Because

---

[1972] H.R. Rep. No. 105-551 Part 2, at 65 (1998).

[1973] 17 U.S.C. § 512(n).

[1974] Ian C. Ballon & Keith M. Kupferschmid, "Third Party Liability under the Digital Millennium Copyright Act: New Liability Limitations and More Litigations for ISPs," *Cyberspace Lawyer*, Oct. 1998, at 3, 4. The legislative history states that the definition "includes universities and schools to the extent they perform the functions identified in" the definition. H.R. Rep. No. 105-551 Part 2, at 64 (1998).

[1975] 2005 U.S. Dist. LEXIS 8448 (C.D. Cal. Mar. 9, 2005).

the issues on which the plaintiffs sought declaratory judgment related only to the defendants' liability for the remainder of the plaintiffs' claims, the declaratory judgment would not independently resolve the controversy between the parties, but rather would merely determine a collateral legal issue governing certain aspects of the dispute. The court concluded that the plaintiffs were therefore inappropriately seeking an advance ruling on a potential affirmative defense.[1976]

(i) Acting as a Mere Conduit for Infringing Information – Section 512(a)

The first safe harbor is essentially a codification of the Netcom case and a rejection of the Frena case, at least to the extent that the Frena case suggested that passive, automatic acts engaged in through a technological process initiated by another through the facilities of an OSP could constitute direct infringement on the part of the OSP.[1977]

Specifically, under Section 512(a), a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if:

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content."

[1976] Id. at *18-19.

[1977] H.R. Rep. No. 105-551 Part 1, at 11 (1998); ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001). "Subsections (a)(1) through (5) limit the range of activities that qualify under this subsection to ones in which a service provider plays the role of a 'conduit' for the communications of others." H.R. Rep. No. 105-551 Part 2, at 51 (1998).

This safe harbor will not be available to a Service Provider that initiates, selects, or modifies the content of a transmission, or stores it on a system in a way that its content becomes generally accessible to third parties.

The safe harbor of Section 512(a) has been tested in the following cases to date:

a. The Napster Case

In the Napster case, discussed extensively in Section III.C.2.(c)(1) above, Napster moved for summary judgment that it was immune from the plaintiffs' claims by virtue of the Section 512(a) safe harbor. Napster argued that it fell within the subject matter of the safe harbor because its "core function" was to offer the "transmission, routing, or providing of connections for digital online communications" by enabling the connection of users' hard-drives and the transmission of MP3 files "directly from the Host hard drive and Napster browser through the Internet to the user's Napster browser and hard drive."[1978] Napster argued that it satisfied the preceding five specific conditions for the safe harbor because "(1) a Napster user, and never Napster itself, initiates the transmission of MP3 files; (2) the transmission occurs through an automatic, technical process without any editorial input from Napster; (3) Napster does not choose the recipients of the MP3 files; (4) Napster does not make a copy of the material during transmission; and (5) the content of the material is not modified during transmission."[1979]

The court rejected the applicability of the Section 512(a) safe harbor to Napster for several reasons. First, the court held that the safe harbor could not provide a complete defense to Napster's entire system because the system performed more than just the functions of transmission, routing, and providing of connections. Specifically, the court noted that Section 512(n) of the DMCA provides that the four safe harbors "describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsections."[1980] The court ruled that the Napster system, through its index of user files and its "hot list" feature that each functioned as an "information location tool," undisputedly performed some information location functions which, if those functions were to be immunized, must satisfy the separate provisions of the safe harbor set forth in Section 512(d) (discussed in subsection (iv) below).[1981]

Napster argued that, even if its system functioned in part as an information location tool, that function should be considered incidental to the system's core function of transmitting MP3 music files, and the safe harbor of Section 512(a) should therefore provide a complete defense to its system. The court rejected this argument, holding that because the parties disputed material issues regarding the operation of Napster's index, directory and search engine, the court could

---

[1978] A&M Records Inc. v. Napster, Inc., 54 U.S.P.Q.2d 1746, 1749 (N.D. Cal. 2000).

[1979] Id.

[1980] 17 U.S.C. § 512(n).

[1981] Napster, 54 U.S.P.Q.2d at 1750.

not hold for purposes of summary judgment that the information location tool aspects of the Napster system were peripheral to the alleged infringement, or that they should not be analyzed separately under Section 512(d).[1982]

The court then rejected the applicability of Section 512(a) to Napster for two principal reasons. First, the court noted that the preamble of Section 512(a) makes the safe harbor applicable only to service providers "transmitting, routing or providing connections for, material through a system or network controlled or operated by or for the service provider" (emphasis added). The court found it undisputed that MP3 files do not pass "through" Napster's servers, but rather "through" the Internet, and ruled that the Internet could not be considered "a system or network controlled or operated by or for the service provider."[1983] The court rejected Napster's argument that its system should be deemed to include the Napster browser on its users' computers and that the MP3 files were transmitted "through" that browser: "[E]ven if each user's Napster browser is part of the system, the transmission goes from one part of the system to another, or between parts of the system, but not 'through' the system. The court finds that subsection 512(a) does not protect the transmission of MP3 files."[1984]

Second, the court called into question whether Napster had complied with the prefatory conditions of Section 512(i) of the DMCA (discussed further in subsection (2) below), which imposes additional requirements on eligibility for any DMCA safe harbor. Section 512(i) requires that the Service Provider adopt and reasonably implement, and inform subscribers and account holders of the Service Provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the Service Provider's system or network who are repeat infringers.

The court found questions about Napster's compliance with Section 512(i) on two grounds. The first ground was that, although Napster claimed to have had an oral policy from the earliest days of its existence, Napster had not adopted a *written* policy for termination of repeat infringers until after the litigation was filed. The court noted that, even were the written policy ultimately adopted an adequate one, the late adoption of a formal written policy would not necessarily moot the plaintiffs' claims to monetary relief for past harms.[1985] The second ground was that the court believed Napster had not established that it *reasonably* implemented a policy for terminating repeat infringers. Specifically, the court noted that Napster blocked users about whom it received notices of infringement by blocking that user's password, but not the Internet

---

[1982] Id. at 1750.

[1983] Id. at 1751.

[1984] Id. (emphasis in original). The court similarly found that the Napster system did not provide *connections* "through" its system. "Although the Napster server conveys address information to establish a connection between the requesting and host users, the connection itself occurs through the Internet. … Drawing inferences in the light most favorable to the non-moving party, this court cannot say that Napster serves as a conduit for the connection itself, as opposed to the address information that makes the connection possible. Napster enables or facilitates the initiation of connections, but these connections do not pass through the system within the meaning of subsection 512(a)." Id. at 1752.

[1985] Id. at 1753.

Protocol (IP) address of the user. (The parties sharply disputed whether it would be feasible or effective to block IP addresses.) The court further noted the plaintiffs' argument that, because Napster did not maintain the actual identity of its users (their real names and physical addresses), blocked users could readily reapply for a new account on the Napster system and continue their infringing activity. The court therefore concluded that the plaintiffs had raised genuine issues of material fact about whether Napster had reasonably implemented a policy of terminating repeat infringers, and therefore denied Napster's motion for summary judgment based on a Section 512(a) defense.[1986]

b. Ellison v. Robertson

In Ellison v. Robertson,[1987] an individual named Robertson scanned several fictional works written by the plaintiff and posted them onto the Usenet group "alt.binaries.e-book," a group that was used primarily to exchange pirated and unauthorized digital copies of text material, principally works of fiction by famous authors. AOL, acting as a Usenet peer, hosted the infringing materials on its Usenet server for a period of fourteen days. The plaintiff sought to hold AOL liable for direct, vicarious and contributory copyright infringement.[1988] AOL asserted that the plaintiff could not establish the elements for common law liability and that it was immune under the Section 512(a) and Section 512(c) safe harbors of the DMCA. The district court, relying on the Netcom case, ruled that AOL could not be liable for direct copyright infringement merely based on its passive role as a provider of Usenet services.[1989] The court's rulings with respect to contributory infringement are discussed in Section III.C.2(e) above.

With respect to vicarious liability, the plaintiff argued that, under the Ninth Circuit's Napster I decision, AOL's ability to block infringers' access to its Usenet servers was sufficient to establish the right and ability to control infringing activity. The court rejected this argument, noting the same Catch 22 under the Section 512(c) safe harbor this would set up that the court noted in the Hendrickson v. eBay case: Because an OSP is required under Section 512(c)(1)(C) to delete or block access to infringing material, if this ability to delete or block were sufficient to establish the "right and ability to control" infringing activity, the OSP would thereby be disqualified from the safe harbor under Section 512(c)(1)(B), at least if it received a financial benefit directly attributable to the infringing activity.[1990] "The Court does not accept that Congress would express [an intention that ISPs which receive a financial benefit directly attributable to the infringing activity could not qualify for the Section 512(c) safe harbor under any circumstance] by creating a confusing, self-contradictory catch-22 situation that pits 512(c)(1)(B) and 512(c)(1)(C) directly at odds with one another, particularly when there is a much simpler explanation: the DMCA requires more than the mere ability to delete and block

---

[1986] Id.

[1987] 189 F. Supp. 2d 1059 (C.D. Cal. 2002).

[1988] Id. at 1053-54.

[1989] Id. at 1056.

[1990] Id. at 1060-61.

access to infringing material after that material has been posted in order for the ISP to be said to have 'the right and ability to control such activity.'"[1991]

The court further found that AOL's right and ability to control the infringing behavior was substantially less than that enjoyed by the OSP in the Netcom case, where the OSP was one of two entities responsible for providing the direct infringer with access to the Internet. As a result, by taking affirmative steps against the other entity, the OSP had the ability to target the infringer himself and deny him access to the Internet. By contrast, AOL had no such ability to go after the individual who had posted the infringing copies of the plaintiff's works onto Usenet. The court therefore concluded that AOL's ability to delete or block access to the infringing postings after they had found their way onto AOL's Usenet servers was insufficient to constitute the right and ability to control the infringing activity for purposes of common law vicarious liability.[1992]

With respect to the financial benefit prong of vicarious liability, the district court held that AOL received no direct financial benefit from the infringing activity. The court ruled that the direct financial benefit prong requires a showing that a "substantial" proportion of a defendant's income be directly linked to infringing activity.[1993] AOL did not receive any financial compensation from its peering agreements and participation in Usenet, and the availability of Usenet did not act as a "draw" for customers under the Napster I case. In particular, the court noted that any "draw" to a particular newsgroup, such as alt.binaries.e-book, was miniscule, as the pro rata "draw" of a single newsgroup was only about 0.00000596% of AOL's total usage (there were 43,000 total newsgroups available through AOL). Usenet usage constituted a very small percentage of total AOL usage, and the plaintiff had not produced any evidence that a significant portion of even that minimal usage entailed the illegal exchange of copyrighted material.[1994] Accordingly, the court granted summary judgment to AOL on the plaintiff's claim for vicarious liability.[1995]

On appeal, the Ninth Circuit affirmed the finding of no vicarious liability, although the Ninth Circuit disagreed with the district court's ruling that to establish a direct financial benefit, the plaintiff must show that a "substantial" proportion of a defendant's income be directly linked to infringing activity. The Ninth Circuit stated that it is sufficient if infringing activity is a "draw" for customers, and there is no requirement that such draw be "substantial."[1996] "The essential aspect of the 'direct financial benefit' inquiry is whether there is a causal relationship

---

[1991] Id. at 1061.

[1992] Id. at 1061-62.

[1993] Id. at 1062-64.

[1994] Id. at 1062-63.

[1995] Id. at 1064.

[1996] Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004).

between the infringing activity and any financial benefit a defendant reaps, regardless of *how substantial* the benefit is in proportion to a defendant's overall profits."[1997]

The Ninth Circuit ruled that the plaintiff had not submitted sufficient evidence to raise a triable issue of fact under the direct financial benefit prong, and in the course of its discussion, fleshed out what sort of evidence would be required to show that infringing activity on a particular site constitutes a "draw" to that site:

> We recognize, of course, that there is usually substantial overlap between aspects of goods or services that customers value and aspects of goods or services that ultimately draw the customers. There are, however, cases in which customers value a service that does not "act as a draw." Accordingly, Congress cautions courts that "receiving a one-time set-up fee and flat periodic payments for service … [ordinarily] would not constitute receiving a 'financial benefit directly attributable to the infringing activity.'" S. Rep. 105-190, at 44. But "where the value of the service lies in providing access to infringing material," courts might find such "one-time set-up and flat periodic" fees to constitute a direct financial benefit. *Id*. at 44-45. Thus, the central question of the "direct financial benefit" inquiry in this case is whether the infringing activity constitutes a draw for subscribers, not just an added benefit.[1998]

The Ninth Circuit found that there was no evidence that AOL customers either subscribed because of the available infringing material or canceled subscriptions because it was no longer available. Accordingly, no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material, and the claim for vicarious liability failed.[1999]

The district court also ruled on an assertion by AOL of two of the DMCA safe harbors – the Section 512(a) and the Section 512(c) safe harbors. The district court noted that as a predicate for any of the safe harbors, AOL had to satisfy the requirement of Section 512(i) that it have adopted and reasonably implemented, and informed its subscribers, of a policy for the termination in appropriate circumstances of subscribers who are repeat infringers.[2000] Citing the legislative history, the court ruled that Section 512(i) does not require OSPs to take affirmative steps to investigate potential infringement and set up notification procedures in an attempt to identify the responsible individuals committing infringement through the system. Rather, it was sufficient to satisfy Section 512(i) that AOL's terms of service, to which every AOL member had to agree, included a notice that AOL members could not make unauthorized copies of content

---

[1997] Id. at 1079 (emphasis in original).

[1998] Id.

[1999] Id.

[2000] The court noted that such a policy must have been adopted, reasonably implemented and noticed to subscribers at the time the allegedly infringing activity occurred. "Doing so after the infringing activity has already occurred is insufficient if the ISP seeks a limitation of liability in connection with that infringing activity." Ellison v. Robertson, 189 F. Supp. 2d 1059, 1064 (C.D. Cal. 2002).

protected by intellectual property rights and their accounts could be terminated for making such unauthorized copies.[2001]

The plaintiff challenged whether AOL had reasonably implemented its termination policy by noting that no subscriber had ever been terminated from AOL as a repeat infringer and AOL had not at the time of the infringement defined how many times a user had to be guilty of infringement before being classified as a repeat infringer. The court rejected this challenge, noting that Section 512(i) does not require AOL to actually terminate repeat infringers or even to investigate infringement in order to determine if AOL users are behind it. "That is the province of subsection (c), which provides detailed requirements related to notification of infringement and the ISPS' responsibility to investigate and, in some instances, delete or block access to infringing material on their systems. Subsection (i) only requires AOL to put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights."[2002] The court therefore held that AOL had satisfied the predicate requirements of Section 512(i).[2003]

The district court then turned to application of the Section 512(a) safe harbor. The court first noted that Section 512(a) "does not require ISPs to remove or block access to infringing materials upon receiving notification of infringement, as is the case with subsections (c) and (d)."[2004] The plaintiff argued that AOL was not engaged in "intermediate and transient storage"[2005] required under Section 512(a) because it maintained Usenet materials on its server for fourteen days. The court posed the issue under Section 512(a) as follows: "Certain functions such as the provision of e-mail service or Internet connectivity clearly fall under the purview of subsection (a); other functions such as hosting a web site or chatroom fall under the scope of subsection (c). The question presented by this case is which subsection applies to the function performed by AOL when it stores USENET messages in order to provide USENET access to

---

[2001] Id. at 1064-65.

[2002] Id. at 1066. An important implication of this ruling appears to be that an OSP can qualify for the Section 512(a) safe harbor regardless of whether it promptly deletes infringing material or terminates repeat infringers, so long as it has a policy to do so and otherwise complies with the requirements of the Section 512(a) safe harbor. The court further stated: "[T]he 'realistic threat of losing [Internet] access' that Congress wishes ISPs to impress upon would-be infringers remains just that – a mere threat – unless the ISP decides to implement procedures aimed at identifying, investigating, and remedying infringement in hopes of meeting the requirements of subsection (c)'s safe harbor. Such an arrangement makes a certain amount of sense. If subsection (i) obligated ISPs to affirmatively seek out information regarding infringement and then investigate, eradicate, and punish infringement on their networks, then most if not all of the notice and takedown requirements of the subsection (c) safe harbor would be indirectly imported and applied to subsections (a) and (b) as well. This would upset the carefully balanced, "separate function-separate safe harbor-separate requirements" architecture of the DMCA." Id. at 1066 n.15.

[2003] Id. at 1066.

[2004] Id. at 1068.

[2005] Clause (4) of Section 512(a) requires that "no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections."

users."[2006] The court answered that Section 512(a) applies, based primarily on the fact that the legislative history of the Section 512(a) safe harbor expressly noted that the exempted storage and transmissions under that section "would ordinarily include forwarding of customers' Usenet postings to other Internet sites in accordance with configuration settings that apply to all such postings."[2007] The court further ruled that storage of the Usenet postings for fourteen days was not too long to disqualify the storage as intermediate and transient. The court noted that Usenet messages had been stored for eleven days in the Netcom case, and that three days was an insufficient difference to distinguish the present case from Netcom. Accordingly, the court ruled that AOL's Usenet storage was "intermediate and transient."[2008]

The court further ruled that AOL had satisfied the remaining requirements of Section 512(a). The transmission of the plaintiff's newsgroup message was not initiated by AOL, AOL did not select the individual postings on the alt.binaries.e-book newsgroup (and the fact that AOL decided not to carry every newsgroup did not constitute selection of the specific material giving rise to the claim of infringement[2009]), AOL did not select the recipients of the material,[2010] and the material was transmitted through AOL's system without modification of its content.[2011] Accordingly, the court concluded that AOL qualified for the Section 512(a) safe harbor, and that it therefore needed not reach the issue of whether the Section 512(c) safe harbor also applied.[2012]

On appeal, the Ninth Circuit reversed the ruling that AOL was entitled to the Section 512(a) safe harbor on the ground that there were triable issues of material fact concerning whether AOL had met the threshold requirements of Section 512(i). The Ninth Circuit ruled, however, that if after remand a jury found AOL to be eligible under Section 512(i) to assert the DMCA safe harbors, then "the parties need not relitigate whether AOL qualifies for the limitation of liability provided by § 512(a); the district court's resolution of that issue at the summary judgment stage is sound."[2013]

With respect to Section 512(i), the Ninth Circuit found it difficult to conclude that AOL had reasonably implemented a policy against repeat infringers, because there was ample evidence in the record suggesting that AOL did not have an effective notification procedure in place at the time the alleged infringing activities were taking place. Although AOL had notified the Copyright Office of its correct email address before Ellison's attorney attempted to contact

---

[2006] Id. at 1068.

[2007] Id. at 1069-70 (quoting H.R. Rep. 105-551(I) at p. 24).

[2008] 189 F. Supp. 2d at 1070.

[2009] To impute selection of the infringing material to the ISP, "the better interpretation of [512](a)(2) is that the ISP would have to choose specific postings, or perhaps block messages sent by users expressing opinions with which the ISP disagrees." Id. at 1071.

[2010] To impute selection of the recipients of the material to AOL, "the better interpretation is that AOL would have to direct material to certain recipients (e.g. all AOL members whose names start with 'G') but not others."Id.

[2011] Id. at 1070-72.

[2012] Id. at 1072 & n.22.

[2013] Ellison v. Robertson, 357 F.3d 1072, 1074 (9th Cir. 2004).

AOL and did post its correct email address on the AOL website with a brief summary of its policy as to repeat infringers, AOL also changed the email address to which infringement notifications were supposed to have been sent and failed to provide for forwarding of message sent to the old address or notification that the email address was inactive.[2014] The Ninth Circuit found that AOL should have closed the old email account or forwarded the emails sent to the old account to the new one. The fact that AOL had allowed notices of potential copyright infringement to go unheeded for a period of time was sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers.[2015]

c. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(a) safe harbor (as well as the Section 512(c) safe harbor, discussed in Section III.C.6(b)(1)(iii).e below). In ruling on Aimster's assertions of the safe harbors, the district court first noted that the DMCA safe harbors could potentially apply to liability for direct, vicarious and contributory copyright infringement.[2016] Note that this holding is consistent with the Ninth Circuit's holding in Napster I, in which the court ruled that the safe harbors could potentially shield against vicarious liability,[2017] but inconsistent with the CoStar case, which concluded that the safe harbors cannot shield against vicarious liability (see the discussion in Section III.C.6(b)(1)(iii).c below).

The district court then turned to whether Aimster had satisfied the predicate conditions of meeting the definitions of "service provider" in Sections 512(k)(1)(A) & (B) and adopting an adequate policy of termination of repeat infringers under Section 512(i)(1)(A). The court found that Aimster qualified as a "service provider" because a "plain reading of both definitions reveals that 'service provider' is defined so broadly that we have trouble imagining the existence of an online service that *would not* fall under the definitions."[2018]

The district court found, however, that Aimster had not adopted an adequate policy to terminate repeat infringers. Although Aimster's copyright notice on its site informed users of a procedures for notifying Aimster when infringing activity was taking place on the system and stated that users who were found to repeatedly violate copyright rights of other may have their access to all services terminated, the court held that the policy was not reasonably implemented because it is fact *could not* be implemented. In particular, the encryption on Aimster rendered it impossible to ascertain which users were transferring which files, nor did Section 512(i) obligate the plaintiffs to provide the Internet protocol address of a particular copyright infringer on the

---

[2014] Id. at 1080.

[2015] Id.

[2016] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 657 (N.D. Ill. 2002).

[2017] The district court's 2002 decision on the plaintiffs' motion for summary judgment in the MP3Board case, discussed in Section III.D.8 below, also at least implicitly recognized that the Section 512(d) safe harbor could apply to a claim of vicarious liability.

[2018] Id. at 658 (emphasis in original).

Aimster system to assist Aimster in implementing its termination policy.[2019] "Adopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an 'implementation' as required by § 512(i)."[2020] Accordingly, Aimster's failure to comply with Section 512(i) rendered it ineligible for any of the safe harbors.[2021]

In addition, the court ruled that Aimster had not satisfied the particular conditions for the Section 512(a) safe harbor because, relying on one of the district court's decisions in the Napster case, the information transferred between individual Aimster users did not pass "through" Aimster's system at all by virtue of its peer-to-peer architecture (Section 512(a) immunizes liability by virtue of a service provider's transmitting, routing or providing connections for, "materials through a system or network controlled or operated by or for the service provider").[2022] The holdings of the Napster and Aimster courts on this point, if adopted by other courts, will make it difficult for the Section 512(a) safe harbor ever to apply to a peer-to-peer architecture. The court rejected Aimster's argument that "through" should be interpreted to mean "by means of" or "by the help or agency of."[2023] Finally, the court noted that Aimster was ineligible for the Section 512(a) safe harbor because its encryption of the information transferred between users constituted a modification of that information, which Section 512(a) does not permit.[2024]

On appeal, the Seventh Circuit affirmed that Aimster was not entitled to any of the safe harbors of the DMCA, but based its conclusion solely on the ground that Aimster had not complied with the predicate conditions of Section 512(i). "Far from doing anything to discourage repeat infringers of the plaintiffs' copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement."[2025]

d. Perfect 10 v. CCBill

The District Court's Decision.

The plaintiff, Perfect10, owner of the copyrights in an extensive collection of pornographic photos, brought a copyright infringement lawsuit against CWIE, an OSP hosting various sites that allegedly contained infringing copies of Perfect10's photos, as well as several related third parties providing ancillary services to such sites: IBill, a company that processed payments for online merchants, Internet Key, an age verification service for adult content

---

[2019] Id. at 659.

[2020] Id.

[2021] Id.

[2022] Id. at 659-60.

[2023] Id. at 660.

[2024] Id. at 660 n.19.

[2025] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

websites, and CCBill, a provider of a fully automated Internet service that enabled consumers to use credit cards or checks to pay for subscriptions or memberships to e-commerce venues created and offered by CCBill's clients.[2026] Each of the defendants raised various of the DMCA safe harbors as defenses, of which the Section 512(a) defenses will be discussed here (the remaining defenses are discussed in the subsections below).

Perfect 10 challenged the various defendants' ability to rely on the safe harbors for failure to comply with the predicate requirements of Section 512(i) as well as failure to meet the substantive criteria of the individual safe harbors. The court considered the factual posture of each of the defendants in turn, and the case is particularly interesting because it is the first to comprehensively adjudicate the adequacy of specific language comprising a policy to terminate repeat infringers. The court began its analysis with some general observations about the DMCA, and quoted from the Fourth Circuit's decision in the ALS Scan case that the safe harbor immunity is afforded "only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter …"[2027]

The court then turned to the applicability of the safe harbors to each of the individual defendants as follows:

IBill. The court first considered the adequacy of IBill's policy to terminate repeat infringers under Section 512(i). Under IBill's policy, when it received a notice of infringement that substantially complied with the DMCA requirements, it suspended payment processing services to that client. If IBill determined that it had received previous complaints about that client or the website, IBill terminated the account permanently. Perfect 10 argued that this policy was inadequate because it suspended services for particular websites without terminating the webmaster responsible for that material. The court rejected this argument, noting that the focus of Section 512(i) is on infringing users rather than on content. The policy of disabling of IBill clients accused of infringing third party copyrights was therefore adequate.[2028]

Perfect 10 argued that IBill had not reasonably implemented its termination policy because it had not kept a log of its notifications of infringement. The court held that the DMCA does not require an OSP to keep a log of its notifications. Because IBill had kept the actual DMCA notifications it had received, this was sufficient to demonstrate that it adequately tracked its notifications.[2029] The court further held that many of the notifications Perfect 10 had sent to IBill were inadequate to trigger a duty to act on them. Several such notices were emails from Perfect 10's counsel that identified several websites run by IBill's clients that contained

---

[2026] Perfect 10, Inc. v. CCBill, 340 F. Supp. 1077, 1082-84 (C.D. Cal. 2004).

[2027] Id. at 1086 (citations omitted).

[2028] Id. at 1088-89.

[2029] Id. at 1089.

allegedly infringing material, but did not identify the URLs of the infringing images nor identify which of Perfect 10's copyrighted images were being infringed. The court held that the failure to identify the URLs or the copyrighted images made the notices inadequate. Another notice identified the URL of an infringing image, although not the copyrighted work that it allegedly infringed. The court ruled that, although the notice did not comply with all of the requirements of Section 512(c)(3)(a), the supply of a URL was sufficiently substantial compliance to give rise to a duty to act.[2030] Because IBill had acted on the single sufficient notice by suspending the account of the website, the court concluded that IBill had reasonably implemented its repeat infringer policy.[2031]

With respect to the Section 512(a) safe harbor, Perfect 10 argued that IBill did not qualify because it did not transmit the infringing material at issue, but rather only credit card information. In an important holding, the court read the scope of Section 512(a) very expansively to cover IBill based on the language of Section 512(a) that affords immunity for "providing connections for material through a system or network controlled or operated by or for the service provider."[2032] The court concluded that IBill was within this language: "IBill provides a connection to the material on its clients' websites through a system which it operates in order to provide its clients with billing services."[2033] Accordingly, the court granted summary judgment to IBill under the Section 512(a) safe harbor.[2034]

Internet Key. Perfect 10 challenged Internet Key's compliance with the threshold requirements of Section 512(i) based on its termination policy, which read as follows:

> **Banned Webmaster**
> If a webmaster, identified by either the webmaster's name, vendorID or common ownership entity, has had three (3) websites which have been denied participation in the SexKey program in accordance with this policy, that webmaster will be denied participation in its program of any webmaster or website in its discretion.
> . . .
> **Repeat Offenders**
> The participation of any website deemed to be a repeat offender will be terminated.
> **Banned Websites**
> Pending receipt of a Counter Notification, participation of the website subject to a Notification will be suspended. A website will be permanently prohibited from

---

[2030] Id. at 1089-90.

[2031] Id. at 1090.

[2032] Id. at 1091.

[2033] Id. The court rejected Perfect 10's reliance on the Aimster case, noting that the Aimster case dealt with the transmission of material, not the provision of a connection to the material. Id. at 1091-92.

[2034] Id. at 1092.

participating in the SexKey program upon receipt by the Company of a second Notification.[2035]

The court ruled that this policy, which provided that Internet Key would disable access to an affiliate website after it received a single notification of an infringement, and would permanently ban a webmaster from Internet Key after it had received three notifications regarding websites of any particular webmaster, was legally adequate.[2036] "In order for an infringer to be a 'repeat' infringer, he or she must infringe at least twice. Therefore, the Court finds that Internet Key's policy of terminating a webmaster after 3 notifications is reasonable."[2037]

Perfect 10 next challenged Internet Key's implementation of its termination policy, arguing that it had provided Internet Key with 22,000 pages of printouts from SexKey affiliated web sites which infringed its rights, together with many full-sized printouts of the images that constituted infringement, and Internet Key did not disable access to the infringing web sites. The court found Perfect 10's notices of infringement inadequate under the DMCA. A letter from Perfect 10's counsel accompanying the document production failed to identify which documents were found on Internet Key's affiliate web sites, did not contain a statement that the information in the notification was accurate, and did not state that the author had a good faith belief that the information in the letter was accurate nor was there a declaration under penalty of perjury. Although the letter identified which images were infringing, it did not identify which copyrights of Perfect 10 the images infringed. Perfect 10's notice was therefore not compliant with the DMCA, and absent a DMCA-compliant notice, the court ruled that Perfect 10 had failed to raise a genuine issue of material fact concerning whether Internet Key met the threshold requirements of Section 512(i).[2038]

With respect to the Section 512(a) safe harbor, the court ruled that Internet Key's age verification service function fell within the functions described in Section 512(a) – specifically, Internet Key was "providing connections for material" on its client web sites through a system it operated to provide its clients with adult verification services. The court therefore granted summary judgment to Internet Key on the Section 512(a) safe harbor for infringement claims arising after the date it adopted its DMCA policy (but denying summary judgment for infringement claims prior to the date Internet Key put a DMCA policy into place).[2039]

[2035] Id. at 1093-94..

[2036] Id. at 1094.

[2037] Id. at 1094 n.12. The court also rejected Perfect 10's challenge to the reasonableness of Internet Key's termination policy on the ground that Internet Key's web site identified one person as its designated copyright agent, whereas Internet Key's owner testified that its agent was a company. The court rejected this challenge, noting that Internet Key had never failed to respond to notices, and in any event it appeared that Internet Key likely had more than one individual who responded to notifications of copyright infringement. Id. at 1094.

[2038] Id. at 1095-97.

[2039] Id. at 1098-99.

CWIE and CCBill. Perfect 10 challenged the repeat infringer policies of CWIE and CCBill under Section 512(i) on a number of grounds. First, it argued that their DMCA notice spreadsheet was missing several webmaster names of its affiliate sites. The court rejected this challenge, noting that only a few webmaster names were missing from the spreadsheet in instances where the notice was deficient or the issues were resolved, and such was insufficient to raise a genuine issue of material fact that CWIE and CCBill did not reasonably implement their repeat infringer policies.[2040]

Second, Perfect 10 argued that CWIE and CCBill had failed to act in response to a number of infringement notices Perfect 10 had sent. The court found, however, that such notices were deficient under the DMCA because they identified only the web sites containing allegedly infringing material, but did not identify the URLs of the infringing images or which of Perfect 10's copyrights were being infringed.[2041]

Finally, Perfect 10 argued that it submitted several emails to CWIE regarding password hacking web sites that provided passwords to Perfect 10's web sites and CWIE failed to discontinue hosting those web sites. The court ruled, however, that Perfect 10 had not submitted any evidence that the use of the passwords actually resulted in the infringement of Perfect 10's copyrights. Accordingly, Perfect 10 had failed to raise any genuine issues of material fact that CWIE and CCBill did not reasonably implement their repeat infringer policies.[2042]

With respect to the applicability of the Section 512(a) safe harbor to CCBill, Perfect 10 argued that CCBill did not fall within that safe harbor because it did not transmit the infringing material at issue. Perfect 10 argued that Section 512(a) provides protection only for OSPs who transmit the allegedly infringing material and not other material, such as credit card information. Once again, however, the court found CCBill entitled to Section 512(a)'s safe harbor because CCBill provided a "connection" to the material on its clients' web sites through a system which it operated in order to provide its clients with billing services. Accordingly, the court granted summary judgment to CCBill under the Section 512(a) safe harbor.[2043]

The Ninth Circuit's Decision.

Perfect 10 appealed the rulings that CCBill and CWIE qualified for immunity under the Section 512 safe harbors. Turning first to the threshold question of whether CCBill and CWIE had reasonably implemented a policy for termination of repeat infringers, the Ninth Circuit ruled that a service provider "implements" a policy "if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications."[2044] The court

---

[2040] Id. at 1099-1100.

[2041] Id. at 1100-01.

[2042] Id. at 1101.

[2043] Id. at 1102-03.

[2044] Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir.), cert. denied, 2007 U.S. LEXIS 12812 (2007).

noted that the statute permits service providers to implement a variety of procedures, "but an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright."[2045]

The Ninth Circuit agreed with the district court's rejection of Perfect 10's argument that CCBill and CWIE had prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters. Citing the Ellison and Aimster cases, the court ruled that, although substantial failure to record webmasters associated with allegedly infringing websites could raise a genuine issue of material fact as to the implementation of the service provider's repeat infringer policy for purposes of summary judgment, in this case the record did not reflect such a failure. Perfect 10 had submitted a single page from CCBill's and CWIE's "DMCA Log" showing some empty fields in the spreadsheet column labeled "Webmasters Name," and argued that this page showed no effort to track notices of infringements received by webmaster identity. The court noted, however, that the remainder of the DMCA Log indicated that the email address and/or name of the webmaster was routinely recorded in CCBill's and CWIE's DMCA Log, and CCBill's interrogatory responses also contained a chart indicating that CCBill and CWIE largely kept track of the webmaster for each website. Accordingly, the district court had properly concluded that the DMCA Log did not raise a triable issue of fact that CCBill and CWIE did not implement a repeat infringer policy.[2046]

With respect to whether CCBill and CWIE had reasonably implemented their repeat infringer policies, the Ninth Circuit first noted that to identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.[2047] Perfect 10 argued that CCBill's and CWIE's implementation of their repeat infringer policies was unreasonable because that had received notices of infringement from Perfect 10, yet the infringement identified in the notices continued. The Ninth Circuit, however, agreed with the district court's rulings that such notices did not substantially comply with the requirements of Section 512(c)(3). To be substantially compliant, a notice from a copyright holder must substantially comply with all of Section 512(c)(3)'s clauses, not just some of them.[2048]

Specifically, the court noted that a 22,185 page set of notices including pictures with URLs of Perfect 10 models allegedly posted on CCBill or CWIE client websites did not contain a statement under penalty of perjury that the complaining party was authorized to act, as required by Section 512(c)(3)(A)(vi). Other notices sent by Perfect 10 similarly had one or more of the required elements missing. The court noted that a copyright holder should not be permitted to cobble together adequate notice from separately defective notices.[2049] "The DMCA notification procedures place the burden of policing copyright infringement – identifying the potentially infringing material and adequately documenting infringement – squarely on the owners of the

---

[2045] Id. at 758-59.

[2046] Id. at 759-60.

[2047] Id. at 760.

[2048] Id. at 760-61.

[2049] Id. at 761-62.

copyright. We decline to shift a substantial burden from the copyright owner to the provider; Perfect 10's separate communications are inadequate."[2050]

The Ninth Circuit disagreed, however, with the district court's refusal to consider evidence of notices provided by any party other than Perfect 10 on the basis that such notices would be irrelevant to Perfect 10's claims. The court held that CCBill's and CWIE's actions toward copyright holders who were not a party to the litigation would be relevant in determining whether CCBill and CWIE reasonably implemented their repeat infringer policies. Accordingly, the court remanded for determination of whether CCBill and/or CWIE implemented its repeat infringer policy in an unreasonable manner with respect to any copyright holder other than Perfect 10.[2051]

The court next noted that, in importing the knowledge standards of Section 512(c) to the analysis of whether a service provider reasonably implemented its Section 512(i) repeat infringer policy, Congress had also imported the "red flag" test of Section 512(c)(1)(A)(ii). Perfect 10 argued that CCBill and CWIE had failed to reasonably implement their repeat infringer policy because they were aware of a number of red flags that signaled apparent infringement and had failed to act. Specifically, Perfect 10 argued that, because CCBill and CWIE had provided services to "illegal.net" and "stolencelebritypics.com," they must have been aware of apparent infringing activity.[2052] The Ninth Circuit disagreed. "When a website traffics in pictures that are titillating by nature, describing photographs as 'illegal' or 'stolen' may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider."[2053]

The court also rejected Perfect 10's argument that password-hacking sites hosted by CWIE obviously infringed. The court noted that, in order for a website to qualify as a red flag of infringement, it would need to be apparent that the website instructed or enabled users to infringe another's copyright.[2054] "We find that the burden of determining whether passwords on a website enabled infringement is not on the service provider. The website could be a hoax, or out of date. … There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on services providers. Password hacking websites are thus not *per se* 'red flags' of infringement."[2055]

Perfect 10 argued that CCBill and CWIE had also failed the predicate condition of Section 512(i)(1)(B) of not interfering with standard technical measure used to identify or protect

---

[2050] Id. at 762.

[2051] Id. at 762-63.

[2052] Id. at 763.

[2053] Id.

[2054] Id.

[2055] Id. at 763-64.

copyrighted works, by blocking Perfect 10's access to CCBill affiliated websites in order to prevent Perfect 10 from discovering whether those websites infringed Perfect 10's copyrights. The Ninth Circuit found two disputed facts at issue for purposes of summary judgment. First, the court was unable to determine on the record whether accessing websites is a standard technical measure that was developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process, as required by Section 512(i)(2)(A). Second, even if it were a standard technical measure, CCBill claimed it blocked Perfect 10's credit card only because Perfect 10 had previously reversed charges for subscriptions. Perfect 10 insisted it did so in order to prevent Perfect 10 from identifying infringing content. If CCBill were correct, Perfect 10's method of identifying infringement – forcing CCBill to pay the fines and fees associated with chargebacks – might well impose a substantial cost on CCBill. If not, CCBill might well have interfered with Perfect 10's efforts to police the websites in question for possible infringements. Accordingly, the court remanded to the district court for determinations on whether access to a website is a standard technical measure, and if so, whether CCBill's refusal to process Perfect 10's transactions interfered with that measure for identifying infringement.[2056]

Finally, the court turned to issues of whether CCBill and CWIE were entitled to the Section 512(a) safe harbor. Agreeing with the district court, the Ninth Circuit rejected Perfect 10's argument that CCBill was not eligible for immunity under Section 512(a) because it did not itself transmit the infringing material. The court noted that Section 512(a) provides a broad grant of immunity to service providers whose connection with the infringing material is transient. In the course of an Internet transmission of information through multiple computers, all intervening computers provide transient connections among users. The court read Section 512(a) to grant immunity to all service providers for transmitting all online communications, not just those that directly infringe.[2057]

The court noted that CCBill transmitted credit card information and proof of payment, both of which were digital online communications. However, there was little information in the record as to how CCBill sent the payment it received to its account holders, and it was unclear whether such payment was a digital communication, transmitted without modification to the content of the material, or was transmitted often enough such that CCBill was only a transient holder. Accordingly, on the record before it, the court ruled that it could not conclude that CCBill was a service provider under Section 512(a), and remanded to the district court for further consideration of the issue.[2058]

e. Columbia Pictures v. Fung

In Columbia Pictures Industries, Inc. v. Fung,[2059] the defendants operated BitTorrent sites through which users could search indexes for dot-torrent files pointing to infringing movies and

[2056] Id. at 764.

[2057] Id. at 765.

[2058] Id.

[2059] 2009 U.S. Dist. LEXIS (C.D. Cal. Dec. 21, 2009).

other content. The court found the defendants liable for inducement of infringement and rejected assertion of a safe harbor under Section 512(a) – because of the way the BitTorrent protocol worked, infringing materials did not pass through the defendants' system, which the court ruled was a prerequisite for the Section 512(a) safe harbor.[2060]

(ii) Caching – Section 512(b)

Section 512(b) provides that a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for caching (i.e., what Section 512(b) calls the "intermediate and temporary storage") of material on a system or network operated by the Service Provider which was made available online by a person other than the Service Provider.[2061] Such caching must occur through an automatic technical process upon the original

---

[2060] Id. at *60 n.26.

[2061] Section 512(b) provides: "(1) Limitation on liability – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of the other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions – The conditions referred to in paragraph (1) are that –

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

transmission of such material to a requester, in order to make the material available to subsequent persons requesting it from the person who first made it available online. Thus, the literal language of Section 512(b) appears not to cover "advance" caching, in which material is copied into a cache for anticipated requests for it, rather than upon the first actual request for it,[2062] although the case of Field v. Google, discussed in the next subsection, reached a contrary result.

In addition, the safe harbor requires that the Service Provider must (i) not modify the cached material; (ii) comply with all rules of the originator of the material for refreshing, reloading or other updating of the cached material in accordance with a generally accepted industry standard data communications protocol (provided such rules are not used by the originator to unreasonably impair intermediate storage); (iii) not interfere with any technology associated with the cached material that returns information to the originator (such as cookies) that would have been obtained in the absence of transmission through caching (provided such technology does not interfere with the performance of the system or network, is consistent with accepted industry standard communications protocols, and does not extract other information from the system or network); (iv) if the originator has conditioned access to the information, such as upon payment of a fee or provisions of a password, permit access to the cached information "in significant part"[2063] only upon the same conditions; and (v) respond expeditiously to remove or disable access to any cached information upon receipt of notice that such information has been removed or disabled from the originating site (or ordered by a court to be removed) from which the information was cached.

a. Field v. Google

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if –

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled."

[2062] See also H.R. Rep. No. 105-551 Part 2, at 52 (1998): "For subsection (b) to apply, the material must be made available on an originating site, transmitted at the direction of another person through the system or network operated by or for the service provider to a different person, and stored through an automatic technical process so that users of the system or network who subsequently request access to the material from the originating site may obtain access to the material from the system or network."

[2063] This language appears to have been inserted in recognition of the fact that hackers or others may be able to circumvent such restrictions on access without knowledge of the Service Provider. Id. at 7.

The facts of the case of Field v. Google[2064] are set forth in Section III.B.4(a) above. In that case, the court ruled that Google was entitled to the Section 512(b) safe harbor for its activities of caching web sites through its Web crawler known as the "Googlebot" and making the cached copies of particular pages available for download directly from Google's computers by end users clicking on the "Cached" link to a web page contained in search results returned by Google's search engine.

The court rejected a number of arguments by the plaintiff, Field, concerning why Google should not be entitled to the Section 512(b) safe harbor. First, Field contended that, in operating its cache, Google did not make "intermediate and temporary storage" of the cached material, as required by Section 412(b)(1). The court cited the Ellison v. Robertson case,[2065] involving the Section 512(a) safe harbor, which ruled that AOL's storage of Usenet postings for about 14 days was both "intermediate" and "transient" as required by Section 512(a). Analogizing to that case, the court noted that the copy of Web pages Google stored in its cache were present for approximately 14 to 20 days. The court found that this period was sufficiently short to be deemed "temporary" under Section 512(b).[2066]

In a significant aspect of its ruling, the court also implicitly held that, to qualify for the Section 512(b) safe harbor, the caching need not be done only after a user has made an initial request for the materials being cached, but could be done in anticipation of user requests for the materials: "Like AOL's repository of Usenet postings in Ellison which operated between the individuals posting information and the users requesting it, Google's cache is a repository of material that operates between the individual posting the information, and the end-user requesting it."[2067]

Field also contended that Google's cache did not satisfy the requirements of Section 512(b)(1)(B) that the material in question be transmitted from the person who makes it available online, here the plaintiff, to a person other than himself, at the direction of the other person.[2068] The court rejected this argument: "Field transmitted the material in question, the pages of his Web site, to Google's Googlebot at Google's request. Google is a person other than Field. Thus, Google's cached meets the requirement of Section 512(b)(1)(B)."[2069] Here the court appears to have misidentified the parties that Section 512(b)(1)(B) is directed to, although the misidentification would not seem to change the conclusion that Section 512(b)(1)(B) is satisfied. Specifically, the court's quoted language treats Google as the "other person." However, because Google is acting as the service provider, it should not be treated as the "other person." Rather, Google's users are the "other persons" to whom Section 512(b)(1)(B) appears to be directed.

[2064] 412 F. Supp. 2d 1106 (D. Nev. 2006).

[2065] 357 F.3d 1072, 1081 (9th Cir. 2004).

[2066] Field v. Google, 412 F. Supp. 2d at 1124.

[2067] Id.

[2068] Id.

[2069] Id.

Finally, Field contended that Google's cache did not fully satisfy the requirements of Section 512(b)(1)(C) requiring that Google's storage of Web pages be carried out through "an automated technical process" and be "for the purpose of making the material available to users … who … request access to the material from [the originating site]."[2070] The court rejected this argument, noting that Field's complaint stated that third party web page content was added to the Google cache by an automated software process. Nor was there any dispute that one of Google's principal purposes in including Web pages in its cache was to enable subsequent users to access those pages if they were unsuccessful in requesting the materials from the originating site for whatever reason, which was sufficient to meet the requirements of Section 512(b)(1)(C). Accordingly, the court granted Google's motion for partial summary judgment that it qualified for the Section 512(b) safe harbor.[2071]

b. Parker v. Google

In Parker v. Google,[2072] the court ruled, citing Field v. Google, that Google had immunity under Section 512(b) for claims of direct infringement based on Google's automatic caching of USENET messages, including an excerpt of the plaintiff's copyrighted work that he had posted to USENET, as a means of indexing web sites and producing results to search queries.[2073] Similar to Field v. Google, the court did not impose any requirement that, to qualify for the Section 512(b) safe harbor, the caching must be done only after a user has made an initial request for the materials being cached, but rather could be done in anticipation of user requests for the materials.

c. Perfect 10 v. Google

In Perfect 10 v. Google,[2074] Perfect 10 alleged that Google infringed on its copyrights in pictures of nude models by caching portions of websites that hosted infringing images, by linking to third party websites that hosted infringing images, and by hosting infringing images on its own servers that had been uploaded by users of Google's "Blogger" service. On remand from the Ninth Circuit with respect to issues of common law secondary liability and fair use (see discussion in Section II.C.4 above), Google moved for summary judgment that it was entitled to the safe harbors under Sections 512(b), (c) and (d).[2075]

The court first turned to the preliminary issues of whether Google satisfied the safe harbor threshold condition of implementation of a suitable repeat infringer policy and whether Perfect 10's notices were adequate. With respect to a suitable repeat infringer policy, Google had a system for receiving and processing notifications of infringement and would terminate an

---

[2070] Id.

[2071] Id. at 1124-25.

[2072] 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS (3d Cir. July 10, 2007).

[2073] Id. at 497-98. The issue of immunity under Section 512(b) was not addressed by the Third Circuit on appeal.

[2074] 2010 U.S. Dist. LEXIS 75071 (C.D. Cal. July 26, 2010).

[2075] Id. at *2-3.

account holder on its Blogger service if it determined that three DMCA notices of infringement against that blogger were valid.[2076] With respect to its Web Search and Image Search services, Google did not have account holders, but that fact did not eliminate eligibility for the safe harbors: "Google points out – and P10 does not dispute – that Web Search, Image Search, and the caching feature do not have account holders or subscribers. P10 does not contend that Google must, or even can, have a repeat infringer policy for those services. *See 17 U.S.C. § 512(i)(1)(A)* (requiring a repeat infringer policy for those services with 'subscribers and account holders')."[2077] The court rejected a challenge by Perfect 10 to the adequacy of Google's repeat infringer policy with respect to the Blogger service based on the fact that Google tracked only email addresses, not the actual names of users. The court held that the DMCA does not impose an obligation on service providers to track their users in any particular way.[2078]

Turning to Google's assertion of the Section 512(b) safe harbor, the court noted that it was undisputed that Google's cache servers did not store images found on a cached page, only the text – images displayed on a cached page were made available to a viewer by links to their original source, if they still existed at that source. Accordingly, Perfect 10's claims for infringement based on images "located in" Google's cache were really claims based on Google's linking to outside infringing content, to which the Section 512(d) safe harbor would be relevant.[2079] In any event, the court noted that in none of Perfect 10's relevant notices of infringement did it identify any specific material in Google's cache as infringing, so its notices were deficient as to the cached pages. The court also rejected Perfect 10's argument that a notice identifying a web page necessarily identifies the cached page as well. Accordingly, the court ruled that it need not decide whether Google would be separately entitled to the Section 512(b) safe harbor for its caching activity, in addition to the Section 512(d) safe harbor for linking to allegedly infringing images through its cached pages.[2080]

Turning to the applicability of the Section 512(d) safe harbor to Google's Web Search and Image Search services, the court examined in detail the adequacy under DMCA requirements of Perfect 10's notices of infringement.[2081] The litigants divided those notices into Groups A, B, and C, based on when they were sent to Google. The Group A notices were all sent by email to webmaster@google.com instead of to the address of Google's designated agent listed at the Copyright Office and were otherwise deficient for not identifying specifically which

---

[2076] Id. at *7, 13.

[2077] Id. at *13.

[2078] Id. at *14.

[2079] Id. at *5-6, 37.

[2080] Id. at *38 & n.10, 45.

[2081] Perfect 10 did not argue that Google received a direct financial benefit from the infringing activity, had the right and ability to control such activity, and thus could not enjoy safe harbor protection for its web and image search results. Id. at *20.

copyrighted works were infringed. Accordingly, the Group A notices were inadequate to disqualify Google from the Section 512(d) safe harbor.[2082]

With respect to the Group B notices, the court held that Google had not met its burden of showing that there was no dispute of material fact as to whether these notices were valid under the DMCA. Each notice contained references to dozens or even hundreds of alleged infringing links. Google argued that the notices were invalid in their entirety because the majority of the references were invalid since they contained incomplete URLs, lacked image-specific URLs, or did not reference the copyrighted work with specificity. The court agreed that references having those deficiencies did not confer adequate notice under the DMCA and Google was not required to act to remove any entry that did not meet the DMCA requirements. However, other Group B notices did meet all of the requirements of the DMCA, such as one that contained a complete URL along with the volume, issue, and page number of the *Perfect 10* magazine in which the image originally appeared. The court noted that the Group B notices enabled Google to scan the entries to determine their compliance with the DMCA and it would not be an undue burden on Google to do so. In addition, Perfect 10 offered evidence that in some instances Google waited between four and seventeen months to process a number of the Group B notices, as well as evidence that some notices were not processed at all.[2083] Accordingly, the court denied Google's motion for summary judgment "as to safe harbor for at least some of the Group B notices."[2084] Significantly, this statement suggests that the DMCA safe harbors are to be applied on a notice-by-notice basis.

The Group C notices, like those notices at issue in the Ninth Circuit's CCBill case, required Google to move back and forth between several different files in order to determine whether a given URL was infringing. The Group C notices generally consisted of a cover letter, a spreadsheet, and a hard drive or DVDs containing electronic files. Where Perfect 10 provided spreadsheets, the spreadsheets did not identify the infringing URL, but merely the top-level URL for the entire website. The court noted that Perfect 10 apparently expected Google to comb through hundreds of nested electronic folders containing over 70,000 distinct files, including raw image files such as JPEG files and screen shots of Google search results, in order to find which link was allegedly infringing. In many cases, the file containing the allegedly infringing image did not even include a URL, or the URL was truncated. The spreadsheets also did not identify the copyrighted work that was allegedly infringed – Google would have been required to search through a separate electronic folder supplied by Perfect 10 with its cover letter to the notice of infringement containing all of the more than 15,000 images that appeared on Perfect 10's website as of June 2007, in order to identify the copyrighted work that was infringed. Thus, no single document of any of the Group C notices contained all of the information required in a valid DMCA notification, and the court ruled that the Group C notices were therefore deficient. Accordingly, the court concluded that Perfect 10 had not raised a genuine issue of material fact

---

[2082] Id. at *22.

[2083] Id. at *22-26.

[2084] Id. at *27.

as to whether Google was eligible for safe harbor under Section 512(d) with respect to the Group C notices.[2085]

Next, the court turned to whether Google was entitled to the Section 512(c) safe harbor with respect to its Blogger service, which some of its account holders had used to upload allegedly infringing images onto Google's servers. With respect to the Group B notices, the court noted that Perfect 10 had not contended in either its opposition papers or in oral argument that Google had failed to expeditiously process even a single Blogger URL identified within the Group B notices. With respect to the Group C notices, the court noted that the requirements for a copyright holder are slightly less stringent under Section 512(c) than under Section 512(d) in that the former does not explicitly require the copyright holder to provide what the latter does, a specific "identification of the reference or link" to material or activity claimed to be infringing. Section 512(c) merely requires the copyright holder to provide "identification of the material that is claimed to be infringing … and information reasonably sufficient to permit the service provider to locate the material." Nevertheless, the court noted that Google had a tenable argument that a copyright holder would need to provide the post-URL of a particular Blogger post in order to constitute information "reasonably sufficient" to permit the location of the material. However, the court decided it need not address that argument, since the other manifest deficiencies in the Group C notices – including the lack of specific identification of the copyrighted material and their unduly complicated organization – prevented them from imparting knowledge under the statute.[2086]

Finally, the court addressed whether Google was ineligible for the Section 512(c) safe harbor because it received a financial benefit directly attributable to infringing activity that Google had the right and ability to control. Perfect 10's only argument that Google had a right and ability to control the infringing activity on Blogger was that the infringing material was on Google's servers and Google could take it down. The court ruled that the mere ability of a service provider to remove content after it had been uploaded was insufficient as a matter of law to establish the right and ability to control infringing activity. Accordingly, Google had demonstrated that it was entitled to the Section 512(c) safe harbor for its Blogger service as a matter of law.[2087]

In sum, the Court granted in part and denied in part Google's motion for partial summary judgment of entitlement to safe harbor under Section 512(d) for its Web and Image Search, granted Google's motion for partial summary judgment for its caching feature based on Section 512(d), without having to assess whether it would be separately entitled to safe harbor under Section 512(b), and granted Google's motion for partial summary judgment of entitlement to safe harbor under Section 512(c) for its Blogger feature.[2088]

[2085] Id. at *27-36.

[2086] Id. at *40-43.

[2087] Id. at *43-44.

[2088] Id. at *45.

The district court also denied Perfect 10's motion for a preliminary injunction on the basis that it had not shown it was likely to suffer irreparable harm in the absence of such relief, and that it had failed to satisfy any of the other requirements for a preliminary injunction.[2089] On appeal, Perfect 10 claimed the district court erred in denying its motion for a preliminary injunction and sought review of the district court's summary judgment order under the safe harbors, arguing that the order was inextricably intertwined with its request for a preliminary injunction.[2090]

The Ninth Circuit affirmed the district court's denial of a preliminary injunction. First, the court ruled that, following the Supreme Court's decision in eBay Inc. v. MercExchange, LLC,[2091] "the propriety of injunctive relief in cases arising under the Copyright Act must be evaluated on a case-by-case basis in accord with traditional equitable principles and without the aid of presumptions or a 'thumb on the scale' in favor of issuing such relief."[2092] Although eBay dealt with a permanent injunction, the Ninth Circuit concluded that the rule enunciated in that case is equally applicable to preliminary injunctive relief.[2093] The court then affirmed the district court's denial of a preliminary injunction because Perfect 10 had not shown a sufficient causal connection between its business harm and Google's operation of its search engine. Perfect 10 argued that its revenues had declined from nearly $2 million per year to less than $150,000 per year during the period in which thumbnails of Perfect 10's images had become more widely available through Google's search engine, and that Perfect 10 was very close to bankruptcy. The Ninth Circuit held this was insufficient evidence to establish that failure to enjoin Google's operations would cause Perfect 10 irreparable harm. First, Perfect 10 had not alleged that it was ever in sound financial shape, and the company's president and founder acknowledged that search engines other than Google contributed to making Perfect 10 images freely available. In addition, Perfect 10 had failed to submit a statement from even a single former subscriber who ceased paying for Perfect 10's service because of the content freely available via Google. Accordingly, the Ninth Circuit affirmed the denial of a preliminary injunction.[2094]

(iii) Innocent Storage of Infringing Information – Section 512(c)

Section 512(c) provides that a service provider is not liable for monetary relief, and is subject only to limited injunctive relief, for storage at the direction of a user of infringing material on its system or network where the service provider does not have actual knowledge that the material is infringing; is not aware of facts or circumstances from which infringing activity is apparent; does not receive a financial benefit directly attributable to any infringing

---

[2089] Perfect 10, Inc. v. Google, Inc., 653 F.3d 976, 978 (9th Cir. 2011), cert. denied, 132 S. Ct. 1713 (2012).

[2090] Id.

[2091] 547 U.S. 388 (2006).

[2092] Perfect 10 v. Google, 653 F.3d at 980. The Ninth Circuit was persuaded by the Second Circuit's reasoning when it reached the same conclusion in the case of Salinger v. Colting, 607 F.3d 68, 75, 79 (2d Cir. 2010).

[2093] Perfect 10 v. Google, 653 F.3d at 981.

[2094] Id. at 981-82.

activity for which it has the right and ability to control; and, if properly noticed of the infringing activity by the copyright holder or its authorized agent, or otherwise obtaining knowledge or awareness of the infringement, responds expeditiously to remove or disable access to the infringing material.[2095]

The service provider can become aware of infringing activity either by notice from the copyright holder (or its authorized agent) or by virtue of other facts or circumstances of which it becomes aware. Absent direct notice from the copyright holder or its agent, the standard of awareness of infringing activity appears by its terms to require more knowledge on the part of the service provider than a "should have known" (or reason to know) standard. Specifically, it requires that the service provider have actual awareness of facts from which infringing activity is apparent. The legislative history describes the standard of awareness as a "red flag" test. "[I]f the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The 'red flag' test has both a subjective and an objective element. In determining whether the service provider was aware of a 'red flag,' the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a 'red flag' – in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances – an objective standard should be used."[2096]

Section 512(c)(3) specifies the requirements for proper notice of infringement by the copyright holder to the Service Provider, which constitutes a written communication provided to the designated agent of the Service Provider that includes "substantially" the following:[2097]

[2095] Section 512(c) provides: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider –

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."

[2096] H.R. Rep. No. 105-551 Part 2, at 53 (1998).

[2097] Section 512(c)(3) provides: "Elements of notification –

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

- identification of the copyrighted work or a representative list of works at the site (if multiple copyrighted works at a single online site are covered by a single notification);[2098]

- identification of the infringing material in sufficient detail to permit the Service Provider to locate the material;

- information (including an e-mail address) where the complaining party can be contacted; and

- a statement signed by physical signature or electronic signature under penalty of perjury that the complaining party has the authority to enforce the rights that are claimed to be infringed and a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

Section 512(c)(3)(B)(ii) provides that, if a notice complies with at least the first three of the preceding requirements, then in order to take advantage of the safe harbor, the Service Provider must promptly attempt to contact the complaining party or take other reasonable steps to assist in

---

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A)."

[2098] A notice may cover multiple works: "Where multiple works at a single on-line site are covered by a single notification, a representative list of such works at that site is sufficient." H.R. Rep. No. 105-551 Part 2, at 55 (1998); see 17 U.S.C. § 512(c)(3)(A)(ii). What constitutes an adequate "representative list" of works was adjudicated in the case of ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), discussed below.

the receipt of notification that substantially complies with all the preceding requirements for notice.

The DMCA does not define what constitutes a "direct financial benefit" from the infringing activity, but presumably the mere receipt of monthly subscription fees from the infringing user would not be a "direct" financial benefit from the infringing activity.[2099] It is also unclear what constitutes sufficient "right and ability to control" the infringing activity. Most Service Providers impose certain rules on the users of their system, but, as a practical matter, do not and are not able to control the myriad individual actions of users of the system. The same phrase – "right and ability to control" – appears in the safe harbor of Section 512(d) as well, which was asserted in the Napster case, as discussed in subsection (iv) below.

Finally, to take advantage of this safe harbor, the OSP must designate an agent to receive notifications of claimed infringements and make available the contact information for such agent through its service and through the U.S. Copyright Office. The specifics for designation of such agent are set forth in subsection (6) below.

Several cases have interpreted and adjudicated the scope of the Section 512(c) safe harbor:

a. The ALS Scan Case – What Constitutes a "Substantially" Compliant Notice

The issue of what constitutes a "substantially" compliant notice under Section 512(c)(3) was addressed in the case of ALS Scan, Inc. v. RemarQ Communities, Inc.[2100] In that case, the defendant RemarQ was an OSP that provided access to its members to over 30,000 newsgroups. RemarQ did not monitor, regulate, or censor the content of articles posted in the newsgroups, but did have the ability to filter information contained in the newsgroups and to screen its members from logging onto certain newsgroups, such as those containing pornographic material.[2101] The plaintiff ALS Scan, Inc. (ALS Scan) was in the business of creating and marketing "adult" photographs. The plaintiff discovered that two newsgroups on the RemarQ service – both of which had "als" in their titles (alt.als and alt.binaries.pictures.erotica.als) – contained virtually nothing other than unauthorized photographs owned by ALS Scan. ALS Scan sent a cease and

---

[2099] "In general, a service provider conducting a legitimate business would not be considered to receive a 'financial benefit directly attributable to the infringing activity' where the infringer makes the same kind of payment as noninfringing users of the provider's service. Thus, receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity.' Nor is subsection (c)(1)(B) intended to cover fees based on the length of the message (e.g., per number of bytes) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material." H.R. Rep. No. 105-551 Part 2, at 54 (1998).

[2100] 239 F.3d 619 (4th Cir. 2001).

[2101] Id. at 620.

desist letter to RemarQ, demanding that RemarQ block access to both of the newsgroups at issue.[2102]

RemarQ responded by refusing to comply with ALS Scan's demand but advising ALS Scan that RemarQ would eliminate individual infringing items from the newsgroups if ALS Scan identified them "with sufficient specificity."[2103] ALS Scan filed suit, alleging copyright infringement and violations of Title II of the DMCA. In response, RemarQ filed a motion to dismiss the complaint or, in the alternative, for summary judgment, and attached affidavits stating that it was prepared to remove articles posted in its newsgroups if the allegedly infringing articles were specifically identified as required by the DMCA. The district court dismissed the complaint, ruling that RemarQ could not be liable for contributory infringement because ALS Scan failed to comply with the notice requirements of Section 512(c)(3)(A) of the DMCA.[2104]

On appeal, ALS Scan contended that it "substantially" complied with the notice requirements of the DMCA and that it therefore put RemarQ sufficiently on notice of infringement activities that RemarQ lost its immunity under the DMCA by failing to remove the infringing material. RemarQ argued in response that it did not have knowledge of the infringing activity as a matter of law because ALS Scan failed to identify the infringing works as required by the DMCA, and RemarQ was entitled to the safe harbor provisions of the DMCA.[2105]

The Fourth Circuit reversed on two grounds. First, the court noted that, in order to be entitled to the safe harbor of Section 512(c), an OSP must satisfy all three of the safe harbor requirements of Section 512(c)(1), specifically, that: (i) it has neither actual knowledge that its system contains infringing materials nor awareness of facts or circumstances from which infringement is apparent, or it has expeditiously removed or disabled access to infringing material upon obtaining actual knowledge of infringement; (ii) it receives no financial benefit directly attributable to infringing activity; and (iii) it responded expeditiously to remove or disable access to material claimed to be infringing after receiving notice from the copyright holder conforming to the requirements of Section 512(c)(3). The Fourth Circuit held that "a showing under the first prong – the lack of actual or constructive knowledge – is prior to and separate from the showings that must be made under the second and third prongs."[2106] The Fourth Circuit noted that, although it had treated RemarQ's motion as a motion to dismiss, rather than as a motion for summary judgment, it had failed to take into account the allegation in the complaint that RemarQ had actual knowledge of the infringing nature of the two newsgroups even before being contacted by ALS Scan. Although this allegation was denied by RemarQ, the Fourth Circuit noted that the district court was required to accept the allegation as true for purposes of testing the adequacy of the complaint under F.R.C.P. 12(b)(6).[2107]

[2102] Id.

[2103] Id. at 621.

[2104] Id.

[2105] Id. at 622.

[2106] Id. at 623.

[2107] Id.

Second, whether or not RemarQ's motion was treated as one to dismiss or for summary judgment, the Fourth Circuit held that ALS Scan had substantially complied with the notice requirement of the third prong. The district court had found that ALS Scan's notice failed to comply with two of the six requirements of notification – namely, that the notice include a list of infringing works on the RemarQ site and that the notice identify the infringing works in sufficient detail to enable RemarQ to locate and disable them (per Section 512(c)(3)(A)(ii) & (iii)).[2108]

The Fourth Circuit disagreed, noting that under Section 512(c)(3)(A), a notice need comply with the prescribed format only "substantially," and under Section 512(c)(3)(A)(ii), a copyright holder need only provide a "representative" list of infringed works on the site.[2109] The court stated: "This subsection specifying the requirements of a notification does not seek to burden copyright holders with the responsibility of identifying every infringing work – or even most of them – when multiple copyrights are involved. Instead, the requirements are written so as to reduce the burden of holders of multiple copyrights who face extensive infringement of their works. Thus, when a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements."[2110]

The Fourth Circuit found that on the particular facts of the case, ALS Scan's notice constituted an adequate representative list of infringed works and substantially complied with the DMCA notice requirements:

> In this case, ALS Scan provided RemarQ with information that (1) identified two sites created for the sole purpose of publishing ALS Scan's copyrighted works, (2) asserted that virtually all the images at the two sites were its copyrighted material, and (3) referred RemarQ to two web addresses where RemarQ could find pictures of ALS Scan's models[2111] and obtain ALS Scan's copyright information. In addition, it noted that material at the site could be identified as ALS Scan's material because the material included ALS Scan's 'name and/or copyright symbol next to it.' We believe that with this information, ALS Scan substantially complied with the notification requirement of providing a

---

[2108] Id. at 621.

[2109] Id. at 625.

[2110] Id.

[2111] It is curious that the Fourth Circuit found the supplied Web address where RemarQ could find pictures of ALS Scan's models to aid ALS Scan's argument that RemarQ had adequate notice of what particular infringing photographs were contained on RemarQ's site. The referenced Web address contained adult "teaser" photos of the ALS Scan models. There is nothing in the opinion of the court indicating that the "teaser" photos were the actual ones allegedly on the RemarQ site. Rather, the argument seems to be that the "teaser" photos would identify what the ALS Scan models looked like. Is the Fourth Circuit implying that RemarQ then bore the burden to go look at the photos on the newsgroups at issue to see if they contained pictures of the same humans as those in the "teaser" photos? Perhaps the truly key facts were that the infringing photos in the newsgroups were identified with ALS Scan's name and/or copyright notice and they were all contained in one "place" – namely, a couple of particular newsgroups almost entirely devoted to ALS Scan photos.

representative list of infringing material as well as information reasonably sufficient to enable RemarQ to locate the infringing material.[2112]

Because RemarQ had received adequate notice of infringement and had failed to act to remove the infringing material, it was not entitled to the safe harbor of the DMCA.[2113] The Fourth Circuit observed that the immunity of the DMCA "is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence; i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing material …."[2114] The Fourth Circuit remanded the case for further proceedings on ALS Scan's copyright infringement claims and any other affirmative defenses that RemarQ might have.[2115]

There are a few lessons to be learned from the ALS Scan case. First, where multiple copyrighted works are allegedly infringed, a copyright holder need not specifically identify all particular instances of infringing material at the site in order to give adequate notice to the Service Provider sufficient to give rise to a duty on its part to act in order to preserve the DMCA safe harbors. Second, at least in the specific factual scenario where all the allegedly infringing material is contained in a single area such as a newsgroup, and the area comprises almost all infringing material, the Service Provider may need to remove or block access to the entire area as a precaution to preserve the safe harbor. It might have been sufficient for RemarQ to have removed or blocked access only to those photos within the newsgroups that bore ALS Scan's name or copyright notice (the opinion does not address this question) – but even if so, it appears that the Fourth Circuit may have contemplated that RemarQ, and not ALS Scan, would bear the burden of identifying the individual photos for removal or blocking access to. Third, the decision suggests that a Service Provider may not be wise to rely on certain failures on the part of a copyright holder to comply with all the technical notice requirements of Section 512(c)(3) as a basis for not having to act to remove or block allegedly infringing material. If a court later determines that the notice was "substantially" compliant, the Service Provider may have lost its DMCA safe harbor by failing to act.

In sum, the ALS Scan case reflected a rather low threshold of knowledge of infringing activity, at least under the specific facts of the case, and a rather lax application of the technical notice requirements of Section 512(c). The net effect of these rulings was to make the Section 512(c) safe harbor rather fragile for the OSP. Subsequent cases have given the Section 512(c) safe harbor a stronger reading in favor of the OSP and have insisted on a stricter compliance with the technical notice requirements on the part of the copyright holder:

[2112] Id.

[2113] Id. at 625-26.

[2114] Id. at 625.

[2115] Id. at 626.

b. Hendrickson v. eBay

In Hendrickson v. eBay Inc.,[2116] the plaintiff Hendrickson, a pro se plaintiff, sought to hold defendant eBay Inc. secondarily liable for the sale through the eBay auction site of allegedly infringing copies of the documentary film "Manson" in DVD format. The plaintiff sent a cease and desist letter to eBay, which stated generally that pirated copies of "Manson" were being offered for sale on eBay, but did not explain which copies of "Manson" were infringing, nor did it identify the plaintiff's copyright interest. eBay responded by requesting that the plaintiff comply with the notice requirements of Section 512(c), and suggesting that the plaintiff submit a copy of eBay's "Notice of Infringement" form, which would comply with the notice requirements of the DMCA and would specify which particular item numbers (each listing on eBay's site had its own item number) were infringing so eBay could remove them. The plaintiff refused to submit the Notice of Infringement form or otherwise specify which particular items on eBay were allegedly infringing, and instead filed a copyright infringement lawsuit.[2117]

eBay asserted the safe harbor of Section 512(c) as a defense. The court began its analysis by noting that there was no dispute over whether eBay qualified as a "service provider" within the meaning of Section 512(k)(1)(B).[2118] The court noted that Section 512(c) was the appropriate safe harbor potentially applicable to eBay because that safe harbor applies to infringing "activity using the material on" an OSP's system.[2119]

The court then turned to an analysis of the issue of proper notice of infringement. Under Section 512(c)(1)(C), a service provider's duty to act to remove material that is the subject of infringing activity is "triggered only upon receipt of proper notice" substantially compliant with the required elements of notification set forth in Section 512(c)(3).[2120] As a preliminary matter, the court rejected the plaintiff's argument that he need not submit written notification in compliance with the notice requirements of Section 512(c)(3) "as long as other facts show the service provider received actual or constructive knowledge of infringing activity."[2121] The court replied that, under Section 512(c)(3)(B)(i), if the copyright holder's attempted notification fails to comply substantially with the elements of Section 512(c)(3), then the notification cannot be considered when evaluating whether the service provider had actual or constructive knowledge of the infringing activity.[2122]

Because the plaintiff admitted that he had not strictly complied with the notice requirements of Section 512(c)(3), the court turned to an analysis of whether his imperfect

---

[2116] 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

[2117] Id. at 1084-85.

[2118] Id. at 1088.

[2119] Id. (quoting 17 U.S.C. § 512(c)(1)(A)(i)).

[2120] 165 F. Supp. 2d at 1089.

[2121] Id.

[2122] Id.

attempt to give notice constituted "substantial" compliance, and ruled that it did not because his notice did not include several key elements for proper notification:

– There was no written statement attesting under penalty of perjury that the information in the notification was accurate and that the plaintiff was authorized to act on behalf of the copyright owner, or that the plaintiff had a good faith belief that use of the material in the manner complained of was not authorized. The court held that the plaintiff's complete failure to supply the preceding two elements, even after eBay specifically asked for them, rendered the plaintiff's notification of claimed infringement deficient under Section 512(c)(3).[2123]

– There was not sufficient information to identify the various listings on eBay that purportedly offered pirated copies of "Manson," and the plaintiff had refused to supply such information when specifically asked by eBay.[2124] The plaintiff contended that it was "not his job to do so once he has notified eBay of the existence of infringing activity by eBay sellers."[2125] The court rejected this argument, stating: "The Court recognizes that there may be instances where a copyright holder need not provide eBay with specific item numbers to satisfy the identification requirement. For example, if a movie studio advised eBay that all listings offering to sell a new movie (*e.g.*, 'Planet X,') that has not yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title 'Planet X' and identify the offensive listings. However, the record in this case indicates that specific item numbers were necessary to enable eBay to identify problematic listings."[2126]

– There was no written statement to eBay that all DVD copies of "Manson" were unauthorized copies. Although the plaintiff stated at oral argument that he had orally notified eBay that all copies of "Manson" in DVD format were unauthorized, this was insufficient because it was not in writing. "The writing requirement is not one of the elements listed under the substantial compliance category [of Section 512(c)(3)(A).] Therefore, the Court disregards all evidence that purports to show Plaintiff gave notice that all DVDs violate his copyright in 'Manson.'"[2127]

The court rejected two other arguments offered by the plaintiff concerning why he should not be required to supply eBay with specific item numbers of allegedly infringing copies. First, he argued that he had supplied eBay with user IDs of four alleged infringers, and the user IDs should be sufficient notice to locate the listings offering pirated copies of "Manson." The court ruled the notice of user IDs insufficient because the email containing the user IDs did not identify either the listings claimed to be the subject of infringing activity or describe the infringing activity, nor did it contain a statement attesting to the good faith and accuracy of the

---

[2123] Id. at 1089-90.

[2124] Id. at 1090.

[2125] Id.

[2126] Id.

[2127] Id. at 1091. Similarly, noting Plaintiff's admission that authorized copies of "Manson" had been released in VHS format, the Court ruled that the plaintiff had offered no explanation to eBay how it could determine which "Manson" VHS tapes being offered for sale were unauthorized copies. Id.

allegations.[2128] Second, the plaintiff argued that eBay could identify listings offering infringing copies without item numbers because eBay had previously removed two listings even though the plaintiff did not provide the item numbers. The court rejected this argument also, noting that the plaintiff had identified one of the sellers that eBay removed, who because it had only a single listing at the time of removal, eBay had removed out of an abundance of caution, and the record did not reflect why eBay removed the second listing.[2129]

In sum, the court ruled that proper identification under Section 512(c)(3)(A)(iii) should include the item numbers of the listings that were allegedly offering pirated copies of "Manson."[2130] Because the plaintiff had failed to submit a written notice substantially complying with the notice requirements of Section 512(c), eBay did not have a duty to act under Section 512(c)(1)(C) to remove the allegedly infringing listings, and would therefore be entitled to the Section 512(c) safe harbor if it met the remaining prongs of the safe harbor test:[2131]

– Absence of Actual or Constructive Notice: Because the plaintiff's notices did not substantially comply with the notice requirements of Section 512(c), the court ruled that they could not, as a matter of law, establish actual or constructive knowledge that particular listings were involved in infringing activity. Since the record showed that eBay otherwise did not have actual or constructive knowledge before the lawsuit was filed, the court ruled that eBay had satisfied the first prong of the safe harbor test under Section 512(c)(1)(A).[2132]

– Right and Ability to Control the Infringing Activity: Under Section 512(c)(1)(B), eBay was required to show that it did not receive a financial benefit directly attributable to the infringing activity in a case in which it had the right and ability to control such activity. The court ruled that, because the undisputed facts established that eBay did not have the right and ability to control the infringing activity, the court need not evaluate the financial benefit element.[2133] Plaintiff argued that eBay had the ability to control infringing activity based on its ability to remove infringing listings after receiving proper notification, and its program of prophylactic searching for apparent infringements based on searching its website daily for generic key words such as "bootleg," "pirated," "counterfeit" and "taped off TV" that might indicate potentially infringing activity.[2134] The court rejected these arguments, first noting the Catch 22 that would arise if the mere ability to remove infringing materials were sufficient to satisfy the control prong, since the DMCA requires an OSP to remove infringing materials:

> [T]he 'right and ability to control' the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or

---

[2128] Id.

[2129] Id. at 1091-92.

[2130] Id. at 1092.

[2131] Id.

[2132] Id. at 1093.

[2133] Id.

[2134] Id. at 1093 & n. 14.

> block access to materials posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. The DMCA also provides that the limitations on liability *only* apply to a service provider that has 'adopted and reasonably implemented … a policy that provides for the termination in appropriate circumstances of [users] of the service provider's system or network who are repeat infringers.' Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA."[2135]

Nor could eBay's voluntary practice of engaging in limited monitoring of its website for apparent infringements satisfy the control prong. The court cited a passage of the legislative history of the DMCA stating that courts "should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."[2136] Finally, the court noted that the infringing activity actually took place offline in the form of the sales and distribution of pirated copies of "Manson," and that eBay could not control such offline activity.[2137]

The court concluded that eBay had established that it met the test for the safe harbor under Section 512(c), and accordingly granted eBay summary judgment on the plaintiff's copyright claims.[2138]

Important Principles. The Hendrickson v. eBay case establishes a number of significant points about the Section 512(c) safe harbor. First, insofar as the OSP receives notice of alleged infringement on its system from the *copyright holder*, such notice must be in writing and must substantially comply with the technical notice requirements of Section 512(c). The OSP can, of course, receive actual or constructive notice through channels other than the copyright holder, but notice from the copyright holder must come in written form in order to trigger the OSP's duty to act on that information. The ALS Scan case is consistent on this point, since in the ALS Scan case, notice from the copyright holder was in writing. Second, the copyright holder bears the burden to identify specific instances of infringing activity on the system. It is insufficient to identify only the users who are committing allegedly infringing acts without further

---

[2135] Id. at 1093 (citations omitted).

[2136] Id. at 1094 (quoting House Report 105-796 at 73 (Oct. 8, 1998)).

[2137] 165 F. Supp. 2d at 1094. This is an interesting holding, since removing the listing from eBay's service would have had the derivative effect of controlling the ability of users to make offline purchases and distributions in the first place. The same rationale would seem to apply to the Napster service, in which Napster could not control whether its users elected to make downloads of allegedly infringing materials posted on the Napster index, which downloads did not pass through the Napster servers. Notwithstanding this fact, the district court in the Napster case, as discussed above, found that Napster did in fact have sufficient "control" over the infringing activity by virtue of its control over the listings in the Napster index.

[2138] Id. The court also held that eBay's immunity under the safe harbor extended to the plaintiff's claims against eBay employees. Id. at 1094-95.

identification of the infringing *materials* that are the subject of those acts. Third, neither the OSP's mere ability to terminate infringing users or activity, or the OSP's voluntary policing of its system or website, will of themselves be sufficient to establish "control" of the infringing activity for purposes of adjudicating the availability of the Section 512(c) defense.

c. CoStar v. LoopNet

In CoStar Group Inc. v. LoopNet, Inc.,[2139] the plaintiff CoStar maintained a copyrighted commercial real estate database that included photographs. The defendant LoopNet offered a service through which a user, usually a real estate broker, could post a listing of commercial real estate available for lease. The user would access, fill out, and submit a form for the property available. To include a photograph of the property, the user was required to fill out another form. The photograph would initially be uploaded into a separate folder on LoopNet's system, where it would first be reviewed by a LoopNet employee to determine that it was in fact a photograph of commercial property and that there was no obvious indication the photograph was submitted in violation of LoopNet's terms and conditions. If the photograph met LoopNet's criteria, the employee would accept it and post it along with the property listing. CoStar claimed that over 300 of its copyrighted photographs had been posted on LoopNet's site, and sued LoopNet for both direct and contributory copyright liability.[2140] The court entered a preliminary injunction against LoopNet. CoStar then moved for summary judgment on LoopNet's liability, and LoopNet moved for summary judgment on noninfringement and its entitlement to the safe harbor of Section 512(c).

CoStar argued that LoopNet should be directly liable for copyright infringement because, acting through its employees' review and subsequent posting of the photographs, LoopNet was directly copying and distributing the photographs, citing the Frena case discussed above in Section II.A.4(d). The court rejected this argument, noting that the Fourth Circuit in the ALS Scan case had concluded that the legislative history of the DMCA indicated Congress' intent to overrule the Frena case and to follow the Netcom case, under which an OSP's liability for postings by its users must be judged under the contributory infringement doctrine.[2141]

The court then turned to an analysis of contributory infringement and the safe harbor of Section 512(c) of the DMCA asserted by LoopNet. CoStar argued, citing the Fonovisa "swap meet" case[2142] that was relied on by the Ninth Circuit in the Napster I case,[2143] that once it had given LoopNet notice of specific alleged infringements, LoopNet had sufficient knowledge of ongoing infringements by its users to be liable for contributory infringement based on its failure to take more "drastic measures" to prevent infringement.[2144] LoopNet argued that it could not be

---

[2139] 164 F. Supp. 2d 688 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

[2140] Id. at 691-92.

[2141] Id. at 695-96.

[2142] Fonovisa v. Cherry Auction, 76 F.3d 259 (9th Cir. 1996).

[2143] A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[2144] CoStar, 164 F. Supp. 2d at 696-97.

liable for contributory infringement because it had no knowledge of the infringements prior to notice from CoStar, and it discontinued access to the infringing material immediately upon discovery. LoopNet also argued that its DMCA policy for removal of infringing material and of denying access to repeat infringers was sufficient both to give it the benefit of the Section 512(c) safe harbor and to avoid common law contributory liability.[2145]

Turning first to the issue of knowledge, the court held that LoopNet did not have knowledge of the alleged infringements prior to receiving notice from CoStar, based on the facts that CoStar did not attach copyright notices to its photographs and LoopNet did not know what rights CoStar may have granted in license agreements to users of its commercial real estate database containing the photographs.[2146] Citing the Netcom case, the court ruled, "In the case of a service provider, knowledge giving rise to liability only exists when there is no colorable claim of users' noninfringement."[2147] LoopNet could therefore not be charged with any form of knowledge before receiving claims of infringement from CoStar. The central issue, then, was whether LoopNet's policies to deter infringement, remove infringing works, and prevent repeat infringement were adequate both under the common law and for purposes of the DMCA safe harbor.[2148] In an important ruling, the court held that the parameters of the liability protection provided by the Section 512(c) safe harbor were "not contiguous with the bounds of liability for contributory infringement."[2149] This is contrary to the opposite conclusion reached by the district court in an early decision in the Napster case,[2150] later reversed by the Ninth Circuit,[2151] that the parameters for safe harbor liability protection and common law contributory liability were contiguous, and the safe harbor could therefore not protect contributory infringers.

The court then turned to a detailed analysis of whether CoStar was entitled to the benefit of the Section 512(c) safe harbor. As a threshold matter, the court held that the definition of "service provider" under Section 512(k)(1)(B) was broad and easily encompassed the type of service provided by LoopNet.[2152] The court also ruled that the safe harbor could not protect LoopNet for any alleged infringements taking place before December 8, 1999, the date that LoopNet designated an agent to receive notifications of claimed infringement under the DMCA,

---

[2145] Id. at 697-98.

[2146] Id. at 698. The court further noted that the fact that CoStar's employees were involved in manually examining photographs before they were posted on the site did not change the knowledge analysis. "LoopNet has people checking photographs for purposes other than copyright infringement and CoStar's own experts could not distinguish between a CoStar and non-CoStar photograph upon inspection." Id. at 700 n. 6.

[2147] Id. at 698. This is a rather high standard for knowledge for contributory infringement – it seems that in the many circumstances in which an OSP does not have any direct involvement with its users' postings of materials on its site, the OSP will be unable to be certain that there is "no colorable claim" of its users' noninfringement.

[2148] Id. at 698-99.

[2149] Id. at 699.

[2150] A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 n. 24 (N.D. Cal. 2000).

[2151] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

[2152] CoStar, 164 F. Supp. 2d at 701.

as required by Section 512(c)(2) of the DMCA.[2153] The court then turned to an analysis of several specific issues under the safe harbor.

Storage at the Instance of the User. CoStar argued that the Section 512(c) safe harbor should not apply at all because the allegedly infringing photographs were uploaded to the site only after review and selection by LoopNet and so were not stored at the instance of LoopNet's users. The court rejected this argument, reasoning that the photographs were uploaded at the volition of the LoopNet users and that LoopNet subjected them only to a gateway screening process, not a selection process. The court also held that the mere ability to remove or block access to materials could not mean that those materials were not stored at the user's discretion. Noting that Section 512 mandates a "take down" procedure to qualify for the Section 512(c) safe harbor, the court held that it would be internally illogical if the statute were construed to mean that in order to get into the safe harbor, an OSP needed to lack control to remove or block access.[2154]

Knowledge for Purposes of the Safe Harbor. Turning to the issue of knowledge, the court noted that three types of knowledge could take a service provider outside the safe harbor: (i) actual knowledge; (2) awareness of facts raising a "red flag" that its users are infringing; and (iii) notification from the copyright holder in compliance with the technical notice requirements of Section 512(c)(3). The court noted that a service provider does not automatically lose the safe harbor upon receiving notice, but the DMCA shifts responsibility to the service provider to disable the infringing material.[2155] Specifically, "[i]f the service provider has actual knowledge under § 512(c)(1)(A)(i) or 'red flag' knowledge under § 512(c)(1)(A)(ii), the 'take down' provisions of § 512(c)(1)(A)(iii) must be met to stay in the safe harbor. Alternatively, if it receives notification of claimed infringement in accordance with § 512(c)(3), the 'take down' provisions of § 512(c)(1)(C) must be met."[2156]

Because LoopNet had not challenged the adequacy of notification it had received from CoStar, the court turned to the adequacy of LoopNet's removal policy. The court noted that LoopNet had two responsibilities after receipt of notice from the copyright holder:[2157] First, under Section 512(c)(1)(C), it must respond "expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity." Second, under Section 512(i)(1)(A), it must adopt and reasonably implement, and inform subscribers of, a policy "that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

The court ruled that factual issues on each of these two issues precluded summary judgment: CoStar claimed that LoopNet had failed to remove several photographs after being

---

[2153] Id. at 697 & n.4.

[2154] Id. at 701-02.

[2155] Id. at 702.

[2156] Id. at 702 n. 8.

[2157] Id. at 703.

notified that they were infringing and that several photographs had been posted more than once after notification. CoStar also alleged that there was no evidence LoopNet had ever terminated any user's access despite the fact that some of them had an extensive history as repeat infringers.[2158] LoopNet countered that its "Terms and Conditions" for its site included the removal of listings alleged to be infringing and the possibility of termination. LoopNet also claimed that it promptly removed photographs once it received notice of alleged infringement, sent an email to brokers explaining the potential consequences of repeat infringement and investigated brokers it suspected to be repeat infringers. It also claimed to have implemented additional precautions to avoid reposting of infringing photographs in the future. In addition, the court noted that because LoopNet's take down and termination policies had changed over time, to resolve the issue of the adequacy of those procedures, a factfinder would have to focus on each photograph alleged to be infringing and the policy in effect before the posting of each photograph.[2159]

Financial Benefit. To begin its analysis of the financial benefit prong of the Section 512(c) safe harbor, the court, in a significant ruling, noted that, "[r]egardless of whether LoopNet complied with the 'take down' requirements, a finding that it received a direct financial benefit from the infringement automatically would remove it from the safe harbor. … Basically, the DMCA provides no safe harbor for vicarious infringement because it codifies both elements of vicarious liability."[2160] The ruling that the DMCA provides no safe harbor for vicarious infringement seems to contradict the Ninth Circuit's ruling in the Napster I case, discussed in the next subsection, in which the Ninth Circuit noted that "[w]e do not agree [with the district court's ruling] that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se."[2161]

The court held that LoopNet did not meet either element of the test for vicarious liability. CoStar had not asserted that LoopNet had any right to control its users beyond its mere ability to control or block access to its site. The court, citing the Hendrickson v. eBay case, held that such ability to block access could not constitute sufficient "right and ability" to control for vicarious liability. The court noted that otherwise one would have the illogical result that the very policy of blocking access and terminating infringers mandated by the DMCA in Section 512(c)(1)(C) would force service providers to lose their immunity by violating § 512(c)(1)(B).[2162] The court also ruled that LoopNet did not receive a direct financial benefit from the infringing activity because LoopNet did not charge a fee for posting any real estate listing, with or without a photograph.[2163]

[2158] Id.

[2159] Id. at 703-04.

[2160] Id. at 704 (citing 3 M. Nimmer & D. Nimmer, Nimmer on Copyright, § 12B.04[A][2], at 12B-38 (2001)).

[2161] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

[2162] CoStar, 164 F. Supp. 2d at 704 & n.9.

[2163] Id. at 704.

Contributory Liability Before the Safe Harbor Applicability Date. The court next turned to an analysis of LoopNet's contributory liability for activity before December 8, 1999, the date that LoopNet designated an agent to receive notifications of claimed infringement under the DMCA and therefore first became eligible for the Section 512(c) safe harbor. The court's discussion of common law liability provides a nice analysis of the interplay and differences between the standards of knowledge and policing for infringing activity required under the common law versus the DMCA safe harbors.

Knowledge for Purposes of Common Law Liability. CoStar argued that once it gave LoopNet notice of specific infringements, LoopNet was on notice that ongoing infringements were occurring and had a duty to prevent repeat infringements. LoopNet argued that it could not be charged with imputed knowledge of future infringements. The court held that the amount of policing for future infringements LoopNet would be required to do would depend upon the level of knowledge it possessed:

> There is a critical interplay between the level of knowledge possessed by LoopNet as a result of CoStar's notices and the amount of policing, deterrence and removal demanded of LoopNet to avoid being liable for contributory infringement. If CoStar's notice to LoopNet gave LoopNet a broad scope of knowledge that infringements were occurring, then it creates a high level of policing necessary by LoopNet to avoid inducing infringement.
>
> The issue of the adequacy of LoopNet's removal policy is different at this stage than it was when assessing its adequacy for the purposes of the DMCA safe harbor. In the safe harbor context, the removal policy had adequately to remove infringing or allegedly infringing material. If LoopNet met the standard following notice it was shielded from damages liability by the safe harbor. In the context of assessing liability for contributory infringement, the question is not whether LoopNet adequately removed the infringing material, but whether, at some point, it created an inducement to put infringing material up on the site.[2164]

The court noted that, while LoopNet's continued control over access to its site made it more similar to the swap meet owner in the Fonovisa case or the BBS operator in the Maphia case than to the mere seller of goods in the Sony case, there were elements of knowledge in the Fonovisa and Maphia cases that the court found not present in the instant case. Instead, the court analogized to the Netcom case, finding that LoopNet's circumstances resided "in that gray middle range of cases in which the service provider has information suggesting, but not conclusively demonstrating, that subscribers committed infringement. … Netcom stands for the proposition that the bare claim of infringement by a copyright holder does not necessarily give rise to knowledge of an infringement."[2165]

[2164] Id. at 706.

[2165] Id. at 707. The court further observed: "In the analysis of LoopNet's safe harbor defense to liability, mere notification of claimed infringement by CoStar was enough to trigger one of two scenarios. Either LoopNet could comply with the 'take-down' provisions of the DMCA and remain in the safe harbor or refuse to remove

The court contrasted LoopNet's situation from the Napster and Fonovisa cases, where the defendant had actual, specific knowledge of infringements and continued to provide support and facilities to infringers. "Thus, in order to prove its claim, CoStar needs to establish that the notice it gave to LoopNet comprised at least constructive knowledge of specific infringing activity which LoopNet materially contributed to or induced by its alleged failure to halt the activity. There remain too many material factual disputes for the court to decide on summary judgment either that such a level of knowledge did or did not exist or that LoopNet's actions in trying to stop the infringement were or were not insufficient to the point of comprising inducement as a matter of law."[2166] Accordingly, the court denied summary judgment on the issue of common law contributory liability.[2167]

Statutory Damage Award. CoStar elected to take a statutory damages award under Section 504(c)(1) of the copyright statute, which provides that the copyright owner may elect to take statutory damages in lieu of actual damages and profits for "all infringements involved in the action, with respect to any one work …" The court turned to the issue of what constitutes a "work" for purposes of statutory damages. LoopNet argued that CoStar was limited to no more than 13 statutory damages awards because it had only 13 copyright registrations (the photographs had been registered in groups as compilations). CoStar argued that each of its 348 photographs constituted a separate work and, therefore, it was entitled to 348 separate statutory damages awards.[2168]

The court noted a division of authority over whether the copyright registration is determinative of the number of works or whether the determinative factor is whether each work is independently copyrightable. After reviewing the facts of various cases, the court concluded that the critical fact was "not that CoStar registered multiple photographs on the same registration form, but whether it registered them as compilations or as individual copyrights."[2169] The court noted that the language on the registration application under "Nature of Authorship" on all but the first registration read "revised compilation of database information; some original text and photographs."[2170] The first registration read "compilation, text, and photographs," but under the description of the work to be registered, the form read "compilation of public domain material, substantial original text, and original photographs."[2171] The court concluded that the

---

the allegedly infringing material and expose itself to the choppier waters of contributory infringement liability."Id.

[2166] Id. at 707-08.

[2167] LoopNet raised a misuse defense, arguing that CoStar had misused its copyrights in the photographs by extending them beyond their intended reach to limit its licensees from distributing the entire database, including data and photographs in which it had no copyright. Id. at 708. The court rejected this defense with relatively little analysis, distinguishing other copyright misuse cases factually and concluding "there is no allegation or tying or abuse of copyright serious enough to offend the public policy behind copyright and rise to the level of misuse." Id. at 709.

[2168] Id.

[2169] Id. at 711.

[2170] Id.

[2171] Id.

preceding language indicated that all of the registrations were compilation registrations, because the reference to "photographs" could only have efficacy as a description of the work to be registered if it was made with reference to the other elements being copyrighted – the compilation of work.[2172] Accordingly, CoStar was eligible for only 13 statutory damage awards, corresponding to the number of registered compilations.[2173]

The Scope of the Preliminary Injunction. An interesting aspect of the case concerned the scope of preliminary injunction the court entered against LoopNet and the obligations the court imposed on LoopNet once it was notified that one of its users had posted an infringing photograph on the LoopNet system. In an earlier proceeding, the court had entered a preliminary injunction directing LoopNet to "(1) remove from its web site all photographs for which it received notification of claimed infringement from CoStar; (2) notify the user who uploaded the photograph of CoStar's claim of the removal and that repeat acts of infringement might result in restrictions on the user's (or the brokerage firm's) access to the web site; and (3) with regard to identified brokers, require *prima facie* evidence of copyright ownership prior to posting a photograph."[2174] Dissatisfied with LoopNet's performance, CoStar sought a number of substantial modifications to the requirements imposed on LoopNet, including a requirement to obtain a hand-signed written declaration of copyright ownership prior to any posting and a requirement that any repeat infringer thereafter be prohibited from submitting any further photographs.[2175]

The court refused to make the modifications requested by CoStar. In view of its rulings with respect to the contributory infringement and safe harbor issues, the court concluded that CoStar had not shown a sufficient likelihood of success to justify the enhancements to the order it sought.[2176] The court did, however, rule that a probation/termination policy LoopNet had set up, in which brokers who posted infringing photographs could have their probationary status removed in three, six, or twelve month intervals, was inadequate in two respects: "First, all brokers in an office in which any broker posted an allegedly infringing photograph after notice to any broker in that same office should be subject to the *prima facie* evidence requirement."[2177] Second, the court required that the status of "repeat infringer," once achieved, remain during the pendency of the proceedings, with no possibility of discontinuing such status after a time interval.[2178]

Subsequent to the district court's rulings, the parties stipulated to the dismissal of all claims except the district court's summary judgment in favor of LoopNet on direct infringement,

---

[2172] Id. at 711-12.

[2173] Id. at 712.

[2174] Id. at 715.

[2175] Id. at 715-16.

[2176] Id. at 716.

[2177] Id.

[2178] Id. at 717.

and CoStar appealed.[2179] The Fourth Circuit's rulings with respect to the issue of direct infringement are discussed in Section II.A.4(i) above. With respect to the safe harbors, CoStar argued on appeal that Congress intended the DMCA safe harbors to supplant the common law immunity of the Netcom case, and LoopNet could therefore rely solely on the safe harbors for immunity. The Fourth Circuit rejected this argument, noting that the statute expressly states in Section 512(l) that the failure to qualify for limitation of liability under the safe harbors does not bear adversely upon the consideration of other defenses, including a defense that conduct simply does not constitute a prima facie case of infringement.[2180] The court also rejected CoStar's argument that, because Congress codified Netcom in the DMCA, it can be only to the DMCA that a defendant can look for enforcement of the principles Netcom embodied. "When Congress codifies a common-law principle, the common law remains not only good law, but a valuable touchstone for interpreting the statute, unless Congress explicitly states that it *intends* to supplant the common law."[2181] The court found it clear that Congress intended the safe harbors to be a floor, not a ceiling, of protection, and the common law principles of Netcom are therefore still good law.[2182]

Important Principles. The decisions by the district court and by the Fourth Circuit in the CoStar case contain a number of important principles. First, some gateway screening of posted material by an OSP will not necessarily establish sufficient knowledge or control over allegedly infringing works to destroy the potential availability of the Section 512(c) safe harbor. Second, consistent with the Ninth Circuit's ruling in the Napster I case discussed in subsection (iv) below, the boundaries of the contributory liability doctrine and the Section 512(c) safe harbor are not contiguous – Section 512(c) can provide a safe harbor to activity that would otherwise be infringing under the contributory liability doctrine. The CoStar case, however, reached an opposite conclusion from the Ninth Circuit in the Napster I case, as well as the Aimster/Madster and the Hendrickson v. Amazon.com cases discussed in Section III.C.6(b)(1)(i).c and Section III.C.6(b)(1)(iii).g respectively, on the issue of whether the Section 512(c) safe harbor can shield against vicarious liability (the CoStar case concluding no, the Napster I, Aimster/Madster, and Hendrickson v. Amazon.com cases concluding potentially yes).

Third, consistent with the Hendrickson v. eBay case, the OSP's mere ability to terminate infringing users or activity will not of itself be sufficient to establish "control" of the infringing activity for purposes of adjudicating the availability of the Section 512(c) defense. Fourth, the amount of policing for future infringements an OSP may be required to do may depend upon the level of knowledge it possesses concerning the scope of infringing activity on its system. Although not stated as such in the Napster cases, those cases bear evidence of the principle, for the Ninth Circuit in that case imposed a heavy duty of policing in a case in which it seemed to have concluded that Napster had a substantial level of knowledge of infringing activity using its system.

[2179] CoStar Groups, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004).

[2180] Id. at 552.

[2181] Id. at 553 (emphasis in original).

[2182] Id. at 555.

d. Perfect 10 v. Cybernet Ventures

The Section 512(c) safe harbor was further adjudicated in the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.,[2183] the facts of which are set forth in Section III.C.2(f) above. Assuming that Cybernet qualified as a "provider of online services" within the definition of Section 512(k),[2184] the court turned to whether Cybernet had satisfied the predicate requirements of Section 512(i) that it adopt and reasonably implement a policy providing for termination in appropriate circumstances of repeat copyright infringers. Disagreeing with the ruling of the Ellison case discussed in Section III.C.6(b)(1)(i) above, which held that Section 512(i) does not require a service provider to actually terminate repeat infringers or even to investigate infringement, but rather merely to establish a threat of termination for repeat infringement, the court in Perfect 10 v. Cybernet Ventures held that Section 512(i) does in fact imply some substantive responsibilities for service providers. Although it does not require active investigation of possible infringement, or taking action for isolated infringing acts by single users, or addressing "difficult infringement issues," or even actively monitoring for copyright infringement, the court concluded that when confronted with "appropriate circumstances," Section 512(i) requires a service provider to reasonably implement termination.[2185]

> These circumstances would appear to cover, at a minimum, instances where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature. … Under this reading, section 512(i) is focused on infringing users, whereas 512(c) is focused primarily on the infringing material itself.[2186]

Analyzing the interplay between the requirements of Sections 512(i) and 512(c), the court viewed "512(i) as creating room for enforcement policies less stringent or formal than the 'notice and take-down' provisions of section 512(c), but still subject to 512(i)'s 'reasonably implemented' requirement." The court ruled that Cybernet had not satisfied the requirements of Section 512(i). Cybernet had not submitted any documentary evidence that it had ever taken action against individual webmasters who repeatedly put up infringing sites so that such webmasters could not simply move infringing materials from site to site. Instead, Cybernet had only removed from its search engine and links page any site about which it had received a notice of infringement, without ever refusing to provide further services to the operators of those sites. Accordingly, the court concluded that Cybernet had not reasonably implemented a policy to

---

[2183] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[2184] The court noted that, although the definition is quite broad, its applicability to Cybernet was made a bit complicated by the fact that Cybernet insisted that it did not host any infringing images and that no image files passed through any of its computers, but rather that it was purely a provider of age verification services. Id. at 1175.

[2185] Id. at 1176.

[2186] Id. at 1177.

terminate repeat infringers from its service and had therefore not satisfied the predicate requirements of Section 512(i) for the safe harbors.[2187]

The court further ruled that, even if Cybernet could be found to have satisfied the predicate requirements of Section 512(i), it still would not be eligible for the safe harbor of Section 512(c) for two reasons: defective implementation of notice procedures required by Section 512(c) and receipt of a direct financial benefit from infringing activity that it had a right and ability to control.

With respect to the defective implementation of notice procedures, the court noted that Cybernet's take down policy required a complaint to comply strictly with all its stated notice requirements before Cybernet would take action, and there was no indication that Cybernet tried to work with parties whose notice was deficient but satisfied the minimal requirements of Section 512(c)(3)(B)(ii).[2188] In addition, Cybernet's notice requirements did not allow for submission of a representative list of copyrighted works being infringed – they required the specific web page at which a given infringing work was located, "rather than the site."[2189]

Cybernet's counter-notification procedures were also ruled defective. The court held that the counter-notification procedures of the DMCA implicate the requirement of a reasonably implemented Section 512(i) policy "because there is an implication that a party who cannot sign the required statement is a knowing infringer. Thus, the counter-notification procedures appear to serve the generally self-policing policy that section 512 reflects."[2190] Cybernet's counter-notification procedures provided that, if an alleged infringer stated under penalty of perjury that it had removed the named infringing material, the alleged infringer's access to the service would be restored. The court held that this policy "allows Cybernet to reinstate an infringer without the Congressionally-required statement and provides cover for Cybernet to water down its termination policy by treating these minimalist take-down statements as neither an admission nor a denial of the copyright infringement allegations, regardless of how blatant the infringement might be."[2191]

The court also concluded that the Section 512(c) safe harbor was not available for the further reason that Cybernet received a financial benefit "directly attributable" to infringing activity with respect to which it had the right and ability to control. The court noted that the direct financial benefit requirement was satisfied for the same reasons noted in its analysis of Cybernet's vicarious liability (see Section II.C.3(d) above),[2192] although it agreed with the Hendrickson v. eBay and CoStar courts that the mere ability to exclude users from its system is not of itself sufficient right and ability to control infringing activity to deny the safe harbors to a

---

[2187] Id. at 1178-79.

[2188] Id. at 1179-80.

[2189] Id. at 1180.

[2190] Id.

[2191] Id.

[2192] Id. at 1181.

service provider.[2193] The court expressed no opinion on the question whether the "directly attributable" language in the safe harbor is narrower or equivalent to the general vicarious infringement requirement of a direct financial benefit, but ruled that in any event the direct flow of income to Cybernet based on the number of new subscribers signed up by its member sites at which infringing activity was taking place was sufficient to establish a financial benefit "directly attributable" to infringing activity.[2194]

Finally, the court held that there was no evidence presented that Cybernet ever "expeditiously" removed infringing material from its system, disabled links, or altered its search engine under its DMCA policy. Accordingly, the court concluded that there was little likelihood that Cybernet would qualify for the safe harbors.[2195] (An additional aspect of the court's ruling with respect to the Section 512(d) safe harbor is set forth in Section III.C.6(b)(1)(iv) below.)

Important Principles. The court's interpretation of the obligations imposed on a service provider by Section 512(i) are interesting. Specifically, Section 512(i) is directed toward elimination of repeatedly infringing users, whereas Section 512(c) is directed to elimination of infringing materials. Thus, under "appropriate circumstances," a service provider must deny all further service to a user who is repeatedly using the service to infringe, even if the service provider has in every instance removed the particular infringing material that has been identified. In the Perfect 10 v. Cybernet Ventures case, webmasters who had their sites taken down upon notice of infringing material would often simply set up a new site and continue offering infringing materials. The Perfect 10 v. Cybernet Ventures court ruled that in such circumstances, the defendant should have ceased allowing those webmasters to be a part of its service entirely, regardless of the site from which they were operating.

What constitutes an "appropriate circumstance" for denial of further services to a repeat infringer is unclear from the case. The court speaks of "blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature."[2196] This suggests a fairly high standard for an "appropriate circumstance." However, the court also stated that these were circumstances in which a service provider should "at a minimum" terminate services to an infringer, so one cannot assume that blatant or willful infringements of a commercial nature are the only circumstances under which it would be "appropriate" to terminate a user.

The court's rulings with respect to the notice requirements of Section 512(c) are also interesting. First, under those rulings, a service provider's notification procedures must allow for notification of a representative list of copyright works being infringed, rather than always requiring an exact itemization of the allegedly infringed works. It is unclear from the opinion whether the representative list possibility must be an explicitly stated part of the service provider's formal notification procedures, or whether it would be sufficient for the service provider to in fact accept such representative list and act on it. Second, the court interpreted the

---

[2193] Id.

[2194] Id.

[2195] Id. at 1182.

[2196] Id. at 1177.

counter-notification procedures of the safe harbors in effect to require a statement by the alleged infringer that the allegedly infringing materials were in fact not infringing – i.e., that they were removed "as a result of mistake or misidentification of the material."[2197] It is not sufficient for the alleged infringer to inform the service provider that allegedly infringing materials have been removed. If the alleged infringer does not state that the materials were removed by mistake or misidentification, or at least somehow otherwise indicate that the materials were not infringing, the Perfect 10 v. Cybernet Ventures opinion suggests that the service provider is to treat the user as a knowing infringer with respect to that material and count a "strike" against the user for purposes of measuring whether the user is a "repeat infringer."

e. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(c) safe harbor. As discussed in Section III.C.6(b)(1)(i).c above, the district court concluded that Aimster was not entitled to any of the DMCA safe harbors because of its failure to satisfy the Section 512(i) predicate with respect to implementation of a policy to terminate repeat infringers on its system. In addition, the court held that Aimster had not satisfied the specific conditions of Section 512(c) because the plaintiffs were not asserting liability based on the caching of infringing material anywhere within Aimster's system, and the infringing materials were not transmitted "through" the Aimster system.[2198] As discussed in Section III.C.6(b)(1)(i).c, on appeal the Seventh Circuit affirmed the ruling that the safe harbors were not available to Aimster because of failure to comply with Section 512(i).[2199]

f. Hendrickson v. Amazon.com

The case of Hendrickson v. Amazon.com, Inc.[2200] adjudicated the interesting issue of the extent of an ISP's obligation to police its system for infringing material once it receives notice from a copyright holder that all copies of a particular work are unauthorized. This case involved facts similar to the Hendrickson v. eBay case discussed above. On Jan. 28, 2002, Hendrickson sent a letter to Amazon.com notifying it that all copies of the movie *Manson* on DVD infringed his copyright. On Oct. 21, 2002, Hendrickson noticed that a *Manson* DVD was posted for sale on Amazon's website. Hendrickson purchased a copy of the DVD, then filed an action against both Amazon and the poster of the DVD, asserting claims of direct infringement against Amazon and the poster, and a claim of vicarious liability against Amazon. Amazon moved for summary judgment on the ground that it was not liable for direct infringement, since the movie had not been sold by Amazon, and that it was entitled to the safe harbor of Section 512(c) for the claim of vicarious liability.[2201]

[2197] 17 U.S.C. § 512(g)(3)(C).

[2198] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 660-61 (N.D. Ill. 2002) & n.21.

[2199] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[2200] 69 U.S.P.Q.2d 1471 (C.D. Cal. 2003).

[2201] Id. at 1471-72.

The court first ruled that Amazon was not liable for direct infringement, even though it had offered the website pages that the seller and buyer used to complete the purchase, because Amazon was not the actual seller of the item.[2202] With respect to the DMCA safe harbor, the court first held, consistent with the Aimster/Madster case and the Ninth Circuit's decision in Napster I, that the DMCA safe harbors can shield against vicarious liability.[2203] The court then noted that, although the DMCA places the burden on the copyright owner in the first instance to monitor the Internet for potentially infringing sales,[2204] "because the DMCA is relatively new, the question as to how long an adequate notice should remain viable is still unanswered."[2205]

Turning to an analysis of this question, the court noted that it was not the intention of Congress that a copyright owner could write one blanket notice to all service providers alerting them of infringing material, thereby relieving himself of any further responsibility and placing the onus forever on the service provider. However, the court also noted that it would be against the spirit of the DMCA if the entire responsibility were to lie with the copyright owner to forever police websites in search of possible infringers.[2206]

To resolve a balance between these competing concerns, the court looked to the language of the safe harbor, noting that to qualify for the safe harbor, Section 512(c) requires that the service provider not have actual knowledge that material on its system "is infringing" or that infringing activity "is apparent."[2207] The court concluded that, by use of the present tense, Congress intended for the notice to make the service provider aware of the infringing activity that is occurring at the time it receives the notice.[2208] "If the infringing material *is on* the website *at the time* the ISP receives the notice, then the information, that all *Manson* DVD's are infringing, can be adequate to find the infringing material expeditiously. However, if at the time the notice is received, the infringing material is not posted, the notice does not enable the service provider to locate infringing material that is not there, let alone do it expeditiously."[2209]

Drawing on these principles, the court ruled that the DMCA places a limit on the viability of an otherwise adequate notice, and with respect to the instant case, "Hendrickson's January, 2002, letter, claiming all *Manson* DVDs violate his copyright, although adequate for the listings then on Amazon, cannot be deemed adequate notice for subsequent listings and sales, especially, as here, when the infringing item was posted for sale nine months after the date of the notice."[2210] Accordingly, Amazon's lack of knowledge of the infringing activity satisfied the

---

[2202] Id. at 1472.

[2203] Id.

[2204] Id. at 1473. In an earlier opinion, the court had ruled that Hendrickson's Jan. 2002 letter substantially complied with the DMCA notice requirements. Hendrickson v. Amazon.com, Inc., CV 02-07394 TJH (C.D. Cal. 2003).

[2205] 69 U.S.P.Q.2d at 1473.

[2206] Id.

[2207] Id.

[2208] Id.

[2209] Id. at 1473-74 (emphasis in original).

[2210] Id. at 1474.

first prong of the safe harbor under Section 512(c)(1)(A).[2211] Amazon satisfied the second prong of the safe harbor under Section 512(c)(1)(B) because, although it received a financial benefit from its third party sellers, the court held that there was no evidence to suggest that Amazon had "the ability to know that an infringing sale by a third party seller would occur," and hence it could not control such sales.[2212] Accordingly, the court granted Amazon summary judgment under the safe harbor of Section 512(c).[2213]

g. Rossi v. MPAA

A peripheral issue relating to the notice provisions of the Section 512(c) safe harbor was raised in the case of Rossi v. Motion Picture Association of America, Inc.,[2214] in which the plaintiff was the operator of a web site called internetmovies.com, an online directory of artists' works and an Internet news magazine providing information and resources about movies on the Internet. The MPAA found statements on the web site such as "Join to download full length movies online now! New movies every month"; "Full Length Downloadable Movies"; and "NOW DOWNLOADABLE" followed by graphics from a number of the MPAA's copyrighted movies. The MPAA sent a Section 512(c) written notice to the plaintiff's Internet service provider asking that it remove the plaintiff's web site from its server because of the site's allegedly infringing content.[2215]

The plaintiff sued the MPAA for, among other things, tortious interference with contractual relations and tortious interference with prospective business advantage, and the MPAA moved for summary judgment. Under Hawaiian law, the plaintiff was required to show that the MPAA acted without justification. The MPAA argued that its actions were justified because the DMCA authorized it to send the plaintiff's Internet service provider a notice requesting that it shut down the plaintiff's web site.[2216]

The plaintiff argued that the MPAA was not justified in sending the DMCA notice because, in order to have "a good faith belief" of infringement, the copyright owner is required to conduct a reasonable investigation into the allegedly offending website. The plaintiff argued that the reasonableness of the investigation should be judged under an objective standard of review, and that the MPAA had failed to meet that standard because, if it had reasonably investigated the site by attempting to download movies, it would have discovered that no movies could actually be downloaded from the site or related links.[2217]

[2211] Id.

[2212] Id.

[2213] Id.

[2214] Rossi v. Motion Picture Ass'n of America, Inc., 391 F.3d 1000 (9th Cir. 2004).

[2215] Id. at 1002.

[2216] Id.

[2217] Id. at 1003-04.

The MPAA countered that the "good faith belief" requirement should be a subjective one, and the Ninth Circuit agreed. Although no court had yet interpreted the standard under Section 512(c), the court noted that several decisions interpreting other federal statutes had traditionally interpreted "good faith" to encompass a subjective standard. The court also found that the overall structure of Section 512 supported the conclusion that Section 512(c)(2)(A)(v) imposes a subjective good faith requirement on copyright owners. Congress included in Section 512(f) a limited cause of action for improper infringement notifications, imposing liability only if the copyright owner's notification is a knowing misrepresentation. Juxtaposing the "good faith" proviso of the DMCA with the "knowing misrepresentation" provision revealed a statutory structure intended to protect potential violators only from subjectively improper actions by copyright owners.[2218]

The Ninth Circuit found that the plaintiff had failed to raise a genuine issue of material fact under the subjective standard regarding the MPAA's good faith. The statements on the plaintiff's web site strongly suggested that movies were available for downloading, and the court noted that the plaintiff had admitted that his own customers often believed that movies were available for downloading. Accordingly, the Ninth Circuit affirmed the district court's ruling on summary judgment that there was no issue of material fact as to the MPAA's "good faith belief" that the plaintiff's web site was infringing its copyrights.[2219] The Ninth Circuit also affirmed the district court's holding that the MPAA's good faith compliance with the notice and takedown procedures of the DMCA constituted sufficient "justification" under Hawaiian law to avoid the plaintiff's claim for tortuous interference with contractual relations.[2220]

h. Perfect 10 v. CCBill

The facts of this case are set forth in Section III.C.6(b)(1)(i)d. above. In that case, the defendant CWIE, an OSP hosting various sites that allegedly contained infringing copies of Perfect10's photos, moved for summary judgment under the Section 512(c) safe harbor. Perfect 10 argued that CWIE was not entitled to the safe harbor because it had actual knowledge of Perfect 10's infringements on its clients' web sites, it was aware of facts or circumstances from which infringing activity was apparent, it failed to expeditiously remove or disable access to infringing material of which it had knowledge, and it received a financial benefit directly attributable to the infringing activity and had the right and ability to control such activity.[2221]

With respect to the issue of knowledge, the district court found Perfect 10's notifications to CWIE of infringement to be deficient under Section 512(c) because they identified only the web sites containing allegedly infringing material, but did not identify the URLs of the infringing images or which of Perfect 10's copyrights were being infringed.[2222] With respect to whether

---

[2218] Id. at 1004-05.

[2219] Id. at 1005-06.

[2220] Id. at 1006.

[2221] Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d 1077, 1103 (C.D. Cal. 2004).

[2222] Id. at 1100-01.

CWIE had constructive notice of infringement, the court noted that the kind of constructive notice Congress contemplated under Section 512(c) was that of "red flag" web sites from which infringements would be apparent based on a cursory review of the web site. Under this test, although some of CWIE's affiliate web sites advertised images of celebrities, they did not contain obvious infringements because the web sites did not advertise themselves as pirate web sites. Accordingly, the court concluded that Perfect 10 had not raised a genuine issue of material fact that CWIE had actual or constructive knowledge of infringements on its clients' web sites.[2223]

With respect to the issue of control, the court noted that CWIE's right and ability to control infringing activity was limited to disconnecting its webmasters' access to CWIE's service. Citing the case of Perfect 10 v. Cybernet Ventures, Inc.,[2224] the court ruled that the mere ability to terminate services to a web site was not sufficient control for purposes of the Section 512(C) safe harbor. Nor was the fact that CWIE reviewed its sites to look for blatantly illegal and criminal conduct sufficient to close the safe harbor, for the DMCA was intended to encourage OSPs to work with copyright owners to locate and stop infringing conduct. Accordingly, the court ruled that CWIE was entitled to summary judgment on the Section 512(c) safe harbor.[2225]

On appeal, the Ninth Circuit, for the reasons discussed above in Section III.C.6(b)(1)(i).d above, agreed with the district court's rulings that Perfect 10's notices of infringement were insufficient to comply with the requirements of Section 512(c)(3) or to provide CWIE with knowledge or awareness within the standard of Section 512(c)(1)(A).[2226] The remaining question was therefore whether Perfect 10 had raised a genuine issue of material fact concerning whether CWIE received a direct financial benefit from the infringing activity.[2227] The Ninth Circuit held that "'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious liability. … Thus, the relevant inquiry is 'whether the infringing activity constitutes a draw for subscribers, not just an added benefit.'"[2228] The court noted that Perfect 10 had alleged only that CWIE hosted websites for a fee, and such allegation was insufficient to show that the infringing activity was a draw. The court also noted that legislative history of Section 512 stated that receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a direct financial benefit. Accordingly, the court ruled that there was no genuine issue that CWIE had received a direct financial benefit from infringing activity, and therefore if on

---

[2223] Id. at 1103-04.

[2224] 213 F. Supp. 1146, 1181 (C.D. Cal. 2002).

[2225] Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d at 1104-05.

[2226] Perfect 10, Inc. v. CCBill, 481 F.3d 751, 766 (9th Cir.), cert. denied, 2007 U.S. LEXIS 12812 (2007).

[2227] Id.

[2228] Id. at 767 (quoting Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004)).

remand the district court were to find that CWIE had met the threshold requirements of Section 512(i), CWIE would be entitled to the Section 512(c) safe harbor.[2229]

i. Corbis Corp. v. Amazon.com, Inc.

The opinion in this case contains a lengthy adjudication of the requirements of Section 512(i) as a predicate for the Section 512 safe harbors. Amazon hosted through its website a platform called "zShops," which allowed individuals and retailer vendors to showcase their products and sell them directly to online consumers. A zShop vendor could include a product image in its sales listing in one of two ways – either by creating a link to an image stored on the vendor's computer or server, or by uploading an image to one of Amazon's servers for display in the listing. Amazon did not actively participate or supervise the uploading or linking of images, nor did it preview the images before the link was created or the upload completed.[2230]

Corbis, the owner of the copyrights in a large collection of images, brought copyright claims against Amazon because 230 of its images were displayed and sold without authorization by zShop vendors through the Amazon website. In addition, two other images were displayed by Amazon in banner ads that appeared on the Internet Movie Database (IMDb), a website owned by Amazon and operated separately from Amazon.com. Amazon asserted the safe harbor of Section 512(c).[2231]

The court turned first to a very detailed analysis of whether Amazon satisfied all the predicate conditions of Section 512(i):

– Whether Amazon was a "Service Provider". The court ruled that Amazon clearly qualified under the definition of "Service Provider" of Section 512(k)(1)(B), and rejected Corbis' argument that a Service Provider must "serve to route or connect online digital communications." Amazon's operation of web sites was sufficient to make it a Service Provider.[2232]

– Whether Amazon Had Adopted an Adequate User Policy. Amazon required all zShop vendors to execute a Participation Agreement, which prohibited vendors from listing or linking to any item that infringed any third party intellectual property right or was counterfeited, illegal, stolen, or fraudulent. The agreement also gave Amazon the right, but not the obligation, to monitor any activity and content associated with the site, and the right and the absolute discretion to remove, screen, or edit any content that violated the agreement or was otherwise objectionable.[2233] In addition, it was Amazon's policy that when it received information that a vendor might be infringing another's copyrights, it would cancel the allegedly infringing listing and send an email to the vendor, notifying it of the cancellation, identifying a contact email

---

[2229] 481 F.3d at 767.

[2230] Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1094 (W.D. Wa. 2004).

[2231] Id. at 1096-98.

[2232] Id. at 1100 & n. 6.

[2233] Id. at 1095.

address for the complaining party, and reminding the vendor that "repeated violations of our Community Rules could result in permanent suspension from our Auction, zShops, and Amazon Marketplace sites."[2234]

Corbis complained that the Participation Agreement and Amazon's related policies were too vague with respect to copyright infringement, in that they did not include the term "repeat infringer" and did not describe the methodology employed in determining which users would be terminated for repeated copyright violations. The court rejected this argument, noting that the language of Section 512(i) and the overall structure of the DMCA indicate that the user policy need not be as specific as Corbis suggested. The fact that Congress left the phrase "repeat infringer" undefined, and chose not to elaborate on what circumstances merit terminating a repeat infringer's access, suggested Congress' intent to leave the policy requirements and the obligations of service providers loosely defined.[2235] "Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, ex ante, the specific types of conduct that will merit restricting access to its services. As Congress made clear, the DMCA was drafted with the understanding that service providers need not 'make difficult judgments as to whether conduct is or is not infringing.'"[2236]

The court found that the Participation Agreement adequately prohibited the listing, linking, or posting of any material that violates copyright laws and made clear that those who violated Amazon's policies could face a variety of penalties. In addition, the court pointed to testimony that those accused of copyright infringement were informed that repeated violations could result in "permanent suspension" from Amazon sites. Accordingly, the court ruled that Amazon had an adequate user policy.[2237]

– Whether Amazon Had Adequately Communicated Its Termination Policy to Its Users. Corbis argued that Amazon had not adequately communicated its termination policy to its users because it did not inform them of the internal criteria it used to determine whether to terminate a user's access to the site. The court held, however, that Section 512(i) is not so exacting, and that Amazon needed only inform users that, in appropriate circumstances, it may terminate the user's accounts for repeated copyright infringement. The statute does not suggest what criteria should be considered by a service provider, much less require the service provider to reveal its decision making criteria to the user. Amazon was required only to put users on notice that they faced exclusion from the service if they repeatedly violate copyright law, and Amazon had done so.[2238]

– Whether Amazon Had Reasonably Implemented Its Infringement Policy. To judge the adequacy of implementation of an infringement policy, the court noted that one must look at two questions – whether a service provider has adopted a procedure for receiving complaints and

---

[2234] Id.

[2235] Id. at 1100-01.

[2236] Id. at 1101.

[2237] Id.

[2238] Id. at 1101-02.

conveying those complaints to users, and whether the service provider nonetheless still tolerates flagrant or blatant copyright infringement by its users.[2239]

Turning to the first question, the court found that Amazon had a sufficient procedure for implementing its infringement policy. Amazon had a practice to promptly cancel a listing once it received adequate notice that the listing violated another's copyrights, to inform the vendor that its listing may have violated intellectual property rights, to give the vendor the contact information of the complaining party, and to warn the vendor that repeated violations could result in permanent suspension from the Amazon site. The fact that certain vendors had been able to reappear on the zShops platform under pseudonyms did not amount to a failure of implementation. The court ruled that an infringement policy need not be perfect; it need only be reasonably implemented. Corbis had not shown any more effective and reasonable method that Amazon could have used to prevent vendors from re-accessing zShops.[2240]

With respect to the second question – tolerance of flagrant abusers – the court noted that Section 512(i) requires only that repeated copyright infringers be terminated in "appropriate circumstances" and that a service provider need not conduct active investigation of possible infringement or make a decision regarding difficult infringement issues.[2241] The court seems to have set a rather high threshold for what might constitute "appropriate circumstances": "Because it does not have an affirmative duty to police its users, failure to properly implement an infringement policy requires a showing of instances where a service provider fails to terminate a user even though it has sufficient evidence to create actual knowledge of that user's blatant, repeated infringement of a willful and commercial nature."[2242]

Corbis alleged that Amazon tolerated repeated infringers because it had received three emails (although not from Corbis) in which the sender claimed that zShop listings posted by one vendor were infringing, and had received seven emails (again not from Corbis) in which the sender claimed that zShop listings of another vendor were infringing, and had not terminated either vendor's access to zShops until after Corbis' suit was filed. The court found that this evidence did not amount to a showing that Amazon had knowledge of blatant, repeat infringement that would have required Amazon to terminate access to the vendors' zShops sites.[2243] In a very significant ruling, the court held the following: "Although efforts to pin down exactly what amounts to knowledge of blatant copyright infringement may be difficult, it requires, at a minimum, that a service provider who receives notice of a copyright violation be able to tell merely from looking at the user's activities, statements, or conduct that copyright infringement is occurring."[2244] Citing various previously decided cases, the court noted that examples of such blatant infringement may include statements from the vendor that a product is

---

[2239] Id. at 1102.

[2240] Id. at 1103-04.

[2241] Id. at 1104.

[2242] Id.

[2243] Id. at 1104.

[2244] Id. at 1104-05.

bootlegged or pirated, chat rooms hosted by the service provider in which users discuss how the service can be used to circumvent copyright laws, or the offering of hundreds of audio files in a single day for peer to peer copying. Corbis had presented no such examples of blatant infringing activity on the vendor defendants' zShops sites.[2245]

In another significant ruling, the court held that notices from copyright owners under Section 512(c)(3) do not, of themselves, necessarily establish evidence of blatant or repeat infringement. "A copyright owner may have a good faith belief that her work is being infringed, but may still be wrong. The notification requirement does not take into account that a vendor may have 'a legitimate fair use defense, or can otherwise invoke any of the myriad other factors that go into evaluating a copyright infringement claim.' Although the notices have brought the listings to Amazon's attention, they did not, in themselves, provide evidence of blatant copyright infringement."[2246] The court ruled that knowledge of blatant, repeat infringement cannot be imputed merely from the receipt of notices of infringement. Instead, there must be additional evidence available to the service provider to buttress the claim of infringement supplied by the notices.[2247] The court went on to state, "In this regard, this Court respectfully disagrees with CCBill, in which the district court for the Central District of California held that receipt by the service provider of two or more DMCA compliant notices about one of its users required termination under § 512(i). Although there may be instances in which two or more DMCA compliant notices make a service provider aware of a user's blatant, repeat infringement, the notices alone do not make the user's activity blatant, or even conclusively determine that the user is an infringer."[2248]

The court noted that, other than the Section 512(c)(3) email notices of infringement, there was no evidence suggesting that Amazon would have been able to tell, merely by looking at the listings of the two vendors, that the posters and photos being sold infringed another's copyrights. Without some evidence from the site raising a red flag, Amazon would not know enough about the photograph, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement. In addition, one of the vendors had unequivocally stated to Amazon that it had the right to sell all of the posters in its inventory. The other vendor had told Amazon that all of its products were officially licensed. The court concluded that for Amazon to determine that the two vendors were infringers, it would have had to conduct the type of investigation that the courts and Congress had found unnecessary.[2249]

– Whether Amazon Had Knowledge of Infringement. Having concluded that Amazon satisfied all predicate conditions of Section 512(i), the court then turned to the conditions of the Section 512(c) safe harbor that Amazon had to establish – that it did not have knowledge of infringing activity or acted expeditiously to remove infringing materials upon gaining

---

[2245] Id. at 1005.

[2246] Id. (citation omitted).

[2247] Id. at 1105-06.

[2248] Id. at 1105 n.9 (citation omitted).

[2249] Id. at 1106.

knowledge, and that it did not receive a financial benefit directly attributable to any infringing activity that it maintained the right and ability to control. Because Corbis did not challenge Amazon's claim that it acted expeditiously to remove or disable access to allegedly infringing material, the court turned to the knowledge and control prongs.[2250]

In view of the fact that Corbis did not challenge that Amazon expeditiously removed access to allegedly infringing material, it is somewhat curious that the court engaged in such an extensive analysis of the knowledge prong of the Section 512(c) safe harbor. Nevertheless, the court issued some important rulings about the knowledge prong that were consistent with its other rulings to afford a broad scope to the Section 512(c) safe harbor.

Because Corbis had chosen not to send notices of infringement to Amazon before filing its lawsuit, Amazon had no actual knowledge of the alleged infringements of Corbis' copyrighted images, and the court turned its analysis to whether Corbis was aware of facts or circumstances from which infringing activity was apparent. Corbis submitted evidence of notices provided by other copyright holders addressing non-Corbis photos and evidence suggesting that Amazon was aware that Corbis licensed celebrity photos, from which Corbis argued that Amazon should have known that zShops vendors sold infringing Corbis images.

The court rejected this evidence as insufficient to establish a material issue of fact regarding Amazon's actual or apparent knowledge of infringing material on the zShops platform. A mere general awareness that a particular type of item may be easily infringed is insufficient to establish actual knowledge. With respect to apparent knowledge, the court cited the Nimmer copyright treatise for the proposition that the standard is not "what a reasonable person would have deduced given all the circumstances," but rather "whether the service provider deliberately proceeded in the face of blatant factors of which it was aware."[2251] The court also quoted from the legislative history of the DMCA that apparent knowledge requires evidence that a service provider "turned a blind eye to 'red flags' of obvious infringement."[2252]

To establish apparent knowledge, Corbis submitted evidence that Amazon received notices that zShops vendors were infringing the copyrights of unrelated parties by selling celebrity photographs. The court found this evidence insufficient, because it was not clear whether any of the vendors receiving such notices were vendors in the instant litigation and whether the notices complied with the requirements of Section 512(c)(3). If the notices were compliant, Amazon asserted that it promptly canceled a listing after receiving a notice of infringement, an assertion that Corbis did not challenge.[2253]

In any event, in a more significant ruling, the court held that third party notices do not, in themselves, constitute red flags. As noted in the legislative history, evidence of blatant copyright infringement will often derive from information on the offending site itself. The court noted that

---

[2250] Id. at 1106-07.

[2251] Id. at 1108 (quoting 3 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 12B.04[A][1], at 12B-49 (2004)).

[2252] Corbis, 351 F. Supp. 2d at 1108 (citing H.R. Rep. No. 105-551 Part 2, at 42 (1998)).

[2253] Corbis, 351 F. Supp. 2d at 1108.

even if the notices had caused Amazon to examine the content of the zShops sites, Corbis had not shown that those sites contained the type of blatant infringing activity that would have raised a red flag for Amazon. Accordingly, Corbis had failed to establish apparent knowledge of infringement on the part of Amazon.[2254]

– Whether Amazon Had the Right and Ability to Control the Infringing Activity. Corbis argued a right and ability to control on Amazon's part from the fact that it had terminated the zShops defendants on the same day Corbis filed and served its complaint. The court cited the CCBill and Costar cases for the proposition that the right and ability to control prong cannot be satisfied merely by the ability of a service provider to remove or block access to materials posted on its website or stored on its systems. Nor did the fact that Amazon advertised the zShops platform amount to a right and ability to control the items sold there absent some showing that Amazon intended to pick infringing material for its site. The court noted that Amazon did not preview the products prior to their listing, did not edit the product descriptions, and did not suggest prices or otherwise involve itself in the sale. Accordingly, the court ruled that Amazon did not have the right and ability to control the infringing material, and the court therefore did not need to look into whether Amazon received a direct financial benefit from the allegedly infringing conduct.[2255]

Based on its various rulings, the court concluded that Amazon was entitled to the Section 512(c) safe harbor and was therefore immune from all monetary relief. The only relief Corbis could be entitled to was the limited injunctive relief set forth in Section 512(j). Because Corbis had not sought injunctive relief, and because Amazon had asserted that it had terminated the accounts of the defendant vendors, it was unclear how the limited injunctive relief would apply in the particular case at bar. The court therefore granted Amazon's motion for summary judgment with respect to the DMCA claims.[2256]

j. Tur v. YouTube, Inc.

In Tur v. YouTube, Inc.,[2257] Robert Tur, owner of the copyright in video footage of the Reginald Denny beatings during the 1992 Los Angeles riots, sued YouTube for copyright infringement based on the unauthorized presence of his copyrighted video footage on the web site. YouTube moved for summary judgment under the Section 512(c) safe harbor. The court denied summary judgment, finding that there were factual issues with respect to whether YouTube had the right and ability to control infringing activity on its site. The court agreed with existing precedents that the right and ability to control requires more than just the ability of a service provider to remove or block access to materials posted on its web site or stored on its system.[2258] "Rather, the requirement presupposes some antecedent ability to limit or filter

---

[2254] Id. at 1108-09.

[2255] Id. at 1109-10.

[2256] Id. at 1110-11 & 1118-19.

[2257] 2007 U.S. Dist. LEXIS 50254 (C.D. Cal. June 20, 2007).

[2258] Id. at *9.

copyrighted material."[2259] The court found, however, that there was insufficient evidence in the record regarding the process undertaken by YouTube from the time a user submitted a video clip to the point of display on the YouTube site, and the extent of YouTube's technical capabilities to detect and pre-screen allegedly infringing videos.[2260] On Oct. 19, 2007, the court granted Tur's motion to voluntarily dismiss his complaint so that he could join as a plaintiff in class action litigation filed by The Football Association Premier League Limited against YouTube on May 4, 2007 in the Southern District of New York.[2261]

k. Io Group v. Veoh Networks

In Io Group, Inc. v. Veoh Networks, Inc.,[2262] a decision by a magistrate judge, Veoh operated a user-generated content web site through which users could also access videos from Veoh's content partners. Once video files were uploaded to Veoh's system, Veoh's employees selected videos to be featured on the "Featured Videos" portion of the web site. A number of clips submitted by users contained content from the Io Group's copyrighted sexually explicit videos, and Io Group sued Veoh for copyright infringement for hosting the clips without giving prior notice to Veoh or demanding that Veoh take down the allegedly infringing material. Veoh asserted the safe harbor under Section 512(c).[2263]

Before users could upload videos to Veoh's site, they were required to register and agree to abide by the Terms of Use and Acceptable Use policies posted on the site. The Terms of Use stated that Veoh reserved the right to monitor user-submitted material and to remove it from the site, that the user was not permitted to publish or make available any material that infringed third party intellectual property rights, and that the user represented and warranted that it had all rights necessary to publish and distribute any material submitted to the site. Upon each upload of particular material, the user was presented with an explicit reminder that it must not upload copyrighted, pornographic, obscene, violent, or other videos that violate Veoh's applicable policies. Upon receiving a notice that a user had uploaded infringing content after a first warning, the user's account would be terminated, all content provided by that user disabled (unless the content was also published by another non-terminated user and was not the subject of a DMCA notice), and the user's email address would be blocked so that a new account could not be opened with that same address. Veoh also had the ability to disable access to such material on its users' hard drives if their computers were still connected to the Internet, and it had adopted means for generating a digital fingerprint for each video file that enabled Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user.[2264]

[2259] Id.

[2260] Id. at *10.

[2261] Order Granting Plaintiff's Motion to Voluntarily Dismiss Complaint, Tur v. YouTube, Inc., CV 06-4436 FMC (C.D. Cal. Oct. 19, 2007).

[2262] 586 F. Supp. 1132 (N.D. Cal. 2008).

[2263] Id. at 1135-36.

[2264] Id. at 1137-38.

When users uploaded a video to Veoh's system, they would provide certain metadata about the video, including title, description, tags, selection of up to four categories best describing the video, and a content rating. Upon receiving a video submission, Veoh's computers would first confirm that the submitted file was, in fact, a video file with a compatible codec, and if so, the system would extract the file format and length, assign a unique video ID number to it, index the user-entered metadata and store the information in a database on Veoh's servers. The database also automatically indexed video files into a series of lists, such as "Most Recent," "Top Rated," "Most Popular," "Most Discussed," and "Top Favorite." In addition to saving the file in its original format, which users could download using Veoh's client software, the system also automatically converted the file into Flash format. The system also extracted during the upload process 16 full resolution screen captures (screencaps) and 16 lower resolution screencaps. One of the lower resolution screencaps was used to represent the video in a search result which, when clicked on, took the user to a video details page containing the video and a link to view all 16 lower resolution screencaps. Veoh employees occasionally spot checked videos after publication for compliance with Veoh's policies and to ensure accuracy in the description and characterization of the content, and on occasion edited the video description field. If a spot check revealed an instance of blatant copyright infringement (e.g., a movie known to have been released only in theaters), Veoh disabled access to the material.[2265]

The court rejected Io Group's argument that Veoh had not implemented its repeat infringer policy in a reasonable manner. The court found that Veoh's evidence established that it had a working notification system and a procedure for dealing with copyright infringement notices. Veoh's policies identified its designated copyright agent and it often responded to infringement notices the same day received, or at most within a few days. When Veoh received notice that user had uploaded infringing content after a first warning, the user's account was termination and all content provided by that user was disabled. Veoh's fingerprint technology enabled it terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user. Since the web site was launched, Veoh had terminated 1,096 users for repeat copyright violations.[2266]

Io Group argued that Veoh's policy failed because it did not prevent repeat infringers from reappearing on the site under a pseudonym and a different email address. The court rejected this argument, ruling that the hypothetical possibility that a rogue user might reappear under a different user name and identity did not raise a genuine fact issue as to the implementation of Veoh's policy. Io Group had presented no evidence that a repeat infringer had, in fact, established a new account under false pretenses, much less that Veoh had intentionally allowed that to happen. The court rejected Io Group's reliance on the Napster case as establishing a requirement under Section 512(i) that a site operator track users by their actual names or IP addresses. Io Group had presented no evidence suggesting that tracking or verifying users' actual identity or that blocking their IP addresses would be a more effective reasonable means of implementation, particularly given that IP addresses identify only a particular computer connected to the Internet and not particular users. The court ruled that Section 512(i) does not

[2265] Id. at 1138-40.

[2266] Id. at 1143.

require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement. Veoh's tracking of content that had been identified as infringing and permanently blocking that content from ever being uploaded by any user was adequate to satisfy Section 512(i) requirements.[2267]

The court then turned to whether the requirements of the Section 512(c) safe harbor had been satisfied. Io Group argued that the Flash files and screencaps created during the publication process were not stored on Veoh's system "at the direction of a user," but by Veoh's own acts and decisions, and that Section 512(c) was not intended to protect the creation of those files because Veoh used them as a means of distribution (e.g., by indexing content and organizing them into lists), and not just storage. The court rejected this argument, noting that the broader definition of "service provider" under Section 512(k)(1)(B) does not contain an express limitation that the content of material stored on the system not be modified. And existing case law such as the CoStar v. LoopNet decision supported the conclusion that Veoh was not precluded from the Section 512(c) safe harbor by virtue of its automated processing of user-submitted content. The court noted that Veoh did not itself actively participate or supervise the uploading of files, nor did it preview or select the files before the upload was completed. Instead, video files were uploaded through an automated process that was initiated entirely at the volition of Veoh's users. Inasmuch as the conversion to Flash format was a means of facilitating user access to material on its web site, the court held that Veoh did not lose the safe harbor through the automated creation of those files.[2268]

Turning to the issue of knowledge of the infringing activity, the court found that, because Io Group had provided Veoh no notice of any claimed copyright infringement before filing its lawsuit, Veoh had no actual knowledge of the infringing activity at issue. With respect to knowledge through signs of apparent infringing activity, the court noted the applicable "red flag" test, which requires the service provider to be aware of blatant factors indicating infringement. The court found no such factors present in the instant case. None of the allegedly infringing video files uploaded by Veoh's users contain Io Group's copyright notices. Although one of the works did contain the plaintiff's trademark several minutes into the clip, there was no evidence from which it could be inferred that Veoh was aware of, but chose to ignore, it. Nor would the professionally created nature of submitted content constitute a red flag per se, particularly given that the video equipment available to the general public was of such quality that there might be little distinction left between professional and amateur productions. Finally, the court rejected Io Group's argument that Veoh should have known that no legitimate producer of sexually explicit material would have omitted the labels required by federal law for sexually explicit material identifying where records as to the performers depicted are kept. The court ruled that the absence of such labels did not give rise to a genuine issue of material fact as to whether Veoh had the requisite level of knowledge or awareness that the plaintiff's copyrights were being violated.[2269]

[2267] Id. at 1143-45.

[2268] Id. at 1146-48.

[2269] Id. at 1148-49.

With respect to the requirement to act expeditiously to remove or disable access to material, undisputed evidence established that when Veoh received DMCA-compliant notices, it responded and removed noticed content on the same day the notice was received or within a few days thereafter. In addition, Veoh also promptly investigated other complaints about content on its web site through a "Flag It!" feature that enabled users to bring certain content to Veoh's attention by flagging it from a set list of reasons such as mis-rated content, sexually explicit content, and obscene content. Io Group argued that Veoh had willfully blinded itself to facts suggesting infringement because the list of reasons on the "Flag It!" feature no longer contained a choice for "appears to contain copyrighted material." The court rejected this argument, noting that the "Flag It!" feature itself contained a notice, prominently displayed at the top of the "Flag It!" dialog box, directing copyright owners to a link with instructions for submitting a copyright infringement notice to Veoh.[2270]

Finally, with respect to the issue of right and ability to control the infringing activity, the court rejected Io Group's argument that the requisite "right and ability to control" was present because Veoh had established and enforced policies prohibiting users from engaging in a host of illegal and other conduct on its web site and exercised the right to police its system by conducting occasional spot checks of video files for compliance. The court noted that the plaintiff was focused on the wrong inquiry. Under Section 512(c), the pertinent inquiry was not whether Veoh had the right and ability to control its *system*, but rather whether it had the right and ability to control the *infringing activity*. The latter cannot simply mean the ability of a service provider to block or remove access to materials posted on its web site. The court distinguished the Napster system, which existed solely to provide the site and facilities for copyright infringement, and Napster's control over its system was directly intertwined with its ability to control infringing activity. In the instant case, by contrast, Veoh's right and ability to control its system did not equate to the right and ability to control infringing activity. Unlike Napster, there was no suggestion that Veoh aimed to encourage copyright infringement on its system or that it could control what content users chose to upload before it was uploaded. Given that Veoh received hundreds of thousands of video files from its users, the court ruled that no reasonable juror could conclude that a comprehensive review of every file would be feasible. And even if it were, there could be no assurance that Veoh could have accurately identified the infringing content at issue. Accordingly, Veoh's ability to control its index did not equate to an ability to identify and terminate *infringing* videos. For the most part, the files in question did not bear titles resembling the plaintiff's works and the plaintiff had not provided Veoh with its titles to search.[2271]

The court further observed that, perhaps most importantly, there was no indication that Veoh had failed to police its system to the fullest extent permitted by its architecture. Once content had been identified as infringing, Veoh's digital fingerprint technology prevented the same infringing content from ever being uploaded again, indicating that Veoh had taken steps to reduce, not foster, the incidence of copyright infringement on its web site. The court rejected Io Group's argument that Veoh should have verified the source of all incoming videos by obtaining

[2270] Id. at 1149-50.

[2271] Id. at 1150-53.

and confirming the names and addresses of the submitting user, the producer, and the submitting user's authority to upload a given file, as required by California Penal Code § 653w and 18 U.S.C. § 2257. The court noted that the issue was not Veoh's compliance with those statutory requirements, nor whether it should have been aware that certain content was infringing. Rather, the question was whether Veoh declined to exercise a right to stop it.[2272] "Declining to change business operations is not the same as declining to exercise a right and ability to control infringing activity."[2273] The plaintiff's suggestion that Veoh must be required to reduce or limit its business operations was contrary to one of the stated goals of the DMCA to facilitate the growth of electronic commerce.[2274]

Accordingly, the court granted Veoh's motion for summary judgment under the Section 512(c) safe harbor. It cautioned however, that

> the decision rendered here is confined to the particular combination of facts in this case and is not intended to push the bounds of the safe harbor so wide that less than scrupulous service providers may claim its protection. Nevertheless, the court does not find that the DMCA was intended to have Veoh shoulder the entire burden of policing third-party copyrights on its website (at the cost of losing its business if it cannot). Rather, the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging copyright infringement, Veoh has a strong DMCA policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website.[2275]

l. UMG Recordings v. Veoh Networks

The District Court Decisions

The case of UMG Recordings, Inc. v. Veoh Networks, Inc.[2276] involved the same user-generated content site, Veoh Networks, as the case described in the previous subsection. The plaintiffs, who owned rights to copyrighted sound recordings and musical compositions allegedly used without authorization in user-submitted videos to the site, sought summary judgment that Veoh was not entitled to the Section 512(c) safe harbor because of four functions performed by Veoh's software that the plaintiffs claimed were not "storage" and were not undertaken "at the direction of the user": automatically creating Flash formatted copies of video files uploaded by users, automatically creating copies of uploaded video files that are comprised of smaller chunks of the original file, allowing users to access uploaded videos via streaming, and allowing users to

---

[2272] Id. at 1153-54.

[2273] Id. at 1154.

[2274] Id.

[2275] Id. at 1155.

[2276] 620 F. Supp. 2d 1081 (C.D. Cal. 2008), aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

access uploaded videos by downloading whole video files. The court denied the plaintiff's motion.[2277]

The court noted that the IoGroup case had held that Section 512(c) was applicable to the creation of Flash formatted files, but the applicability of Section 512(c) to the other three challenged software functions was a question of first impression.[2278] Although the plaintiffs conceded that all four challenged software functions were directed toward facilitating access to materials stored at the direction of users, they argued that Section 512(c) requires that the service provider's conduct *be* storage, and that the storage be at the direction of a user. The court rejected this argument, finding that the safe harbor extends to functions other than mere storage, since the statutory language applies to "infringement of copyright *by reason of* the storage at the direction of a user."[2279] When copyrighted content was displayed or distributed on Veoh's system it was by reason of or attributable to the fact that users uploaded the content to Veoh's servers to be accessed by other means.[2280] The court therefore denied the plaintiffs' motion for summary judgment, concluding:

> The four software functions that UMG challenges fall within the scope of § 512(c), because all of them are narrowly directed toward providing access to material stored at the direction of users. Both the conversion of uploaded files into Flash format and the "chunking" of uploaded files are undertaken to make it easier for users to view and download movies, and affect only the form and not the content of the movies; "streaming" and downloading merely are two technically different means of accessing uploaded videos.[2281]

Following this ruling, Veoh moved for summary judgment that it had satisfied the remaining requirements of Section 512(c) and was therefore not liable for monetary or injunctive relief. The court granted Veoh's motion for summary judgment.[2282] Because the basic facts of the case were not disputed, the court's opinion addressed the significant question of the extent to which the DMCA obligates Internet-based services like Veoh, which rely on content contributed by users, to police their systems to prevent copyright infringement.

The court began its analysis with a review of certain key facts about the way the Veoh system operated, and these facts seemed to provide important context for the court's conclusions concerning whether Veoh should have DMCA immunity. Each time users began to upload a video to the veoh.com web site they were shown a message stating, "Do not upload videos that infringe copyright, are pornographic, obscene, violent, or any other videos that violate Veoh's

---

[2277] Id. at 1083.

[2278] Id.

[2279] Id. at 1088 (emphasis added).

[2280] Id. at 1088-89.

[2281] Id. at 1092.

[2282] UMG Recordings, Inc. v. Veoh Networks Inc., 2009 U.S. Dist. LEXIS 86932 (Sept. 11, 2009), aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

Terms of Use."[2283] Veoh's employees did not review user-submitted content before it became available to other users, although Veoh's system did allow it to disable access to inappropriate videos. Veoh used a number of technologies to automatically prevent copyright infringement on its system. Beginning in 2006, when Veoh disabled access to a video that infringed a copyright, it used hash filtering software to thereafter automatically disable access to any identical video and block any subsequently submitted duplicates. In addition, in 2007, Veoh began using the Audible Magic commercial software to filter out potentially infringing video files from being uploaded in the first instance by taking an audio fingerprint from the video files and comparing it to a database of copyright content that was protected by copyright holders like UMG. Approximately nine months later, Veoh applied the Audible Magic filter to its backlog of videos, resulting in the removal of more than 60,000 videos. Although the vast majority of allegedly infringing files had been removed in response to notices from the RIAA (acting as UMG Recording's agent) and the Audible Magic software, several hundred other allegedly infringing files that the Audible Magic filter had failed to identify as infringing remained on the system.[2284]

The court then turned to analysis of each of the requirements of the Section 512(c) safe harbor. Addressing first the requirement that Veoh act expeditiously to remove infringing content upon obtaining either actual knowledge or awareness of facts and circumstances from which infringing activity is apparent, the court ruled that UMG had failed to rebut Veoh's showing that when it acquired knowledge of allegedly infringing material – whether from DMCA notices, informal notices, or other means – it expeditiously removed such material. Citing the Ninth Circuit's CCBill decision, the court noted that the DMCA notification procedures place the burden of policing copyright infringement by identifying potentially infringing material and adequately documenting infringement squarely on the copyright owner. The court noted that CCBill further taught that if investigation of facts and circumstances is required to identify material as infringing, then those facts and circumstances are not "red flags" of infringement.[2285] The court concluded: "In light of the principles articulated in *CCBill* that the burden is on the copyright holder to provide notice of allegedly infringing material, and that it takes willful ignorance of readily apparent infringement to find a 'red flag,' Veoh has provided substantial evidence that it fulfilled the requirements of *section 512(c)(1)(A)*."[2286]

Specifically, with respect to actual knowledge, the court rejected UMG's argument that Veoh had actual knowledge of infringement merely because it knew that it was hosting an entire category of content – music – that was subject to copyright protection. The court found that if this were the standard for actual knowledge, the Section 512(c) safe harbor would be a dead letter because vast portions of content on the Internet are eligible for copyright protection. Nor did Veoh's automatic tagging of more than 240,000 videos with the label "music video" give it actual knowledge that such videos were infringing. The court also rejected UMG's argument that the RIAA's DMCA notices gave Veoh notice of infringement beyond the specific materials

---

[2283] Id. at *6.

[2284] Id. at *6-12.

[2285] Id. at *19-24.

[2286] Id. at *24-25.

that the RIAA identified because the notices listed artists who made the materials. UMG argued that Veoh should have sought out actual knowledge of other infringing videos by searching its system for all videos by the artists identified in the RIAA notices, because a list of artist names was equivalent to a representative list of allegedly infringing works, which the DMCA allows the copyright holder to supply. The court ruled that providing names of artists is not the same as a representative list of works. An artist's name is not information reasonably sufficient to permit a service provider to locate allegedly infringing material. Accordingly, the court concluded that UMG had not provided evidence establishing that Veoh failed to act expeditiously whenever it had actual notice of infringement, whether from DMCA notices or other sources of information.[2287]

With respect to Veoh's awareness of facts or circumstances from which infringing activity was apparent under the "red flag" test, the court rejected UMG's argument that Veoh was ineligible for the safe harbor because its founders, employees, and investors knew that widespread infringement was occurring on the Veoh system. The court held that, even if this were true and undisputed, UMG had cited no case holding that a service provider's general awareness of infringement, without more, is enough to preclude application of Section 512(c), and such a holding would be contrary to Congress' intent that the DMCA safe harbors facilitate the robust development of world-wide expansion of electronic commerce, communications, and research in the digital age.[2288]

The court also rejected UMG's contention that Veoh avoided gaining knowledge of infringement by delaying implementation of the Audible Magic fingerprinting system for a couple of years after its commercial availability:

> UMG has not established that the DMCA imposes an obligation on a service provider to implement filtering technology at all, let alone technology from the copyright holder's preferred vendor or on the copyright holder's desired timeline. Moreover, it is undisputed that Veoh did take steps to implement filtering technology before it implemented the Audible Magic system that UMG prefers, by using "hash" filtering and by attempting to develop its own filtering software. UMG dismisses hash filtering as "highly ineffectual," but that it proved deficient and that Veoh turned to Audible Magic does not negate Veoh's showing of good faith efforts to avoid or limit storage of infringing content.[2289]

Accordingly, the court concluded that Veoh had shown that it was not aware of "red flags," notwithstanding its knowledge of the general proposition that infringing material was often uploaded to web sites, and UMG had failed to present evidence to the contrary.[2290]

[2287] Id. at *25-31.

[2288] Id. at *32-33.

[2289] Id. at *35.

[2290] Id. at *36.

The court then turned to Section 512(c)'s requirement that the service provider not receive a financial benefit directly attributable to infringing activity that the service provider has the right and ability to control. The court first observed that, because the capacity to control and remove material are features that a service provider that stores content on its system must have in order to implicate the Section 512(c) safe harbor at all, those facts alone cannot constitute the type of control that is disqualifying. Nor could the right and ability to implement filtering software, standing alone or even along with Veoh's ability to control user's access, be the basis for ineligibility for the safe harbor.[2291] The court noted Section 512(m)'s provision that the safe harbors are not conditioned upon a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, and concluded:

> If courts were to find that the availability of superior filtering systems or the ability to search for potentially infringing files establishes – without more – that a service provider has "the right and ability to control" infringement, that would effectively require service providers to adopt specific filtering technology and perform regular searches. That, in turn, would impermissibly condition the application of *section 512(c)* on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity."[2292]

UMG urged the court to follow two "principles" it claimed were established by the Napster cases: (1) that the ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise, and (2) that to escape vicarious liability, the reserved right to police must be exercised to its fullest extent. The court refused, noting that if it were to adopt principle (1) from Napster it would render the statutory phrase "right and ability to control" redundant, because the ability to block infringers' access for any reason whatsoever is already a prerequisite to satisfying the predicate requirements of Section 512(i)(1)(A). And if the court were to adopt principle (2), it would run afoul of Section 512(m). Accordingly, the court ruled that, although the "direct financial benefit" standard should be the same as the common law direct financial benefit standard for vicarious infringement, the phrase "right and ability to control" should be construed to impose a higher standard of control than the common law standard for vicarious liability, and UMG had not established that Veoh met that higher standard of control.[2293]

Finally, the court turned to whether Veoh had met Section 512(i)'s requirement with respect to termination of repeat infringers. UMG contended that Veoh's termination policy was inadequate because it did not automatically terminate users who uploaded videos that were blocked by the Audible Magic filter. The court rejected this argument because however beneficial the Audible Magic technology was in helping to identify infringing material, it did not meet the standard of reliability and verifiability required by the Ninth Circuit to justify

---

[2291] Id. at *37-38.

[2292] Id. at *39. The court also quoted H. Conf. Report 105-796 at 73 (Oct. 8, 1998): "Court should not conclude that the service provider loses eligibility for limitations on liability under *section 512* solely because it engaged in a monitoring program."

[2293] Id. at *46-50.

terminating a user's account. The court reasoned that, in view of the Ninth Circuit's ruling in CCBill that a notice by a copyright holder that specific material was allegedly infringing was not a sufficient basis for terminating a user because it lacked a sworn declaration that the notifier had a good faith belief that the material was unlicensed, it stood to reason that Audible Magic's automated filter also could not be a basis. The court noted that there was no evidence in the record of a feasible way for Veoh to verify information in Audible Magic's database or evaluate Audible Magic's process for compiling the database. Veoh had requested Audible Magic for contact information of copyright claimants for works identified by Audible Magic's filter, for use in implementing a counter-notice procedure, and Audible Magic had refused. Accordingly, the court concluded that Veoh had no way of verifying the accuracy of Audible Magic's database, and even if it did, it would be unreasonable to place that burden on Veoh.[2294] "As a practical matter, when notice of a user's alleged infringement is not reliable enough to justify terminating the user's account, a service provider's removal of the allegedly infringing material is sufficient evidence of compliance with the DMCA. In this case, when Veoh received notices of infringement it promptly removed the material identified."[2295]

The court also rejected UMG's argument that Veoh failed to adequately terminate repeat infringers because it did not necessarily terminate users who uploaded multiple videos that were identified in a single DMCA notice. If a single DMCA notice from the RIAA identified multiple videos uploaded by one user, Veoh sent the user a first warning. It then terminated the user's account if the user subsequently uploaded another infringing video. The court held that this policy satisfied Section 512(i)'s requirements, and UMG had pointed to nothing in the statute, legislative history, or case law establishing that such a policy was not reasonable or appropriate. Accordingly, the court granted Veoh's motion for summary judgment that it was entitled to the Section 512(c) safe harbor.[2296]

The Ninth Circuit's Decision

On appeal, in a very significant and wide ranging opinion, the Ninth Circuit affirmed the entry of summary judgment in Veoh's favor. Because the plaintiffs renewed their arguments that the automated processing performed by Veoh upon a video file uploaded by a user went beyond activities that are the subject of Section 512(c), the Ninth Circuit elaborated on the details of that processing. Upon upload, Veoh's software automatically broke down the video file into smaller 256-kilobyte "chunks," which facilitated making the video accessible to others. Veoh's software also automatically transcoded the video file into Flash 7 format because the vast majority of Internet users had software that could play videos in that format. If the user was a "Pro" user, the uploaded video file was also transcoded into Flash 8 and MPEG-4 formats, which are playable on some portable devices. Accordingly, when a Pro user uploaded a video, Veoh

[2294] Id. at *50-55.

[2295] Id. at *55.

[2296] Id. at *50-51 & *55-56.

automatically created and retained four copies: the chunked file, the Flash 7 file, the Flash 8 file and the MPEG-4 file. None of those automated conversions affected the content of the video.[2297]

Veoh's computers also automatically extracted metadata from information users provided to help other locate the video for viewing. Users could provide a title, as well as tags or keywords that described the video, and could also select preset categories describing the video, such as "music," "faith" or "politics." The Veoh system then automatically assigned every uploaded video a "permalink," or web address, that uniquely identified the video and made it available to users. Veoh employees did not review the user-submitted video, title or tags before the video was made available. Users were able either to stream videos from the site or to download them in a "chunked" copy of the file to the user's computer, upon which software reassembled the chunks into a viewable file. The downloaded file was stored on the user's computer in a Veoh directory, which gave Veoh the ability to terminate access to the files.[2298] The technologies employed by Veoh to automatically reduce copyright infringement on its system, including hash filtering and Audible Magic, are described in the summary of the district courts decisions above.

The plaintiffs made three challenges to the district court's rulings. First, the plaintiffs argued that the alleged infringing activities did not fall within the plain meaning of "infringement of copyright by reason of the storage [of material] at the direction of a user" as required by Section 512(c)(1); second, that genuine issues of fact remained about whether Veoh had actual knowledge of infringement or was aware of facts or circumstances from infringing activity was apparent; and third, that the plaintiffs had present sufficient evidence that Veoh received a financial benefit directly attributable to infringing activity that it had the right and ability to control. The court did not address whether Veoh adopted and reasonably implemented a repeat infringer termination policy or whether, upon notification, Veoh expeditiously removed or disabled access to infringing material as required by Section 512 (c). Although the plaintiffs contested those points in the district court, their only mention of them on appeal was in a footnote in their opening brief and they set forth no arguments as to those points.[2299]

"By reason of the storage." Turning to the first issue, the court held that the phrase "by reason of the storage at the direction of the user" was meant to cover more than mere electronic storage lockers, and the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarified that Section 512(c) encompasses the access-facilitating processes that automatically occurred when a user uploaded a video to Veoh. The court noted that the plaintiffs' narrow reading of the "by reason of" language to be limited solely to storage activities per se would create internal statutory conflicts. By its terms, Section 512(c) presupposes that service providers will provide access to users' stored material (they are required to disable access to such material upon a qualifying notice from the copyright holder), and it

---

[2297] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1027 (9th Cir. 2011).

[2298] Id. at 1027-28.

[2299] Id. at 1030-31 & n.5.

would thus contravene the statute to hold that such access disqualified Veoh from the safe harbor.[2300]

The court did not find persuasive the plaintiffs' effort to reconcile the internal contradictions its reading of the statute created by positing that Congress must have meant Section 512(c) to protect only web hosting services. The court found that this theory failed to account for the reality that web hosts store user submitted materials in order to make those materials accessible to other Internet users. Thus, Section 512(c) should be interpreted to enable web hosting services to copy content and transmit it to Internet users. The court observed that the language of the statute recognizes that one is unlikely to infringe a copyright by merely storing material that no one could access, and so includes activities that go beyond storage in its language stating "the material *or an activity using the material* … is infringing" (emphasis added) in Section 512(c)(1)(A)(i).[2301]

Accordingly, the court concluded, "Under the broader definition [of 'service provider'] applying to § 512(c), there is no limitation on the service provider's ability to modify user-submitted material to facilitate storage and access, as Veoh's automatic processes do. Had Congress intended to include such a limitation, it would have said so expressly and unambiguously, as it did in the narrower definition of 'service provider.'"[2302]

Knowledge. Turning to the second issue of knowledge requirements, the court began with an issue of statutory construction, noting that, "to be coherent, the statute must be read to have an implicit 'and' between § 512(c)(1)(A)(i) and (ii). We thus treat the provisions as stating that to qualify for the safe harbor, a service provider must either (1) have no actual knowledge *and* no 'aware[ness] of facts or circumstances from which infringing activity is apparent' *or* (2) expeditiously remove or disable access to infringing material of which it knows or is aware."[2303]

The Ninth Circuit first dealt with the issue of whether generalized knowledge of infringement on a service provider's system is sufficient to disqualify the safe harbor. The plaintiffs contended that, because Veoh hosted a category of copyrightable content – music – for which it had no license from any major music company, it must have known this content was unauthorized, given its general knowledge that its services could be used to post infringing material, and this fact should be sufficient to demonstrate knowledge of infringement. The court rejected this argument on several grounds. First, it noted there are many music videos that could in fact legally appear on Veoh. And if merely hosting material that falls within a category of content capable of copyright protection, with the general knowledge that one's services could be used to share unauthorized copies of copyrighted material, was sufficient to impute knowledge to services providers, the Section 512(c) safe harbor would be rendered a dead letter. Section 512(c) applies only to claims of copyright infringement, yet the fact that a service provider's web site contained copyrightable material would remove the service provider from Section 512(c)

[2300] Id. at 1031, 1033.

[2301] Id. at 1034.

[2302] Id. at 1035.

[2303] Id. at 1036 n.11.

eligibility.[2304] For support, the Ninth Circuit pointed to the Supreme Court's Sony decision, in which it ruled that, so long as the product distributed by a defendant that is used for copyright infringement is "capable of substantial noninfringing uses," the Court refused to impute knowledge of infringement.[2305]

The Ninth Circuit noted that requiring specific knowledge of particular infringing activity made good sense in the context of the DMCA, which Congress enacted to foster cooperation among copyright holders and service providers in dealing with infringement on the Internet. These considerations were reflected in Congress' decision to enact a notice and takedown protocol encouraging copyrighte holders to identify specific infringing material to service providers. They were also evidenced in the "exclusionary rule" that prohibits consideration of substantially deficient Section 512(c)(3)(A) notices for purposes of determining whether a service provider has actual knowledge or is aware of facts and circumstances from which infringing active is apparent. Thus, Congress had made a considered policy determination that the DMCA notification procedures would place the burden of policing copyright infringement and identifying the potentially infringing material squarely on the owner of the copyright.[2306]

The court noted that its conclusion was bolstered by Section 512(m), which states that nothing in Section 512(c) shall be construed to condition the applicability of the safe harbor on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity. The court rejected the plaintiffs' argument that Section 512(m)'s title, "Protection of Privacy," should cause the provision to be read narrowly. Even if privacy was the impetus for the provision, nothing in Section 512(m) suggested that fact should limit its application. Because the plain language of Section 512(m) is unambiguous, the heading could not limit the plain meaning of the text.[2307]

The court therefore held that merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under Section 512(c)(1)(A)(i). It reached the same conclusion with respect to Section 512(c)(1)(A)(ii), concluding that the district court's conception of the "red flag test" properly followed the Ninth Circuit's analysis in CCBill, which reiterated that the burden remains with the copyright holder rather than the service provider. Accordingly, the court held that Veoh's general knowledge that it hosted copyrightable material and that its services could be used for infringement was insufficient to constitute a red flag.[2308]

The court also was not persuaded that the plaintiffs' other purported evidence of Veoh's actual or apparent knowledge of infringement warranted a trial. The plaintiffs argued that

---

[2304] Id. at 1036-37.

[2305] Id. at 1037 (quoting Sony Corp. of America v. Universal City Studios, Inc., 464 US. 417, 442 (1984)).

[2306] UMG Recordings, 667 F.3d at 1037-38.

[2307] Id. at 1038 & n.12.

[2308] Id. at 1038.

Veoh's purchase of certain search terms through the Google AdWords program demonstrated knowledge of infringing activity because some of the terms purchased, such as "50 Cent," "Avril Lavigne" and "Britney Spears," were the names of the plaintiffs' artists. The court noted that artists are not always in exclusive relationships with recording companies, and other recording companies had given Veoh permission to stream its videos by those artists. In addition, even absent such permission, companies sometimes purchase search terms they believe will lead potential customers to their web sites even if the terms do not describe goods or services the company actually provides.[2309]

The plaintiffs further argued that, although Veoh removed unauthorized content identified in RIAA notices, it should have taken the initiative to use search and indexing tools to locate and remove from its web site any other content by the artists identified in the notices. In addition, the plaintiffs argued that some of the videos on Veoh that had been pulled from MTV or other broadcast television stations bore information about the artist, song title and record label, and Veoh should have used this information to find and remove unauthorized videos. The court rejected these arguments, noting that such a requirement would conflict with Section 512(m) and CCBill's refusal to impose investigative duties on service providers.[2310]

Nor were news articles discussing the availability of copyrighted materials on Veoh, including one reporting that Veoh had been among the least aggressive video sharing sites in fighting copyrighted content, sufficient to charge Veoh with the knowledge required to disqualify the safe harbor. The DMCA's detailed notice and takedown procedure assumes that, from time to time, material belonging to someone else ends up on service providers' web sites, and establishes a process for ensuring its prompt removal. If awareness of news reports discussing this general problem were enough to remove the safe harbor, the notice and takedown procedures would make little sense and the safe harbors would be effectively nullified.[2311]

Significantly, however, the court left open the possibility that notifications of infringement from third parties other than the copyright owner might be sufficient to establish a red flag. The plaintiffs submitted evidence of emails sent to Veoh executives and investors by copyright holders and users identifying infringing content. One email, sent by the CEO of Disney, a major copyright holder, to Michael Eisner, a Veoh investor, stated that the movie *Cinderella III* and various episodes from the television show *Lost* were available on Veoh without Disney's authorization.[2312] "If this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test because it specified particular infringing material. As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3), which this informal email failed to meet."[2313] Accordingly, the deficient notice could not be considered in determining whether Veoh had

---

[2309] Id. at 1039.

[2310] Id.

[2311] Id. at 1039-40.

[2312] Id. at 1040.

[2313] Id.

actual or red flag knowledge. The court noted that, even if the email could have created actual or red flag knowledge, Eisner's email in response assured Disney that he would instruct Veoh to take it down, and Esiner copied Veoh's founder to ensure this happened right away. The plaintiffs also pointed to an email from a Veoh user whose video was rejected for containing infringing content. Upset that Veoh would not post his unauthorized material, he stated that he had seen plenty of other infringing material on the site, and identified another user who he said posted infringing content.[2314] The court observed:

> It is possible that this email would be sufficient to constitute a red flag under § 512(c)(1)(A)(ii), even though it would not qualify as sufficient notice from a copyright holder under § 512(c)(3). But even assuming that is so, UMG has not specifically alleged that Veoh failed to expeditiously remove the infringing content identified by the user's email, or that the content at issue was owned by UMG. Accordingly, this too fails to creat a genuine issue of material fact regarding Veoh's knowledge of infringement.[2315]

Right and Ability to Control. Turning to the third issue on appeal, the Ninth Circuit concluded that the district court correctly determined that Veoh did not have the necessary right and ability to control infringing activity and thus remained eligible for safe harbor protection. As did the district court, the Ninth Circuit imported a knowledge requirement into the control issue. The court noted that a service provider may, as a general matter, have the legal right and necessary technology to remove infringing content, but until it becomes aware of *specific* unauthorized material, it cannot exercise its power or authority over the specific infringing item and therefore could not have the kind of ability to control infringing activity the statute contemplates. The court's bolstered its reasoning by pointing again to Section 512(m), which it found to cut against a holding urged by the plaintiffs that Veoh's general knowledge that infringing material could be uploaded to its site triggered an obligation to exercise control by policing its services.[2316] "We are not persuaded by UMG's suggestion that Congress meant [Section 512(m)'s] limitation on the duty to monitor to apply only to service providers who do not receive a direct financial benefit under *subsection (b)*. Rather we conclude that a service provider must be aware of specific infringing material to have the ability to control that infringing activity within the meaning of § 512(C)(1)(B). Only then would its failure to exercise its ability to control deny it a safe harbor."[2317]

[2314] Id. The court further noted, "Although the user's allegations would not give Veoh actual knowledge under § 512(c)(1)(A)(i), because Veoh would have no assurance that a third party who does not hold the copyright in question could know whether the material was infringing, the email could act as a red flag under § 512(c)(1)(A)(ii) provided its information was sufficiently specific." Id. at 1040 n.14.

[2315] Id.

[2316] Id. at 1041-42.

[2317] Id. at 1042. The court agreed with the many other decisions holding that the mere ability to locate and take down infringing material cannot, by itself, satisfy the control element. Were it otherwise, a service provider could lose immunity under the safe harbor merely because it engaged in acts that are specifically required by the DMCA. Id. at 1042 & n.16.

Summarizing its holding, the court stated: "[W]e hold that the 'right and ability to control' under § 512(c) requires control over specific infringing activity the provider knows about. A service provider's general right and ability to remove materials from its services is, alone, insufficient. Of course, a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge. … [T]he DMCA recognizes that service providers who are not able to locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection."[2318] The court contrasted this more specific form of "right and ability to control" under the DMCA with that of the broader standard for common law vicarious liability, which can be met by merely having the general ability to locate infringing material and terminate users' access, as in the Napster case.[2319] The court did not elaborate in any way on what might constitute willfully burying one's head in the sand to avoid obtaining specific knowledge, and that single sentence may be expected to give rise to litigation in the future.

Based on its rulings, the Ninth Circuit concluded that Veoh met all the Section 512(c) requirements and affirmed the entry of summary judgment in its favor.[2320]

m. Perfect 10 v. Amazon

In Perfect 10, Inc. v. Amazon.com, Inc.,[2321] Perfect 10 sought to hold Amazon's subsidiary A9, which operated the A9 search engine that enabled searching of content on Amazon.com and other sources, contributorily liable for infringing postings of Perfect 10's copyrighted photos. A9 moved for summary judgment under the Section 512(c) safe harbor on the ground that it was undisputed that Perfect 10 sent its DMCA notices to Amazon rather than A9. A9 had designated its own copyright agent in Palo Alto with the Copyright Office. The Copyright Office designation included, in lieu of an email address for the agent, the URL of an online DMCA complaint form.[2322] Meanwhile, on Amazon's web site, Amazon's "Notice and Procedure for Making Claims of Copyright Infringement" instructed users to contact Amazon's copyright agent in Seattle for notifying Amazon "and its affiliates" of copyright infringement.

[2318] Id. at 1043.

[2319] Id. The court rejected the plaintiffs' argument that the broader formulation of the right and ability to control requirement from vicarious liability as applied in the Napster case should be read into the DMCA. First, Section 512(c) nowhere mentions the term "vicarious liability," and second, Napster was decided after the DMCA was enacted, so Congress could not have intended to codify Napster's precise application of vicarious liability. The court also pointed to three legislative history reports of the DMCA where Congress stated explicitly that the DMCA was intended to protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement. Id. at 1043-44. In view of its rulings with respect to the control element, the court noted that it need not consider whether Veoh received a financial benefit directly attributable to the infringing activity. Id. at 1041 n.15.

[2320] Id. at 1045.

[2321] 2009 U.S. Dist. LEXIS 42341 (C.D. Cal. May 12, 2009).

[2322] Id. at *2 & 4-5.

The designation Amazon filed with the Copyright Office listed a number of Amazon-owned entities as "alternative names of service provider" but A9 was not among the listed entities.[2323]

Perfect 10's President, Dr. Zada, sent a letter to Amazon's copyright agent concerning alleged infringements in the search results of A9's search engine. Amazon's corporate counsel, Karen Ressmeyer, called Dr. Zada and informed him that Google, not Amazon or A9, provided the search results and there was nothing Amazon could do about the complaints. After receiving several additional letters from Zada alleging infringements on A9, Ressmeyer contacted Google herself and, at Google's suggestion, forwarded Zada's letters to Google. She informed Zada of this fact in a letter, which she copied to Jonathan Leblang, the individual whom A9 had identified as its copyright agent in its filing at the Copyright Office. Despite all of his correspondence with Ressmeyer, Amazon never told Zada that he had to send his notices of infringement to A9 directly. No one at Amazon told him that the notices were not being forwarded to A9 or that it was not sufficient to send them to Amazon.[2324]

Perfect 10 argued that A9 was not entitled to the safe harbor because it had actual knowledge of infringement by virtue of the fact that it did in fact receive Perfect 10's DMCA notices. In part, Perfect 10 relied on post-litigation notices it sent to A9's copyright agent. The court ruled that the post-litigation instances of A9 receiving information of claimed infringements did not constitute notification under Section 512(c)(3) with respect to pre-litigation infringements claimed in the original complaint. Perfect 10 also cited Ressmeyer's letter to Zada that was copied to A9's copyright agent Leblang. The court rejected this basis also, noting that the letter did not indicate that Amazon forwarded any DMCA notices to A9 and did not provide any information about the infringing material, so the letter alone did not establish either that A9 received any of Perfect 10's notices or that it had actual knowledge of specific infringing activities available using its system.[2325]

Perfect 10 argued that Amazon should be equitably estopped from asserting that Perfect 10 improperly sent its notices to Amazon because the Conditions of Use posted on Amazon's site allegedly instructed copyright owners to send DMCA notices regarding its affiliates directly to Amazon. The court rejected this argument, noting that nowhere in the Conditions of Use did Amazon purport to include A9 among its affiliates and Amazon's filing with the Copyright Office identifying the subsidiary entities for which Amazon's copyright agent would accept complaints did not include A9.[2326]

Perfect 10 further argued that Amazon was the proper recipient of the notices because the infringing activity took place through the A9 search box that was on the Amazon web site. The court rejected this argument, holding that the presence of the search box on Amazon's web site did not make Amazon the proper recipient because A9 had designated its own copyright agent and Zada knew that A9 was a separate corporation entity. Perfect 10 also contended that

---

[2323] Id. at *5-6.

[2324] Id. at *6-10.

[2325] Id. at *13-15.

[2326] Id. at *15-16.

Amazon was obligated to notify A9 of the alleged infringements because it owned and hosted A9. The court also rejected this argument, noting Perfect 10 had cited no authority that would require one OSP, by virtue of its ownership or hosting of another OSP, to pass along a DMCA notice, where the two OSPs were distinct corporate entities and each had properly designated its own copyright agent.[2327]

Lastly, Perfect 10 argued that A9 had failed to comply fully with the requirements of Section 512(c)(2) in designating a copyright agent because A9 had not provided an email address for its copyright agent, but rather a URL for A9's online complaint form. The court held that this departure from the specific requirements of Section 512(c)(2) was inconsequential, and there was no genuine dispute that the Copyright Office designation enabled anyone who saw it to contact A9's designated agent, through mail, fax, telephone, or the online complaint form. Accordingly, the court ruled that A9 was entitled to a safe harbor under Section 512(c), and granted A9's motion for summary judgment as to contributory copyright infringement based on that safe harbor.[2328]

n. Louis Vuitton v. Akanoc Solutions

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.[2329] the defendants operated hosting services for a number of web sites overseas from which counterfeit Louis Vuitton merchandise could be purchased. The plaintiff brought claims for direct and contributory infringement of its copyrights. A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with respect to the claims.[2330] With respect to the DMCA safe harbor, the court found that the jury had adequate evidence for denying the applicability of the Section 512(c) safe harbor. The defendants did not designate an agent with the Copyright Office until about four months after the lawsuit was filed, so at a minimum they would not be able to claim protection of the safe harbors prior to designating an agent. In addition, the evidence that the defendants had reasonably implemented a policy to terminate repeat infringers was limited, at best. For example, the designated agent for the defendants testified that he did not understand the DMCA's requirements as to maintaining or implementing the required policy. Other evidence indicated that the defendants had not terminated certain repeat offenders. Accordingly the court concluded that the jury had sufficient evidence to find for the plaintiff on the issue of the applicability of the safe harbor provisions of the DMCA.[2331]

o. Viacom v. YouTube

[2327] Id. at *17-18.

[2328] Id. at *20-23.

[2329] 2010 U.S. Dist. LEXIS 85266 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part on other grounds, 658 F.3d 936 (9th Cir. 2011)..

[2330] Id. at *1-2.

[2331] Id. at *24.

In Viacom Int'l v. YouTube, Inc.,[2332] the plaintiffs sought to hold YouTube and its owner Google secondarily liable for the postings by users of copyrighted videos owned by the plaintiffs. YouTube asserted the DMCA safe harbor under Section 512(c). Each side moved for summary judgment in the district court.

The District Court's Opinion

Interestingly, in its opinion, the district court noted that from the plaintiffs' submissions on the motion, a jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their web site.[2333] Thus, according to the court, "the critical question is whether the statutory phrases 'actual knowledge that the material or an activity using the material on the system or network is infringing,' and 'facts or circumstances from which infringing activity is apparent" in § 512(c)(a)(A)(i) and (ii) mean a general awareness that there are infringements (here, claimed to be widespread and common), or rather mean actual or constructive knowledge of specific and identifiable infringements of individual items."[2334]

The court first quoted extensively from the legislative history of the DMCA safe harbors, then observed that the "tenor of the foregoing provisions is that the phrases 'actual knowledge that the material or an activity" is infringing, and "facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough."[2335] The court then reviewed existing case law on the Section 512(c) safe harbor and found it to support a similar conclusion: "if a service provider knows (from notice from the owner, or a 'red flag') of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement. General knowledge that infringement is 'ubiquitous' does not impose a duty on the service provider to monitor or search its service for infringements."[2336]

The court rejected the plaintiffs' heavy reliance on the Supreme Court's Grokster case, finding that case's explication of the more general law of contributory liability, and its application to peer-to-peer filing sharing networks (which the court observed are not covered by the DMCA Section 512(c) safe harbor), to be of little applicability in the instant case.[2337] Said the court:

> The Grokster model does not comport with that of a service provider who furnishes a platform on which its users post and access all sorts of materials as

[2332] 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

[2333] Id. at 518.

[2334] Id. at 519.

[2335] Id. at 523.

[2336] Id. at 525.

[2337] Id. at 525-26.

> they wish, while the provider is unaware of its content, but identifies an agent to receive complaints of infringement, and removes identified material when he learns it infringes. To such a provider, the DMCA give a safe harbor, even if otherwise he would be held as a contributory infringer under the general law. In this case, it is uncontroverted that when YouTube was given the notices, it removed the material. It is thus protect "from liability for all monetary relief for direct, vicarious and contributory infringement" subject to the specific provisions of the DMCA. Senate Report at 40, House Report at 50.[2338]

The court then rejected a number of other arguments made by the plaintiffs. First, the plaintiffs asserted that the replication, transmittal and display of videos on YouTube did not constitute infringement "by reason of the storage at the direction of a user of material" on the site. The court found that the argument confined the word "storage" too narrowly to meet the statute's purpose. The court noted that the definition of "service provider" protected by the safe harbor includes an entity "offering the transmission, routing, or providing of connections for digital online communications."[2339] The court inferred from this definition that "the provision of such services, access, and operation of facilities were meant to be within the safe harbor when they flow from the material's placement on the provider's system or network: it is inconceivable that they are left exposed to be claimed as unprotect infringements."[2340] The court agreed with the ruling in Io Group v. Veoh[2341] that "by reason of" in the Section 512(c) safe harbor means "as a result of" or "something that can be attributed to."[2342]

Second, the court rejected the plaintiffs' argument that YouTube did not qualify for the safe harbor because it derived a financial benefit directly attributable to the infringing activity, over which it had the right and ability to control. The court held that the "right and ability to control" the activity requires knowledge of it, which must be item-specific. A service provider must know of a specific infringement before the service provider can control it.[2343] Under the court's logic with respect to this knowledge requirement, so long as YouTube acted to take down infringing material once it received specific knowledge of it (including through red flags), the financial benefit prong would not provide an independent basis on which to disqualify the safe harbor.

Third, the court rejected a number of other smaller bases asserted by the plaintiffs as disqualifying YouTube from the safe harbor:

– The court found YouTube's repeat infringer policy to be reasonable when it counted as only one strike against a user both a single DMCA take-down notice identifying multiple videos

---

[2338] Id. at 526.

[2339] Id. at 526.

[2340] Id. at 526-27.

[2341] 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

[2342] YouTube, 718 F. Supp. 2d at 527.

[2343] Id.

uploaded by the user and multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period.[2344]

– The court also found reasonable YouTube's treatment of takedowns resulting from its "Claim Your Content" system. YouTube used Audible Magic technology to remove an offending video automatically if it matched some portion of a reference video submitted by a copyright owner who had designated the service. It also removed a video if the rightsholder operated a manual function after viewing the infringing video. YouTube assigned strikes only when the rightsholder manually requested the video to be removed. In addition, the court found YouTube's initial hesitation in counting manual removals as strikes to be reasonable. YouTube's six month delay in counting such strikes was needed to monitor the system's use by rightsholders, and for engineering work to assure that strikes would be assigned accurately.[2345]

Finally, in an important ruling, the court rejected the plaintiffs' complaint that YouTube removed only the specific clips identified in DMCA notices, and not other clips which infringed the same works. The plaintiffs pointed to the provision in Section 512(c)(3)(A)(ii) that permits a representative list of infringing works at the site. The court ruled that this "representative list" provision would eviscerate the required specificity of notice if it were construed to mean a merely generic description (such as "all works by Gershwin") would be adequate without also giving the works' location at the site, and would put the provider to the factual search forbidden by Section 512(m).[2346] "Although the statute states that the 'works' may be described representatively, 512(c)(3)(A)(ii), the subsection which immediately follows requires that the identification of the infringing material that is to be removed must be accompanied by 'information reasonably sufficient to permit the service provider to locate the material.'"[2347]

Accordingly, the court granted summary judgment to the defendants that they qualified for the Section 512(c) safe harbor.[2348]

The Second Circuit's Opinion

On appeal, the Second Circuit affirmed in part and reversed in part in a very important opinion. The Second Circuit concluded that the district court correctly held that the Section 512(c) safe harbor requires knowledge or awareness of specific infringing activity, but vacated the order granting summary judgment because a reasonable jury could find that YouTube had actual knowledge or awareness of specific infringing activity on its web site.[2349]

[2344] Id. at 527-28.

[2345] Id. at 528.

[2346] Id. at 528-29.

[2347] Id. at 529.

[2348] Id.

[2349] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).

The Second Circuit turned first to the applicability of the Section 512(c) safe harbor.[2350] The court noted that, with respect to applicability of the safe harbor, the most important question on appeal was whether the safe harbor requires actual knowledge or awareness of facts or circumstances indicating specific and identifiable infringements, as opposed to merely a general awareness that infringing activity is or may be present on the web site. The court concluded that the text of Section 512(c) requires knowledge or awareness of specific infringing activity. The court noted that the nature of the removal obligation in Section 512(c)(1)(A) itself contemplates knowledge or awareness of specific infringing material, because expeditious removal would be possible only if the service provider knows with particularly which items to remove.[2351] "Indeed, to require expeditious removal in the absence of specific knowledge or awareness would be to mandate an amorphous obligation to 'take commercially reasonable steps' in response to a generalized awareness of infringement. Such a view cannot be reconciled with the language of the statute, which requires 'expeditious[]' action to remove or disable '*the material*' at issue."[2352]

The court rejected Viacom's argument that the "red flag" provision of Section 512(c) must require less specificity of knowledge than the actual knowledge provision in order to give rise to a duty to act, else the red flag provision would be superfluous. The court concluded that requiring actual knowledge or awareness of specific instances of infringement does not render the red superfluous, because the phrase "actual knowledge" in Section 512(c)(1)(A)(i) is frequently used to denote subjective belief, whereas the language of "facts or circumstances" appearing in Section 512(c)(1)(A)(ii) is often used to denote an objective reasonableness standard.[2353]

> The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or "subjectively" knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement "objectively" obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.[2354]

Accordingly, the Second Circuit affirmed "the District Court's holding that actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor."[2355]

[2350] Id. at 28.

[2351] Id. at 30.

[2352] Id. at 30-31 (emphasis in original) (citations omitted).

[2353] Id. at 31.

[2354] Id.

[2355] Id. at 32.

Applying these standards, the court next turned to whether the district court had correctly granted summary judgment based on the facts of the case. The plaintiffs cited evidence that YouTube employees conducted web site surveys and estimated that 75-80% of all YouTube streams contained copyrighted material, and that Credit Suisse, acting as financial advisor to Google, estimated that more than 60% of YouTube's content was "premium" copyrighted content and that only 10% of the premium content was authorized. The court held that such estimates were insufficient, standing alone, to create a triable issue of fact as to whether YouTube actually knew, or was aware of facts or circumstances that would indicate, the existence of particular instances of infringement.[2356]

The plaintiffs also relied upon internal YouTube communications that referred to particular clips or groups of clips, citing an email from the director of video partnerships for Google and YouTube, requesting that his colleagues calculate the number of daily searches for the terms "soccer," "football," and "Premier League" in preparation for a bid on the global rights to Premier League content. On another occasion he requested that any "clearly infringing, official broadcast footage" from a specific list of top Premier League clubs be taken down in advance of a meeting with the heads of several major sports teams and leagues. YouTube ultimately decided not to make a bid for the Premier League rights, but the infringing content allegedly remained on the web site. In addition, one of the YouTube founders prepared a report in March 2006 stating that "[a]s of today[,] episodes and clips of the following well-known shows can still be found [on YouTube]: Family Guy, South Park, MTV Cribs, Daily Show, Reno 911, [and] Dave Chapelle [sic]." He further opined that, "although YouTube is not legally required to monitor content … and complies with DMCA takedown requests, we would benefit from *preemptively* removing content that is illegal and likely to attract criticism." He also noted that "a more thorough analysis" of the issue would be required.[2357]

The court held that a reasonable juror could conclude from the March 2006 report that the founder knew of the presence of Viacom-owned material on YouTube, since he presumably located specific clips of the shows in question before he could announce that YouTube hosted the content "as of today." A reasonable juror could also conclude that he believed the clips he located to be infringing since he referred to them as "blatantly illegal," and that YouTube did not remove the content from the web site until "a more thorough analysis," thus exposing the company to liability in the interim. The court also pointed to other email exchanges between founder Chad Hurley and Steven Chen, in which Hurley identified specific copyrighted material that should be taken down but Chen requested that the material stay up a bit longer, in one instance suggesting that a CNN space shuttle clip remain up until "we're bigger and better known."[2358] Based upon this various evidence, the court concluded that the plaintiffs "may have raised a material issue of fact regarding YouTube's knowledge or awareness of specific instances of infringement."[2359] Accordingly, the court vacated the district court's order granting summary

---

[2356] Id. at 32-33.

[2357] Id.

[2358] Id. at 33-34.

[2359] Id. at 34.

judgment and instructed the district court to determine on remand whether any specific infringements of which YouTube had knowledge or awareness corresponded to the specific clips that were in suit.[2360]

The Second Circuit next turned to an issue of first impression – the application of the common law doctrine of willful blindness in the DMCA context – raised by the plaintiffs' argument that the district court also erred in granting summary judgment because there was evidence that YouTube was willfully blind to specific infringing activity, which should be treated as tantamount to knowledge. The court noted that, as a general matter of statutory interpretation, a statute should be interpreted to abrogate a common law principle only if the statute speaks directly to the question addressed by the common law. The DMCA provision most relevant to the abrogation inquiry, in the court's view, was Section 512(m), which provides that safe harbor protection is not conditioned upon a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.[2361] The court noted that Section 512(m) "is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring."[2362] However, that fact did not end the abrogation inquiry because willful blindness cannot be defined as an affirmative duty to monitor. The court ruled:

> Because the statute does not 'speak[] directly' to the willful blindness doctrine, § 512(m) limits – but does not abrogate – the doctrine. Accordingly, we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.[2363]

Because the district court had not expressly addressed the principle of willful blindness or its relationship to the DMCA safe harbors, the Second Circuit instructed the district court to consider on remand the fact question of whether the defendants made a deliberate effort to avoid guilty knowledge of infringement.[2364]

The Second Circuit then turned to the issue of the right and ability to control infringing activity. Under Section 512(c)(A)(B), a service provider loses the safe harbor if it receives a financial benefit directly attributable to the infringing activity in a case in which the service provider has the right and ability to control such activity. The Second Circuit rejected the district court's importation of a knowledge element into the control test on the ground that the service provider must know of the particular infringement before he can control it. The court was troubled by the fact that importing a specific knowledge requirement into Section 512(c)(1)(B) would render the control provision duplicative of Section 512(C)(1)(A): "Any service provider

---

[2360] Id.

[2361] Id. at 34-35.

[2362] Id. at 35.

[2363] Id.

[2364] Id.

that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal."[2365]

The Second Circuit also rejected the construction urged by the plaintiffs – that the control provision codifies the common law doctrine of vicarious copyright liability. The court noted the general rule with respect to common law codification that when Congress uses terms that have accumulated settled meaning under the common law, a court should infer, unless the statute otherwise dictates, that Congress meant to incorporate the established meaning of those terms.[2366] The Second Circuit noted that under the common law vicarious liability standard, "[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise."[2367] However, to adopt that principle in the DMCA context would render the statute internally inconsistent, because Section 512(c) actually presumes that services providers have the ability to block access to infringing material. Indeed, the safe harbor requires the services provider to remove or disable access to material once it has knowledge or awareness of infringing material. But in taking such action, the service provider would – under the plaintiffs' proposed construction – be admitting the right and ability to control the infringing material. Thus, the prerequisite to safe harbor protection under Sections 512(c)(1)(A)(iii) & (C) would at the same time be a disqualifier under Section 512(c)(1)(B).[2368]

In view of this predicament, the Second Circuit concluded that the control provision dictates a departure from the common law vicarious liability standard, and ruled that the right and ability to control infringing activity under Section 512(c)(1)(B) requires something more than the ability to remove or block access to materials posted on a service provider's web site. The court refused to elaborate, however, on what that "something more" might be, choosing instead simply to recite two examples of "something more" that would satisfy the control provision. First, the court cited the only court decision that as of the time had found a service provider had the right and ability to control infringing activity.[2369] In Perfect 10, Inc. v. Cybernet Ventures, Inc.,[2370] the district court found control where the service provider instituted a monitoring program by which user web sites received detailed instructions regarding issues of layout, appearance, and content. The service provider also forbad certain types of content and refused access to users who failed to comply with its instructions.[2371]

[2365] Id. at 36. The Second Circuit's reasoning seems flawed on this point, in that a service provider could obtain financial benefit from infringing activity before it became specifically aware of the infringing material and then acted to remove it.

[2366] Id. at 36-37.

[2367] Id. at 37 (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001)).

[2368] Viacom, 676 F.3d at 37.

[2369] Id. at 37-38.

[2370] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[2371] Id. at 1173.

As a second example, the Second Circuit noted that inducement of copyright infringement as enunciated in the Supreme Court's Grokster decision, which premises liability on purposeful, culpable expression and conduct, might also rise to the level of control under Section 512(c)(1)(B).[2372] The court noted that both of its examples involve a service provider "exerting substantial influence on the activities of users, without necessarily – or even frequently – acquiring knowledge of specific infringing activity."[2373] In view of its holding that the control requirement does not include a specific knowledge requirement, the Second Circuit remanded to the district court to consider in the first instance whether the plaintiffs had adduced sufficient evidence to allow a reasonable jury to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity.[2374]

The Second Circuit next turned to an analysis of what activities fall within Section 512(c)'s safe harbor for infringement "by reason of the storage at the direction of a user" of material residing on the service provider's system or network. The Second Circuit affirmed the district court's holding with respect to three of the challenged software functions at issue – the transcoding of videos into a standard display format, the playback of videos on "watch" pages, and the "related videos" function. The court remanded for further fact finding with respect to a fourth software function, involving the third party syndication of videos uploaded to YouTube.[2375]

The court first noted that the structure of the two alternative definitions of "service provider" suggest that the safe harbors of Section 512(c) do not exclude all activity that involves modification of user posted content. Specifically, although the definition of "service provider" that applies to the Section 512(a) safe harbor requires that there be no modification of content of the material being transmitted by the service provider, the definition of "service provider" applicable to Section 512(c) does not contain that limitation. Accordingly, the court found it apparent that the Section 512(c) safe harbor was intended to cover more than mere electronic storage lockers. Instead, the court pointed to various previously decided safe harbor cases as establishing that the safe harbor extends to software functions performed for the purpose of facilitating access to user stored material. One of those cases had expressly considered two of the software functions challenged here – automatic transcoding and playback – and found liability arising from those functions to have occurred "by reason of the storage at the direction of a user." The Second Circuit therefore ruled that the district court had correctly found that to exclude those automated functions from the safe harbor would eviscerate the protection afforded by Section 512(c).[2376]

A similar analysis applied to the "related videos" function, by which a YouTube computer algorithm identified and displayed thumbnails of clips that were related to the video

---

[2372] Viacom, 676 F.3d at 38.

[2373] Id.

[2374] Id.

[2375] Id. at 38-39.

[2376] Id. at 39.

selected by the user. The court rejected the plaintiffs' argument that this practice constituted content promotion, not "access" to stored content. The record established that the related videos algorithm was fully automated and operated solely in response to user input without the active involvement of YouTube employees. The related videos function served to help YouTube users locate and gain access to material stored at the direction of other users. Because the algorithm was closely related to, and followed from, the storage itself, and was narrowly directed toward providing access to material stored at the direction of users, the Second Circuit concluded that the related videos function was protected by the Section 512(c) safe harbor.[2377]

The court then considered the syndication function, under which YouTube had transcoded a select number of videos into a format compatible with mobile devices and syndicated or licensed the videos to Verizon Wireless and other companies. The plaintiffs argued – with some force, the court noted – that business transactions do not occur at the "direction of a user" when they involve the manual selection of copyrighted material for licensing to a third party. The parties did not dispute, however, that none of the clips in suit were among the approximately 2,000 videos provided to Verizon Wireless. The court therefore held that, in order to avoid rendering an advisory opinion on the outer boundaries of the storage provision, it should remand for fact finding on the question of whether any of the clips in suit were in fact syndicated to any other third party.[2378]

Finally, the Second Circuit addressed the plaintiffs' argument that YouTube's repeat infringer policy was inadequate because YouTube had deliberately set up its proprietary identification tools to try to avoid identifying infringements of the plaintiffs' works by permitting only designated "partners" to gain access to those identification tools by which YouTube would conduct network searches and identify infringing material. The court rejected this argument, noting that Section 512(m) provides that the Section 512(c) safe harbor is not conditioned on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, expect to the extent such monitoring comprises a "standard technical measure" within the meaning of Section 512(i). The court noted that, while refusing to accommodate or implement a "standard technical measure" exposes a service provider to liability, refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result. In this case, the plaintiffs had made no argument that YouTube's content identification tools constituted "standard technical measures," and YouTube could therefore not be excluded from the safe harbor by dint of a decision to restrict access to its proprietary search mechanisms.[2379]

p. Perfect 10 v. Google

The rulings of this case with respect to the Section 512(c) safe harbor are discussed in Section III.C.6(b)(1)(ii) above.

[2377] Id. at 39-40.

[2378] Id. at 40.

[2379] Id. at 40-41.

q. Wolk v. Kodak Imaging Network

In Wolk v. Kodak Imaging Network, Inc.,[2380] the plaintiff sought a preliminary injunction against the Photobucket web site preventing it from infringing on copyrights in her photographs. The plaintiff had submitted various notices to Photobucket requesting that images infringing her copyrights be taken down, some of which complied with the DMCA notice requirements and some of which did not. Where a DMCA compliant notice was submitted, Photobucket took down the allegedly infringing photo. Photobucket also had taken down photos where the plaintiff had sufficiently identified the alleged infringements, even if the notice was not DMCA compliant. Despite these removals, the plaintiff contended that more infringing photos remained on Photobucket, although she had not provided DMCA compliant notices to remove them.[2381]

Photobucket relied on the Section 512(c) safe harbor as a shield against the broad preliminary injunction sought by the plaintiff. The court ruled that Photobucket had satisfied all the predicate conditions of Sections 512(i) and 512(k) for the safe harbor. The plaintiff argued that her past notices of infringement also served as DMCA compliant notice of other present and future alleged infringements of the same copyrighted works posted at different times and at different locations. She contended, in essence, that Photobucket was now aware that her copyrights were being infringed on its site, and it was thereafter required to police its site to uncover current infringements and prevent future infringements, without her providing DMCA compliant notices in each instance. The court rejected this attempt to shift the burden of policing from the plaintiff to Photobucket, citing Section 512(m)(1) and several cases holding that the underlying purpose of the notice requirements of the DMCA was to place the burden of policing copyright infringement on the owner of the copyright. Without receiving notices identifying and locating each instance of infringement, Photobucket did not have actual knowledge of the infringements or awareness of facts or circumstances from which infringing activity was apparent.[2382]

The court also concluded that Photobucket was not disqualified from the Section 512(c) safe harbor, in that it did not have the right or ability to control the posting of infringing photos on its site and did not receive a direct financial benefit from the alleged infringing activity. The court noted that a right and ability to control may take the form of prescreening content, providing extensive advice to users regarding content, and editing user content, but Photobucket did not engage in any of such activities (and the size of its web site curtailed its ability to do so). The court rejected the plaintiff's argument that Photobucket received financial gain through its relationship with Kodak, under which it received a share of sales derived from Photobucket. The court noted that such financial gain was derived from allowing all users access to Kodak's services, not directly and specifically from allowing users to print infringing material.

[2380] 2011 U.S. Dist. LEXIS 27541 (S.D.N.Y. Mar. 17, 2011).

[2381] Id. at *1-2.

[2382] Id. at *4-7, *11-14.

Accordingly, Photobucket was entitled to the Section 512(c) safe harbor, and the court denied the motion for a preliminary injunction.[2383]

The plaintiff subsequently sought summary judgment of infringement against both Photobucket and Kodak – in Kodak's case, for its operation of the Kodak Gallery, which allowed its customers the ability to upload their personal digital photographs, create and store albums to share with family and friends, and to order prints of and products containing their digital photographs. Beginning in 2009, Photobucket and Kodak entered into an agreement that allowed Photobucket users to print images obtained from Photobucket on products available through the Kodak Gallery.[2384]

With respect to Kodak, the plaintiff sought to hold it liable for direct copyright infringement by reproducing unauthorized copies of her images on products available through the Kodak Gallery. The court rejected her claim because there was no evidence of volitional conduct on the part of Kodak required for direct liability. Specifically, the record established that the transfer of information about an order from the Kodak Gallery web site to the fulfillment vendor was done electronically through an automated computer system and that all information displayed on the Kodak Gallery web site, including the simulation of products containing the Photobucket images, was done electronically. There was no dispute that any reproduction, display or transmission of the plaintiff's images by or through the Kodak Gallery web site was an automated process with no human intervention by any employee of the defendants. The fact that the plaintiff's images were copied into product simulations in addition to being transmitted to fulfillment vendors did not constitute a volitional act where the copying was automated. The court also ruled that the display of copyrighted images on the defendant's web site did not demonstrate volition either.[2385]

The court held that Photobucket was entitled to the Section 512(c) DMCA safe harbor. With respect to the threshold conditions of the safe harbor, the court found that Photobucket had an adequate policy to terminate repeat infringers. The evidence established that it had developed a policy, made available on its web site, under which copyright holders could submit a take-down notice and when Photobucket received those notices, both those that included URLs and those that did not, it acted to remove the infringing material. The court rejected the plaintiff's argument that Photobucket failed to accommodate standard technical measures because it afforded its users computer tools that allowed users to obliterate, hide or crop out the copyright watermarks on images uploaded. The court noted that the plaintiff had not suggested that Photobucket advised or encouraged its users to use the photo editing tools to circumvent the copyright notice. In any event, the court found the fact that the watermarks appeared on content on the site suggested that Photobucket did, in fact, accommodate standard technical measures. Although the plaintiff argued that the editing software interfered with standard technical measures, the court noted that it was not Photobucket, but rather users, who would use the editing tools to attempt to circumvent copyright protection measures that were already on the

---

[2383] Id. at *16-19, *25.

[2384] Wolk v. Kodak Imaging Networks, Inc., 840 F. Supp. 2d 724, 728, 730 (S.D.N.Y. 2012).

[2385] Id. at 742-43.

site. Accordingly, the editing tools did not disqualify Photobucket from safe harbor eligibility.[2386]

Turning to the knowledge prong, the court again rejected the plaintiff's argument that her provision of fifteen notices of infringement of nine different works was sufficient to serve as DMCA-compliant notice of any and all other unidentified alleged infringements of those nine works that might appear on the Photobucket site. The court held that notices that do not identify the specific location of the alleged infringement (such as a URL) are not sufficient to confer actual notice on the service provider. In those specific instances where the plaintiff validly notified Photobucket of infringing activity, it was undisputed that Photobucket had acted promptly to take down the infringing material. Even in instances where notices were non-compliant, Photobucket had acted to remove the material.[2387]

With respect to the control and financial benefit prong, the court held that the mere ability to remove or block access to materials on the web site is not sufficient to satisfy the control prong. Rather, "a right and ability to control must take the form of prescreening content, rendering extensive advice to users regarding content and editing user content."[2388] Here, Photobucket had not engaged in any such activity. Although the plaintiff alleged that Photobucket received a financial benefit from infringements from a profit sharing relationship with the Kodak defendants, there was no evidence indicating that either the Kodak defendants or Photobucket capitalized *specifically* because a given image a user selected to print was infringing. Rather, the defendants' profits were derived from the service the provided, not a particular infringement. Further, Photobucket had no knowledge of which images users might select to send to the Kodak defendants to be printed, and, as such, Photobucket had no ability to control whether users requested that infringing material be printed. (The court thus seemingly grafted a knowledge element into the control prong.)[2389]

Next, the court ruled that Photobucket had adequately satisfied the predicate requirement of designating an agent to receive DMCA notifications. Photobucket posted contact information of its agent on its web site, including instructions to send notices to "Copyright Agent" at a listed physical address, email address, or fax. The court held that, although this contact information did not include a name or phone number, the statute mandates that the service provider provide only "substantially the following information" referenced in the statute, and by including the physical address, email address and fax number of the copyright agent, Photobucket had included sufficient information to have properly designated an agent.[2390]

Finally, in some final miscellaneous rulings without much elaboration in the opinion, the court held that under the provisions of Section 512(m), Photobucket had no duty to do the

---

[2386] Id. at 744-45.

[2387] Id. at 746-47.

[2388] Id. at 747-48.

[2389] Id. at 748.

[2390] Id. at 748-49.

policing of its web site for infringements that the Plaintiff suggested, and Photobucket could not be held liable for contributory or vicarious infringement because it was entitled to the Section 512(c) safe harbor. And in any event, the evidence did not support the plaintiff's allegation of contributory infringement because she had not demonstrated Photobucket to have acted with knowledge that it was passing along infringing images to the Kodak defendants, that it acted in concert with the Kodak defendants to infringe upon the plaintiff's copyrights, or that it sought to encourage copyright infringement or promoted its service as a means of circumventing copyright.[2391]

r. Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b). In granting the plaintiff's motion for a preliminary injunction, the court ruled that the defendants were not entitled to the Section 512(c) safe harbor because they had not adopted and reasonably implemented a repeat infringer policy. The owner/operator of the myVidster web site had adopted a definition of "infringer" to mean a user who posted a link to content that was not otherwise publicly available on another web site – i.e., content that was hosted on a password-protected or private web site. The court ruled that this definition did not encompass the law of copyright's definition of "infringer," and therefore any repeat infringer policy based on such a definition could not be adequate. In addition, although the owner/operator removed videos listed in DMCA notices, he did not go any further to terminate users who were the subject of repeat infringement notices.[2392]

s. Capitol Records v. MP3tunes

The case of Capitol Records, Inc. v. MP3tunes, LLC[2393] tested whether the operator of a music "locker" service is liable for infringing music files stored in its users' lockers. The defendant MP3tunes operated a storage service that allowed users to store music files in personal online storage "lockers." Songs uploaded to a user's locker ccould be played and downloaded through any Internet-enabled device. MP3tunes offered free lockers with limited storage space and premium lockers with expanded storage for a subscription fee. The defendant also offered another feature of its web site called "Webload" that allowed a user to enter the web address of a music file stored on a third-party Internet server and transfer the file to the user's locker. MP3 tunes used the standard Content-Addressable Storage system to store music files on its servers. Based on the sequence of data bits in a particular music file, the algorithm created a hash tag as an identification number. If different users uploaded the same song containing identical blocks of data to MP3tunes' servers, those blocks were assigned the same hash tag and typically saved only once. If a user played or downloaded a song from a locker, the storage system used the hash tags associated with the uploaded song to reconstruct the exact file the user originally uploaded to his or her locker.[2394]

[2391] Id. at 749-50.

[2392] Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 82955 at *30-32 (N.D. Ill. July 27, 2011).

[2393] 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

[2394] Id. at 633-34.

MP3tunes also operated a second web site at www.sideload.com, which allowed users to search for free song files. Upon entering a keyword, the site would generate a list of potential matches by searching an index of web sites with free song files and cross-referencing the keywords with information associated with each song file. The index was maintained on MP3tunes' servers. After clicking on a search return, the user was taken to a page where he or she could play the song, follow a link to the third-party web site hosting the song, or download the song to another computer. If the user had a locker on MP3tunes.com, Sideload.com displayed a link that if clicked would "sideload" (download) the song from the third-party web site and save it to his or her locker. Importantly, MP3tunes kept track of the sources of songs in its users' lockers. Thus, MP3tunes could identify the third-party web sites from which users copied songs to their lockers. Sideload servers automatically generated lists of "Most Popular," "Featured," and "New" songs that users could browse.[2395]

Sideload.com also offered users free Sideload plug-in software. When a user of the plug-in came across a web site with a free song file, a button appeared on that site that would copy the song directly to the user's MP3tunes locker without visiting Sideload.com. When a user sideloaded a song from a third-party site, either through the Sideload plug-in or the Webload software, that third-party site was added to Sideload.com's index of searchable songs. Information associated with the song, such as artist, album, title, and track was automatically stored on a "Track Details" page, and the information became part of the searchable index. From then on, Sideload.com returned a potential match whenever any other user searched for that song on Sideload.com by entering keywords that matched the song file. When a downloadable song was removed from a third-party source, the Sideload feature became inoperable and users could no longer add the song to their lockers. However, users who sideloaded the song before it was removed from the third-party source could continue to access the song through their lockers.[2396]

The plaintiff record labels sought to hold MP3tunes liable for copies of infringing music files stored in their lockers and MP3tunes asserted the Section 512(c) safe harbor. One of the plaintiffs, EMI, had submitted a notice of infringement identifying 350 song titles and web addresses that allegedly infringed EMI's copyrights. It also provided a list of EMI artists and demanded that MP3tunes remove all of EMI's copyrighted works, even those not specifically identified with web addresses. MP3tunes removed links to the specific web addresses but did not remove infringing songs from its users' lockers. MP3tunes requested that EMI identify any other infringing links, which EMI declined to do, asserting that its representative list was sufficient to obligate MP3tunes to take down all other infringing material.[2397]

EMI argued that MP3tunes had not satisfied the predicate conditions of Section 512(i) to qualify for the safe harbors because it had purposefully blinded itself to its users' infringement and failed to take any action against hundreds of users who sideloaded copies of songs identified in EMI's takedown notices. MP3tunes countered this argument by noting that it had terminated

---

[2395] Id. at 634.

[2396] Id. at 634-35.

[2397] Id. at 635.

the accounts of 153 repeat infringers who violated copyrights by sharing the contents of their lockers with other users.[2398]

The court analyzed whether MP3tunes had satisfied the predicate conditions of Section 512(i) by drawing a distinction between "(1) users who know they lack authorization and nevertheless upload content to the internet for the world to experience or copy, and (2) users who download content for their personal use and are otherwise oblivious to the copyrights of others. The former are blatant infringers that internet service providers are obligated to ban from their websites. The latter, like MP3tunes users who sideload content to their lockers for personal use, do not know for certain whether the material they download violates the copyrights of others."[2399] The court noted several cases (the Viacom, Io Group, and Corbis cases) requiring the termination of users who repeatedly upload copyrighted material to service providers' web sites, but absolving services providers from policing users who merely consume that content. The court also noted that, unlike in the Aimster case, MP3tunes had not purposefully blinded itself to its users' identities and activities. Rather, MP3tunes had tracked the source and web address of every sideloaded song in its users' lockers and could terminate the accounts of repeat infringers, which it had done in 153 instances. Finally, the court found that MP3 tunes had demonstrated it had a procedure for responding to DMCA takedown notices, and had used such procedure to remove all of the specific web addresses containing infringing files that EMI had identified.[2400]

The court rejected EMI's argument that MP3tunes had an obligation to terminate any user who added multiple links to Sideload.com that appeared on one or more takedown notices because they were automatic repeat infringers. The court noted that takedown notices themselves are not evidence of blatant infringement and users could not be certain that they had downloaded infringing content. Thus, MP3tunes' decision to refrain from termination those user accounts was appropriate. Accordingly, the court ruled that MP3tunes had satisfied the predicate conditions of Section 512(i) for eligibility for the safe harbors.[2401]

Turning to the specifics of the Section 512(c) safe harbor, the court first rejected EMI's argument, relying on Section 301(c) of the copyright statute,[2402] that the safe harbors do not apply to songs recorded prior to Feb. 15, 1972. Although noting it was an issue of first impression, the court concluded that there is no conflict between Section 301 and the DMCA's safe harbors for infringement of pre-1972 recordings. The text of the DMCA limits immunity for the "infringement of copyrights" without drawing any distinction between federal and state law. Although Section 501(a) of the copyright statute makes anyone violating the rights established by Sections 106 through 122 an infringer, that section does not suggest that its list of

---

[2398] Id. at 638.

[2399] Id.

[2400] Id. at 638-39.

[2401] Id. at 639.

[2402] Section 301(c) states, "With respect to sound recordings first fixed before February 15, 1972, any rights or remedies under the common law or statute of any State shall not be annulled or limited by this title until February 15, 2067."

acts constituting infringement is all inclusive. The court also noted that the DMCA was enacted to clarify copyright law for Internet service providers in order to foster fast and robust development of the Internet. Limiting the DMCA to recordings after 1972 would spawn legal uncertainty and subject otherwise innocent Internet service providers to liability for the acts of third parties. Accordingly, the court concluded that the DMCA's safe harbors, read in the light of their purpose, cover both state and federal copyright claims and apply to sound recordings fixed prior to Feb. 15, 1972.[2403]

Turning to the sufficiency of EMI's takedown notices, the court held that a notice merely stating "all songs" by a particular artist, or some other vague descriptor and nothing more, is inadequate to trigger a takedown obligation because it does not enable the service provider to locate the allegedly infringing material. Service providers must take down the specific infringing material identified in the notice but as a general matter are not required to search for and take down other material that may infringe the identified copyrighted works.[2404] However, in this instance:

> MP3tunes was obligated to remove specific works traceable to users' lockers. Because MP3tunes keeps track of the source and web address for each sideloaded song in each user's locker, EMI's notices gave sufficient information for MP3tunes to locate copies of infringing songs in user lockers. … Where service providers such as MP3tunes allow users to search for copyrighted works posted to the internet and to store those works in private accounts, to qualify for DMCA protection, those service providers must (1) keep track of the source and web address of stored copyrighted material, and (2) take content down when copyright owners identify the infringing sources in otherwise compliant notices.[2405]

The court held that there was no genuine dispute that MP3tunes did not qualify for safe harbor protection for songs stored in users' lockers that were sideloaded from the unauthorized web sites identified in takedown notices.[2406]

The court then turned to the question whether MP3tunes was disqualified from the Section 512(c) safe harbor by virtue of having actual or "red flag" knowledge of infringement with respect to which it failed to act. The court noted that the knowledge provisions are designed to deny safe harbor protection to Internet service providers operating or linking to pirate sites whose illegal purpose is obvious to a reasonable person, but general awareness of rampant infringement is not enough to disqualify a service provider of protection. EMI argued that MP3tunes had red flag knowledge in part because its executives sideloaded songs by popular

---

[2403] MP3tunes, 821 F. Supp. 2d at 640-42.

[2404] Id. at 642.

[2405] Id. at 642-43. The court rejected MP3tunes concern for liability if it removed material from its users' lockers, noting that MP3tunes' Terms of Use clearly authorized it to block a user's access to material in lockers. The court also noted the immunity afforded by the DMCA under Section 512(g) to service providers who remove infringing material. Id. at 643.

[2406] Id.

artists from obviously infringing sites like rapidshare.com, fileden.com and filefactory.com. The court noted, however, that those sites do not use words like "pirate" or "bootleg" or other slang to indicate their illegal purpose and are not otherwise clearly infringing. Nor did the DMCA place the burden of investigation on MP3tunes to determine whether those sites were not authorized to distribute EMI's copyrighted works.[2407] Said the court, "Put another way, if investigation is required to determine whether material is infringing, then those facts and circumstances are not 'red flags.'"[2408] Because EMI itself regularly distributed work on the Internet for free, MP3tunes' executives and other Internet users had no way of knowing for sure whether free songs on the Internet were unauthorized. Accordingly, there was no genuine issue that MP3tunes did not have specific red flag knowledge with respect to any particular link on Sideload.com, other than the specific URLs noticed by the plaintiffs.[2409]

The court also ruled that MP3tunes was not disqualified from the safe harbors by virtue of having control and a financial benefit over the infringing activity. As to direct benefit, while Sideload.com could be used to draw users to MP3tunes.com and drive sales of pay lockers, it had noninfringing uses and MP3tunes did not promote infringement. Any link between infringing activity and a direct benefit to MP3tunes was attenuated because sideloaded songs were stored free of charge and infringing and noninfringing users of Sideload.com paid precisely the same or nothing at all for locker services. Nor did MP3tunes have control over its users' activity because its users alone chose the web sites they linked to Sideload.com and the songs they sideloaded and stored in their lockers.[2410] In sum, the court concluded, "there is no genuine dispute that MP3tunes may claim safe harbor protection for EMI works stored on MP3tunes.com and EMI works linked to Sideload.com. However, MP3tunes does not qualify for safe harbor protection for songs sideloaded from links identified in [EMI's] takedown notices which it failed to remove from user lockers."[2411]

The court went on to hold that MP3tunes could have contributory liability for the that infringing material that remained in users' lockers and for which it had received notices of infringement. The takedown notices from EMI were sufficient to establish no genuine dispute that MP3tunes had actual knowledge its users had stored and continued to have access to infringing copies of the plaintiffs' works. And MP3tunes had made a material contribution to the infringing activity because its servers were the sole instrumentality of its users' infringement. The court rejected MP3tunes assertion of the Sony defense that its servers and lockers had substantial noninfringing uses because MP3tunes had a continuing relationship with its users. Here, MP3tunes continued to allow its users to store and access works in their lockers even though it knew they had unlawfully downloaded those works. The court therefore granted EMI's motion for summary judgment on its claim for contributory infringement with respect to the

---

[2407] Id. at 643-44.

[2408] Id. at 644.

[2409] Id. at 644-45.

[2410] Id. at 645.

[2411] Id. at 646.

songs listed on EMI's takedown notices and which MP3tunes failed to remove from users' lockers.[2412]

Finally, EMI argued, relying on the Cartoon Networks case, that MP3tunes' storage system violated its right to public performance because it employed a "master copy" to "rebroadcast" songs to users who uploaded different copies of the same song.[2413] In a ruling that is a bit unclear in its factual rationale, the court rejected this argument:

> EMI's argument, however, mischaracterizes MP3tunes' storage system. The record demonstrates that MP3tunes does not use a "master copy" to store or play back songs stored in its lockers. Instead, MP3tunes uses a standard data compression algorithm that eliminates redundant digital data. Importantly, the system preserves the exact digital copy of each song uploaded to MP3tunes.com. Thus, there is no "master copy" of any of EMI's songs stored on MP3tunes' computer servers.[2414]

Accordingly, MP3tunes was entitled to safe harbor protection again EMI's public performance infringement claims.

In sum, the court granted EMI's motion for summary judgment on its claim of contributory infringement against MP3tunes for songs noticed in EMI's takedown notices and not removed from user lockers. The court granted MPetunes' motion for summary judgment on its defense under the DMCA safe harbors with respect to all claims of infringement except with respect to songs noticed in EMI's takedown notices and not removed from user lockers.[2415]

t. Obodai v. Demand Media

In this case, the owner of a copyrighted work sought to hold the operator of a humor website, Cracked.com, liable for the posting of the plaintiff's work by a third party. The plaintiff did not notify the defendant that the third party had posted the plaintiff's work on Cracked.com before filing suit pro se. The court ruled that the defendant satisfied all the requirements for the Section 512(c) safe harbor. The defendant had adequately adopted and implemented a policy to terminate repeat infringers because Section 16 of its web site Terms and Conditions stated that Cracked could terminate any account or user for repeated infringement of intellectual property

[2412] Id. at 648-49. The court also ruled that the founder was personally directly liable for songs her personally sideloaded from unauthorized sites. However, MP3tunes was not directly liable for his or other executives' sideloading of songs because it was not clear they downloaded those songs during the course of their employment. Id. at 649.

[2413] Id. at 649.

[2414] Id. at 649-50.

[2415] Id. at 650-51.

rights, including copyrights, and reserved the right to terminate an account or user for even one instance of infringement.[2416]

With respect to the requirement that the service provider accommodate and not interfere with standard technical measures, the court noted that an example of a party's failure to comply with standard technical measures may include conduct that advises or encourages users to conceal a work's copyrighted status. To the extent the plaintiff contested this issue, the plaintiff argued that Cracked distributed copyrighted texts and entered into some form of a distribution agreements. The court noted that, while probative of other relevant considerations, these facts were not evidence of interference with standard technical measures under the DMCA.[2417]

Turning to the knowledge prong of Section 512(c), the court rejected the plaintiff's argument that Cracked had knowledge of the infringement based on keyword-targeted advertisements that appeared with the posts of the plaintiff's work by the third party. Even assuming arguendo that the ads were not automatically generated, the court ruled that the existence of such ads did not reflect awareness that the postings had infringed. The plaintiff also argued that Cracked used a software tool called Tynt to measure search engine traffic to specific pages. The court concluded that such a tool does not support an inference that the defendant was aware of infringement, and instead was relevant only as to the defendant's knowledge as to visitors' pageviews. Nor was the fact that the defendant had previously received a considerable number of DMCA takedown notices from copyright holders sufficient in view of the Second Circuit's ruling in Viacom that the defendant must have knowledge that the specific works in dispute were infringing, not merely knowledge or suspicion of broader infringement.[2418]

The court found that the defendant had acted expeditiously to remove the infringing content by taking the content down after the plaintiff filed his complaint but before her served the defendant and had emailed the third party poster informing him of the infringement claim and stating that his profile on Cracked would be deleted. Finally, with respect to the issue of control, the court noted that the defendant's use of Tynt to monitor Cracked traffic reported only on site traffic volume and not the content of user postings, and therefore did not give the defendant control over infringing content. Accordingly, the court ruled that the defendant was entitled to the Section 512(c) safe harbor and entered judgment for the defendant.[2419]

(iv) Referral or Linking to Infringing Material (Information Location Tools) – Section 512(d)

Section 512(d) provides that a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for referring or linking users to an online location

---

[2416] Obodai v. Demand Media, Inc., 2012 U.S. Dist. LEXIS 83109 at *3, 11 (S.D.N.Y. June 13, 2012). The Terms and Conditions also listed the physical and email addresses of its copyright agent and set forth information that a copyright holder should forward if it believed that Cracked contained infringing content. Id. at *24.

[2417] Id. at *13-14.

[2418] Id. at *16-18.

[2419] Id. at *19, 23 & 27.

containing infringing material or activity by using information location tools (including a directory, index, reference, pointer or hypertext link), provided the Service Provider does not have actual knowledge that the material is infringing; is not aware of facts or circumstances from which infringing activity is apparent; does not receive a financial benefit directly attributable to any infringing activity for which it has the right and ability to control; and, if properly noticed of the infringing activity by the copyright holder or its authorized agent, or otherwise obtaining knowledge or awareness of the infringement, responds expeditiously to remove or disable access to the infringing material.[2420] Section 512(d) does not mention framing as an example of an information location tool to which the safe harbor applies. Thus, although framing is accomplished by linking, it is unclear whether framing would fall within the safe harbor.[2421]

The Service Provider can become aware of infringing activity either by notice from the copyright holder (or its authorized agent) or by virtue of other facts or circumstances of which it becomes aware. The same issues of knowledge that were discussed above with respect to the safe harbor of Section 512(c) apply also to the safe harbor of Section 512(d). Specifically, absent direct notice from the copyright holder or its agent, the standard of awareness of infringing activity appears by its terms to require more knowledge on the part of the Service Provider than a "should have known" (or reason to know) standard – it requires that the Service Provider have actual awareness of facts from which infringing activity is apparent. As noted in the discussion of Section 512(c) above, the legislative history describes the standard of awareness as a "red flag" test.

a. The Napster Case

The first case to adjudicate the safe harbor under Section 512(d) was the Napster case, discussed extensively in Section III.C.2(c)(1) above. In that case, Napster asserted that the index

---

[2420] Section 512(d) provides: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider –

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link."

[2421] Ballon & Kupferschmid, supra note 1974, at 8.

it maintained on its servers of MP3 files available on the hard drives of its users constituted an information location tool, and that to the extent the plaintiffs' infringement claims were based on the operation of that index, Napster was entitled to the safe harbor of Section 512(d). The district court, with only a very terse analysis contained entirely in a footnote, ruled that Napster was not entitled to the safe harbor because (I) it had constructive knowledge of infringing activity on its system (thereby failing to satisfy the requirement of Section 512(d)(1)(B))[2422] and (ii) "Defendant has failed to persuade this court that subsection 512(d) shelters contributory infringers."[2423]

On appeal, the Ninth Circuit reversed this ruling of the district court. The Ninth Circuit noted that the district court's ruling that the safe harbor would never apply to a Service Provider that might otherwise be liable as a contributory infringer was contrary to the legislative history of the DMCA.[2424] The Ninth Circuit further stated, "We do not agree that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se. We instead recognize that this issue will be more fully developed at trial. At this stage of the litigation, plaintiffs raise serious questions regarding Napster's ability to obtain shelter under § 512, and plaintiffs also demonstrate that the balance of hardships tips in their favor."[2425]

The Ninth Circuit noted that the following questions would have to be resolved at trial concerning whether Napster was entitled to the safe harbor of Section 512(d): "(1) whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give a service provider 'official' notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies

---

[2422] The district court appears to have misapplied Section 512(d)(1)(B). Because Napster had constructive knowledge of infringing activity, and because Section 512(d)(1)(B) requires that the Service Provider be "not aware of facts or circumstances from which infringing activity is apparent," the district court reasoned that Napster could not qualify for the safe harbor of Section 512(d). However, Section 512(d)(1) contains three prongs, which are stated in the disjunctive, not the conjunctive. Specifically, Section 512(d)(1) requires that the Service Provider have no actual knowledge of infringing material or activity (clause (A)), no awareness of facts or circumstances from which infringing activity is apparent (clause (B)), or "upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material" (clause (C)). Thus, even if a Service Provider has actual or constructive knowledge of infringing activity, so long as the Service Provider acts expeditiously to remove or disable access to the allegedly infringing material upon obtaining such knowledge, the safe harbor is still available. Napster asserted that in every instance in which it had obtained knowledge of infringing activity, it had acted expeditiously to block the account of the user who was allegedly sharing infringing material. Napster's PI Opp. Br., supra note 1389, at 33.

[2423] A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 n. 24 (N.D. Cal. 2000).

[2424] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001) (quoting S. Rep. 105-90, at 40 (1998), which stated: "The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement."). This sentence from the legislative history was also quoted in a discussion of the scope of the DMCA safe harbors by the court in its opinion in In re Verizon Internet Services, Inc., 65 U.S.P.Q.2d 1574 (D.D.C. 2003). The court also stated, in the context of ruling on the scope of the subpoena power under Section 512(h) of the DMCA, that "in exchange for complying with subpoenas under subsection (h), service providers receive liability protection from any copyright infringement – direct or vicarious – by their users." Id. at 1581 n.6.

[2425] Napster, 239 F.3d at 1025.

with § 512(i), which requires a service provider to timely establish a detailed copyright compliance policy."[2426]

b. Perfect 10 v. Cybernet Ventures

The second case to adjudicate the Section 512(d) safe harbor was the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.[2427] As discussed in Section III.C.6(b)(1)(iii)d. above, the court concluded that the defendant Cybernet was not entitled to any of the Section 512 safe harbors because it had failed to satisfy the predicate requirements of Section 512(i). Nevertheless, the court, in a one sentence ruling also concluded that there was "a residual chance that Cybernet will qualify for 17 U.S.C. § 512(d)'s safe harbor for search engines, but not links."[2428] Because the court did not elaborate further, it is difficult to understand why the court reached this conclusion, particularly in view of its rulings with respect to Sections 512(i) and 512(c).

c. The MP3Board Case

Issues relating to the Section 512(d) safe harbor, and particularly its attendant notice requirements, arose in the case of Arista Records, Inc. v. MP3Board, Inc.,[2429] and are discussed below in Section III.D.8.

d. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(d) safe harbor. As discussed in Section III.C.6(b)(1)(i).c above, the district court concluded that Aimster was not entitled to any of the DMCA safe harbors because of its failure to satisfy the Section 512(i) predicate with respect to implementation of a policy to terminate repeat infringers on its system. In addition, the court held that Aimster had not satisfied the specific conditions of Section 512(d) because it had actual and constructive knowledge of the infringing activity for the same reasons that it had such knowledge for purposes of common law contributory liability (see the discussion in Section III.C.2(c)(3) above), and there was no evidence that Aimster had taken steps to remove or disable access to infringing material.[2430] In addition, Aimster received a financial benefit directly attributable to the infringing activity and had the right and ability to control the infringing activity, again for the same reasons that it had such financial benefit and right and ability to control for purposes of common law vicarious liability (see the discussion in Section III.C.3(e) above).[2431] As discussed in Section III.C.6(b)(1)(i).c, on appeal the Seventh Circuit affirmed the

---

[2426] Id. The bases for the district court's doubts about whether Napster satisfied Section 512(i) are discussed in Section C.5(b)(1)(i)a. above with respect to the court's ruling on whether Napster was entitled to the safe harbor of Section 512(a).

[2427] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[2428] Id. at 1182.

[2429] 2002 U.S. Dist. LEXIS (S.D.N.Y. 2002).

[2430] In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 661 (N.D. Ill. 2002).

[2431] Id.

ruling that the safe harbors were not available to Aimster because of failure to comply with Section 512(i).[2432]

e. The Diebold Lawsuit

Diebold was the manufacturer of electronic voting systems that contained a number of flaws. A series of internal Diebold emails acknowledging the flaws were published on the Internet. Diebold sent out dozens of cease and desist letters under the DMCA to websites linking to or publishing the Diebold emails, demanding that the materials, or links to the materials, be removed. The Electronic Frontier Foundation filed suit against Diebold on behalf of one of the ISPs and a news website publisher, arguing that linking to or publishing the materials was a fair use in order to comment on the reliability of electronic voting.[2433] On Nov. 4, 2003, the court ordered Diebold to show why a preliminary injunction should not be issued to prevent Diebold from threatening to sue ISPs. In Dec. 2003, the court dismissed the plaintiffs' motion for the preliminary injunction as moot, after Diebold represented that it no longer demanded that the plaintiffs or any other party cease and desist using Diebold's email archive for noncommercial critical purposes. Diebold also agreed that it would retract all outstanding DMCA safe harbor notifications to ISPs concerning the email archive and would not issue such notifications to any party in any jurisdiction in the future.[2434]

In a subsequent action, one of the ISPs and two individual Swarthmore students who originally posted the Diebold emails on various websites sued Diebold, among other things, to recover damages and attorneys' fees under Section 512(f) of the DMCA on the ground that Diebold's claims of copyright infringement were based on knowing material misrepresentations.[2435] Section 512(f) of the DMCA provides:

> Any person who knowingly materially misrepresents under this section –
>
> (1) that material or activity is infringing, or
>
> (2) that material or activity was removed or disabled by mistake or misidentification,
>
> shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or

---

[2432] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

[2433] "ISP Rejects Diebold Copyright Claims Against News Website," available as of Jan. 17, 2004 at www.eff.org/Legal/ISP_liability/20031016_eff_pr.php. The suit, Online Policy Group v. Deibold, Inc., was filed in federal court in San Jose.

[2434] "Electronic Voting Firm Drops DMCA, Copyright Charges Against ISPs," *Mealey's Litigation Report: Intellectual Property* (Dec. 15, 2003) 13-14.

[2435] Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1198 (N.D. Cal. 2004).

disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

In adjudicating the plaintiff's Section 512(f) claim, the court first had to determine the validity of Diebold's claims that publication of its email archive constituted copyright infringement. The court concluded that publication of at least some of the email archive constituted fair use and was therefore not infringing. With respect to the purpose of the use, the court noted that discussion of problems associated with Diebold's electronic voting machines was clearly in the public interest. Moreover, Diebold had identified no specific commercial purpose or interest affected by publication of the archive, and there was no evidence that Diebold itself had intended to or could profit from such content. Finally, the plaintiffs' use of the material was transformative, in that they used the email archive to support criticism that was in the public interest, not to develop electronic voting technology.[2436] Accordingly, the court ruled that "there is no genuine issue of material fact that Diebold, through its use of the DMCA, sought to and did in fact suppress publication of content that is not subject to copyright protection [because of the fair use doctrine.]"[2437]

The court then turned to whether Diebold knowingly materially misrepresented that publication of the email archive constituted copyright infringement. The parties disputed the meaning of the phrase "knowingly materially misrepresents." The plaintiffs argued that a preliminary injunction standard should be applied – that the court should conclude that Diebold violated Section 512(f) if it did not have a "likelihood of success" on the merits of the a copyright infringement claim when it sent the DMCA letters. Diebold contended that the court should apply a type of Federal Rule of Civil Procedure 11 standard and thus conclude that Diebold did not violation Section 512(f) unless sending the DMCA letters was "frivolous."[2438]

Acknowledging that it was facing an issue of first impression, the court concluded that neither proposed standard was appropriate. A requirement that a party have an objectively measured likelihood of success on the merits in order to assert claims of copyright infringement would impermissibly chill the rights of copyright owners. On the other hand, in requiring a showing of "knowing material misrepresentation," Congress explicitly adopted a standard from Rule 11, which contains a variety of other requirements that are not necessarily coextensive with those of Section 512(f).[2439]

Instead, the court concluded that the statutory language was sufficient clear on its fact and does not require importation of standards from other legal contexts. Citing Black's Law Dictionary, the court held that "knowingly" means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it

---

[2436] Id. at 1203.

[2437] Id.

[2438] Id. at 1204.

[2439] Id.

been acting in good faith, that it was making misrepresentations. "Material" means that the misrepresentation affects the ISP's response to a DMCA letter.[2440]

Under this standard, the court concluded as a matter of law that Diebold knowingly materially misrepresented that the plaintiffs infringed Diebold's copyright interest, at least with respect to the portions of the email archive clearly subject to the fair use exception:

> No reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold's voting machines were protected by copyright, and there is no genuine issue of fact that Diebold knew – and indeed that it specifically intended – that its letters to OPG and Swarthmore would result in prevention of publication of that content. The misrepresentations were material in that they resulted in removal of the content from websites and the initiation of the present lawsuit. The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions – which were designed to protect ISPs, not copyright holders – as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.[2441]

Two weeks after the court rendered its judgment, Diebold agreed to settle the lawsuit by paying $125,000 in damages and fees to the plaintiffs.[2442]

f. Perfect 10 v. CCBill

The facts of this case are set forth in Section III.C.6(b)(1)(i)d. above. In that case, the defendant Internet Key, an age verification service for adult content websites, filed a motion for summary judgment under the Section 512(d) safe harbor. Perfect 10 argued that Internet Key was not entitled to the safe harbor because it was not an information location tool, it had actual knowledge of infringements, and it was aware of facts or circumstances from which infringing activity was apparent.[2443]

With respect to the issue of whether Internet Key was an information location tool, the court rejected Perfect 10's argument that Section 512(d) is limited to OSPs like Google and Yahoo! that provide links to millions of web sites and that do not have contractual relationships

---

[2440] Id.

[2441] Id. at 1204-05. The court also held that the plaintiff's claim that Diebold, through its inappropriate use of the DMCA, had interfered with their contractual relations with their respective ISPs, was preempted. "Even if a copyright holder does not intend to cause anything other than the removal of allegedly infringing material, compliance with the DMCA's procedures nonetheless may result in disruption of a contractual relationship: by sending a letter, the copyright holder can effectuate the disruption of ISP service to clients. If adherence to the DMCA's provisions simultaneously subjects the copyright holder to state tort liability, there is an irreconcilable conflict between state and federal law. Id. at 1205-06.

[2442] "Diebold Settles Landmark DMCA Suit in Dispute Over Voting Machines," *IP Law Bulletin* (Oct. 15, 2004), available as of Oct. 18, 2004 at www.iplawbulletin.com/cgi-bin/absolutenm/anmviewer.asp?a=2381&z=18.

[2443] Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d 1077, 1097-98 (C.D. Cal. 2004).

with their affiliate web sites. Instead, Section 512(d) refers to OSPs who refer or link users to an online location containing infringing material or activity by using a directory, index, reference, point, hypertext link or the like. The court concluded that Internet Key's sexkey.com web site provided that function and was therefore covered by Section 512(d).[2444]

With respect to the knowledge element, Perfect 10 argued that Internet Key should have known that there were copyright infringements on its clients' web sites because of the disclaimers on some of those web sites, which generally claimed that the copyrighted images were in the public domain or that the webmaster was posting the images for newsworthy purposes. The court ruled that these disclaimers were not sufficient to raise a "red flag" of copyright infringement, which is the standard of constructive knowledge under Sections 512(c) and 512(d).[2445]

Turning to the issue of control, the court ruled, citing Costar Group, Inc. v. Loopnet, Inc.[2446] and Perfect 10 v. Cybernet Ventures, Inc.,[2447] that the mere ability to disconnect the webmasters' access to Internet Key's service was not sufficient under the DMCA to demonstrate a right and ability to control the infringing activity. Because no other control had been shown, Internet Key was entitled to summary judgment under the Section 512(d) safe harbor.[2448]

The parties filed an appeal of the rulings in this case with respect to CCBill and CWIE, although not with respect to Internet Key. On appeal, CCBill argued that it should be entitled to the immunity of Section 512(d) because, after processing a consumer's credit card and issuing a password granting access to a client website, it displayed a hyperlink so that the user could access the client website. The Ninth Circuit rejected this argument, noting that, even if the displayed hyperlink could be viewed as an information location tool, Section 512(d) provides a safe harbor only for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or activity. Perfect 10 had not claimed that CCBill infringed its copyrights by providing a hyperlink, but rather through CCBill's performance of other business services for the infringing websites. Accordingly, even if CCBill's provision of a hyperlink were immune under Section 512(d), CCBill could not receive blanket immunity under Section 512(d) for its other services.[2449]

g. Columbia Pictures v. Fung

In Columbia Pictures Industries, Inc. v. Fung,[2450] the defendants operated BitTorrent sites through which users could search indexes for dot-torrent files pointing to infringing movies and

---

[2444] Id.

[2445] Id. at 1098.

[2446] 164 F. Supp. 2d 688, 704 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

[2447] 213 F. Supp. 2d 1146, 1181 (C.D. Cal. 2002).

[2448] Perfect 10 v. CCBill, 340 F. Supp. 2d at 1098.

[2449] Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 765-66 (9th Cir.), cert. denied, 2007 U.S. LEXIS 12812 (2007).

[2450] 2009 U.S. Dist. LEXIS (C.D. Cal. Dec. 21, 2009).

other content. The court found the defendants liable for inducement of infringement and rejected assertion of a safe harbor under Section 512(d). The plaintiffs had established that the defendants had reason to know of their users' infringing activities (plaintiffs' expert testified that approximately 95% of downloads occurring through the defendants' sites were downloads of infringing content) and therefore the defendants had failed to establish the first requirement of the Section 512(d) safe harbor that they were not aware of facts or circumstances from which infringing activity was apparent.[2451] The court found that the defendants also had adequate knowledge of infringing activity under the "red flag" test to have a duty to act to removing links to infringing content. The defendants had not introduced any evidence that they acted expeditiously to remove or disable access to infringing material. In addition, the court held the defendants had failed to raise a triable issue of fact regarding the second requirement of the Section 512(d) safe harbor, because they had received a financial benefit directly attributable to the infringing activity, which acted as a major draw for users to the site and from which the defendants derived revenue, and they had the right and a ability to control such activity.[2452]

Finally, the court ruled that, as a general proposition, "inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business. Here … Defendants are liable for inducement. There is no safe harbor for such conduct."[2453]

h. Perfect 10 v. Google

The rulings of this case with respect to the Section 512(d) safe harbor are discussed in Section III.C.6(b)(1)(ii) above.

(2) General Requirements for Limitations of Liability

In addition to meeting the requirements of one of the specific safe harbors, to be eligible for the limitations of liability, under Section 512(i) the Service Provider must adopt, reasonably implement, and inform subscribers of a policy for the termination in appropriate circumstances of subscribers who are repeat infringers, and must not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works that have been developed "pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process," are available to any person on reasonable and nondiscriminatory terms, and do not impose substantial costs or burdens on Service Providers or their systems.

Most commercial Service Providers have a policy with respect to use of the service by subscribers. The policy may be posted on the Service Provider's website, contained in the

---

[2451] Id. at *17 & *61.

[2452] Id. at *55, *61-66, & *62 n.27..

[2453] Id. at *67-68.

subscription agreement, or both. Operators of corporate intranets will likewise want to post a policy on the intranet itself, and may wish to update employee handbooks or policy manuals to incorporate the policy statements required to take advantage of the safe harbors. All Service Providers should reasonably document their efforts to enforce their policies.

(3) Special Provisions for Nonprofit Educational Institutions

Section 512(e) contains an additional liability limitation for nonprofit educational institutions. According to the Conference Report, Congress recognized that university environments are unique, and a university might otherwise fail to qualify for the safe harbors simply because the knowledge or actions of one of its employees might be imputed to the university under basic principles of respondeat superior and agency law. Based upon principles of academic freedom and independence, Congress believed that in certain circumstances it would be inappropriate for actions online of faculty members and graduate students to be imputed to the university to prevent it from being eligible for the safe harbors.

Accordingly, Section 512(e) provides that online infringing actions of faculty members or graduate student employees that occur when they are "performing a teaching or research function" will not be attributed to the university in its capacity as their employer, and the university will therefore not be charged with such faculty member's or graduate student's knowledge or awareness of his or her infringing activities, if (i) the infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding three-year period, for a course taught at the university by such faculty member or graduate student; (ii) the university has not, within the preceding three-year period, received more than two notifications of claimed infringement by such faculty member or graduate student; and (iii) the university provides all users of its system with informational materials that accurately describe and promote compliance with U.S. copyright law.

(4) Filing of False DMCA Notices – Section 512(f)

Section 512(f) of the DMCA provides:

> Any person who knowingly materially misrepresents under this section –
>
> (1) that material or activity is infringing, or
>
> (2) that material or activity was removed or disabled by mistake or misidentification,
>
> shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

In Twelve Inches Around Corp. v. Cisco Sys.,[2454] the court ruled that Section 512(f) does not apply to misrepresentations of trademark infringement on a website.

(i) Rossi v. MPAA

The first case to adjudicate the scope of Section 512(f) was that of Rossi v. MPAA.[2455] A discussion of the Ninth Circuit's rulings with respect to Section 512(f) may be found in Section III.C.6(b)(1)(iii).g above.

(ii) Online Policy Group v. Diebold, Inc.

The second case to adjudicate the scope of Section 512(f) was that of Online Policy Group v. Diebold, Inc.[2456] A discussion of the court's rulings with respect to Section 512(f) may be found in Section III.C.6(b)(1)(iv).e above.

(iii) Dudnikov v. MGA Entertainment

In Dudnikov v. MGA Entertainment, Inc.,[2457] the court ruled that a request by the defendant to eBay to take down the auction of a fleece hat with a Bratz appliqué on it did not give rise to a claim under Section 512(f) because the defendant acted in a good faith belief that the sale of the hat infringed its copyright and trademark rights and the plaintiffs had failed to satisfy their burden of demonstrating that the defendant knowingly and materially misrepresented that the plaintiffs' auction was infringing. The court rejected the plaintiffs' argument that a higher standard of good faith should be applied just because the defendant's agent who issued the takedown notice was a lawyer trained in intellectual property law.[2458]

(iv) Novotny v. Chapman

In Novotny v. Chapman,[2459] the defendant made instructional videos in which he demonstrated a particular method of cutting women's hair. In 2002, he entered into an agreement with the plaintiffs in which he would deliver originals of his video to the plaintiffs, who would then convert them into digital format and publish and sell them on their Web site as downloadable streaming media clips. In October of 2004, as sales of the videos began to wane, the defendant sent the plaintiffs an email requesting that they remove his videos from their Web site. After the plaintiffs refused to do so, the defendant filed notices of copyright infringement under the DMCA with the plaintiffs' Internet service providers, alleging that material on the plaintiffs' Web site was infringing on the defendant's copyrights in his videos. Both the Internet service providers and the Paypal service, which processed payments for the plaintiffs' Web site,

---

[2454] 2009 U.S. Dist. LEXIS 34966 (S.D.N.Y. Mar. 12, 2009).

[2455] 391 F.3d 1000 (9th Cir. 2004).

[2456] 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

[2457] 410 F. Supp. 2d 1010 (D. Colo. 2005).

[2458] Id. at 1012-13.

[2459] 2006 U.S. Dist. LEXIS 55471 (W.D.N.C. 2006).

suspended the plaintiffs' access to their accounts. In response, the plaintiffs removed the videos from their Web site. The defendant thereafter filed no further DMCA notices.[2460]

The plaintiffs accused the defendant of violating Section 512(f) by filing bad faith complaints of copyright infringement with the plaintiffs' Internet service providers and others, with the intent that such complaints would result in the suspension of the plaintiffs' Internet services and accounts, and asked the court to enjoin the defendant from filing any more such complaints.[2461] The court denied the injunction on the ground that the injury the plaintiffs sought to avoid – the damage to reputation and business interests caused by the defendant's filing of improper DMCA complaints with the plaintiffs' service providers – was not likely to recur since the plaintiffs neither were posting the videos at issue on their Web site, nor had they cited any interest in re-posting the videos before the underlying legal issues were resolved.[2462]

(v) BioSafe-One, Inc. v. Hawks

In BioSafe-One, Inc. v. Hawks,[2463] the defendants inadvertently copied some textual materials from the plaintiffs' web site into the defendants' web site. Upon discovering the copying, the defendants removed the copied materials. After removal of the copied materials, but before the plaintiffs knew that the copied materials had been removed, the plaintiffs sent two DMCA notices to the OSPs hosting the defendants' web site. In both instances, the OSPs shut down the defendants' web site in response. The defendants claimed that the plaintiffs' notices under the DMCA violated Section 512(f) and sought an injunction preventing the plaintiffs from further interfering with their web site.[2464]

The court ruled the defendants had failed to present sufficient evidence that the plaintiffs knowingly materially misrepresented to the OSPs that the defendants' web site was infringing. The plaintiffs had submitted ample evidence and testimony that they believed the defendants' web site violated their copyright when the DMCA notices were submitted. Accordingly, the court denied the defendants' claim under Section 512(f). However, the court granted a preliminary injunction barring the plaintiffs from sending additional DMCA notices in view of the fact that the court had ruled that the defendants' web site, after the copied materials had been removed, was not substantially similar to the plaintiffs' web site.[2465]

[2460] Id. at *2-5.

[2461] Id. at *1.

[2462] Id. at *7-8.

[2463] 2007 U.S. Dist. LEXIS 88032 (S.D.N.Y. Nov. 29, 2007).

[2464] Id. at *1-3.

[2465] Id. at *30-31.

(vi) Lenz v. Universal Music Corp.

In Lenz v. Universal Music Corp.,[2466] Stephanie Lenz videotaped her toddler son dancing in the family's kitchen to the song titled "Let's Go Crazy" owned by the plaintiff, and posted the video on YouTube.com. The plaintiffs sent a DMCA takedown notice to YouTube, which responded by removing the video from the site. Lenz sent YouTube a counter-notification under the DMCA, demanding that her video be re-posted because it did not infringe the plaintiff's copyrights, and the video was then re-posted by YouTube. Lenz then filed an action against the plaintiffs under Section 512(f) seeking redress for the plaintiffs' alleged misuse of the DMCA takedown process, arguing that her posting was a self-evident non-infringing fair use.[2467]

The court rejected Lenz's claim. Citing the Rossi case discussed in subsection (i) above, the court ruled that Lenz must show a knowing misrepresentation on the part of the copyright owner in filing the takedown notice in order to establish liability under Section 512(f). The court noted that the plaintiffs had not conceded that the posting was a fair use, and Lenz had failed to allege facts from which a misrepresentation could be inferred or why her use of the song was a self-evident fair use. Accordingly, Lenz's claim was dismissed with leave to amend.[2468]

Lenz then amended her complaint, alleging that the plaintiffs had issued the DMCA takedown notice only to appease the musician known as "Prince," the author of the song "Let's Go Crazy."[2469] Specifically, Lenz alleged that Universal issued its DMCA notice to YouTube at Prince's behest, based not on the particular characteristics of the video or any good faith belief that it actually infringed, but rather to appease him, as evidenced by an October 2007 statement to ABC News, in which Universal made the following comment:

> Prince believes it is wrong for You-Tube, or any other user-generated site, to appropriate his music without his consent. That position has nothing to do with any particular video that uses his songs. It's simply a matter of principle. And legally, he has the right to have his music removed. We support him and this important principle. That's why, over the last few months, we have asked YouTube to remove thousands of different videos that use Prince music without his permission.[2470]

Universal moved to dismiss the case for failure to state a claim upon which relief could be granted. The issue raised by the motion, which the court found to be an issue of first impression, was whether the requirement of Section 512(c)(3)(A)(v) that a notice issued under Section 512(c) contain a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or

---

[2466] 2008 U.S. Dist. LEXIS 44549 (N.D. Cal. Apr. 8, 2008) (Order Granting Defendants' Motion to Dismiss with Leave to Amend) (not for citation).

[2467] Id. at *1-3.

[2468] Id. at *8-9.

[2469] Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1152 (N.D. Cal. 2008).

[2470] Id. at 1152-53.

the law, requires a copyright owner to consider the fair use doctrine in formulating its good faith belief. Universal contended that Section 512(c)(3)(A)(v) does not require copyright owners to evaluate the question of fair use prior to sending a takedown notice because fair use is merely an *excused* infringement of copyright rather than a use *authorized* by the copyright owner or by law. Universal also contended that even if a copyright owner were required by the DMCA to evaluate fair use with respect to allegedly infringing material, any such duty would arise only *after* a copyright owner received a counter-notice and considered filing suit.[2471]

The court ruled that a copyright owner does have a duty to consider the applicability of the fair use doctrine before issuing a takedown notice:

> An activity or behavior "authorized by law" is one permitted by law or not contrary to law. Though Congress did not expressly mention the fair use doctrine in the DMCA, the Copyright Act provides explicitly that "the fair use of a copyrighted work … is not an infringement of copyright." 17 U.S.C. § 107. Even if Universal is correct that fair use only *excuses* infringement, the fact remains that fair use is a lawful use of a copyright. Accordingly, in order for a copyright owner to proceed under the DMCA with "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," the owner must evaluate whether the material makes fair use of the copyright. 17 U.S.C. § 512(c)(3)(A)(v). An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to *Section 512(f)* of the DMCA.[2472]

The court addressed Universal's concern that, because the question of whether a particular use of copyrighted material is fair is a fact-intensive inquiry, it would be difficult for copyright owners to predict whether a court eventually would rule in their favor. "[W]hile these concerns are understandable, their actual impact likely is overstated. Although there may be cases in which such considerations will arise, there are likely to be few in which a copyright owner's determination that a particular use is not fair use will meet the requisite standard of subjective bad faith required to prevail in an action for misrepresentation under 17 U.S.C. § 512(f)."[2473]

The court then turned to whether the amended complaint contained sufficient allegations of bad faith and deliberate ignorance of fair use to survive the motion to dismiss. The court found that it did. The amended complaint alleged that Universal acted solely to satisfy Prince and his personal agenda and that its actions had nothing to do with any particular YouTube video that used his songs.[2474] The court concluded, "Although the Court has considerable doubt that Lenz will be able to prove that Universal acted with the subjective bad faith required by *Rossi*,

---

[2471] Id. at 1153-54.

[2472] Id. at 1154-55 (footnotes omitted).

[2473] Id. at 1155.

[2474] Id. at 1156.

and following discovery her claims well may be appropriate for summary judgment, Lenz's allegations are sufficient at the pleading stage."[2475]

Finally, the court considered Universal's allegation that the amended complaint failed to allege a compensable loss under the DMCA. The amended complaint alleged that Lenz had incurred injury in the form of the financial and personal expenses associated with responding to the claim of infringement and harm to her free speech rights, and that she had been intimidated into not posting a single video on YouTube since she received Universal's takedown notice. At oral argument, Lenz's counsel stated that while the damages incurred in preparing Lenz's counter-notice could not be elaborated upon for reasons of privilege, Lenz did incur actual damages in reviewing counter-notice procedures, seeking the assistance of an attorney, and responding to the takedown notice. The court ruled that, though damages might be nominal and their exact nature yet to be determined, Lenz had adequately alleged cognizable injury under the DMCA to survive Universal's motion to dismiss.[2476]

In a later opinion (designated not for publication) denying the defendants' motion to certify the court's order for interlocutory appeal, the court elaborated on its ruling a bit as follows: "The Court did not hold that every takedown notice must be preceded by a full fair use investigation. Rather, it recognized, as it has previously, that in a given case fair use may be so obvious that a copyright owner could not reasonably believe that actionable infringement was taking place. In such a case, which is likely to be extremely rare, the policy objectives of the DMCA are served by requiring copyright owners at least to form a subjective good faith belief that the 'particular use is not a fair use' before sending the takedown notice."[2477]

Lenz then moved for partial summary judgment with respect to several affirmative defenses asserted by the defendants.[2478] The defendants' third affirmative defense was that Lenz had suffered no damages cognizable under Section 512(f), which provides that a person who knowingly makes a material misrepresentation in a takedown notice or in a counternotice shall be liable for "any damages," including costs and attorneys' fees, incurred by one injured by the misrepresentation as the result of the service provider relying on the misrepresentation in removing the allegedly infringing materials or in replacing removed material. The parties disagreed about whether the statute recognizes only economic damages. The court ruled that the use of the phrase "any damages" suggested strong congressional intent that recovery be available for damages even if they do not amount to substantial economic damages.[2479] All the plaintiff need show is damages that were "proximately caused by the misrepresentation to the service provider and the service provider's reliance on the misrepresentation."[2480] With respect to

---

[2475] Id.

[2476] Id. at 1156-57.

[2477] Lenz v. Universal Music Corp., 2008 U.S. Dist. LEXIS 91890 at *6-7 (N.D. Cal. Oct. 28, 2008) (citations omitted).

[2478] Lenz v. Universal Music Corp., 2010 U.S. Dist. LEXIS 16899 (N.D. Cal. Feb. 25, 2010).

[2479] Id. at *20-26.

[2480] Id. at *26 (emphasis removed).

attorneys' fees and costs, the court ruled that any fees incurred for work in responding to the takedown notice and prior to the institution of suit under Section 512(f) are recoverable, but recovery of any other costs and fees post institution of suit is governed by the usual standard under Section 505. Because there was no genuine issue of material fact as to whether Lenz incurred at least *some* damages as defined under the statute, the court granted Lenz's motion for summary judgment as to Universal's affirmative defense of no damages.[2481]

(vii) UMG Recordings v. Augusto

In UMG Recordings, Inc. v. Augusto,[2482] UMG brought a claim for copyright infringement based on Augusto's sale on eBay of copies of promotional CDs he had received from UMG in advance of general commercial release. The promotional CDs had been labeled with language stating that they were licensed to the intended recipient for personal use only and that acceptance of the CD constituted an agreement to comply with the terms of the license, which prohibited resale or transfer of possession. UMG sent notices to eBay under the DMCA alleging that sale of the promotional CDs was infringing, in response to which eBay temporarily stopped Augusto's auctions and suspended his eBay account, although eventually his account was restored.[2483] The court rejected UMG's claim for copyright infringement, ruling that the distributions of the CDs should be treated as "sales" for purpose of the first sale doctrine, notwithstanding the "license" agreement because recipients were free to keep the copies forever, UMG received no recurring benefit from recipients' continued possession, and the transfer was properly characterized as a gift, both under common law and under the Postal Reorganization Act.[2484]

Augusto brought a counterclaim against UMG under Section 512(f), alleging that UMG knowingly misrepresented to eBay that Augusto's auction infringed UMG's copyrights. The court rejected this claim because the evidence demonstrated that UMG had a subjective good faith belief that Augusto was infringing its copyrights. UMG was aware that Augusto had entered into a consent judgment in a previous case, in which he had admitted that selling promotional CDs violated the owner's copyright. Augusto also believed that the license language on the CDs enabled it to enforce its copyrights against an unauthorized seller of those CDs. Accordingly, the court granted UMG summary judgment on Augusto's Section 512(f) claim.[2485]

[2481] Id. at *29-30.

[2482] 558 F. Supp. 2d 1055 (C.D. Cal. 2008), aff'd, 628 F.3d 1175 (9th Cir. 2011).

[2483] Id. at 1058.

[2484] Id. at 1060-61. The Ninth Circuit affirmed this ruling with respect to the first sale doctrine. See UMG Recordings, Inc. v. Augusto, 628 F.3d 1175 (9th Cir. 2011).

[2485] 559 F. Supp. 2d at 1065. The Ninth Circuit did not reach the issue under Section 512(f).

(viii) Capitol Records v. MP3tunes, LLC

In Capital Records, Inc. v. MP3tunes, LLC,[2486] a number of record labels brought claims for copyright infringement against MP3tunes.com for offering online storage lockers where users could store illegally downloaded music and against sideload.com, a search engine that allowed users to search for free music downloads. The plaintiffs sent MP3tunes a DMCA take-down notice with a representative list of over 350 songs that were copied, performed, stored, distributed, and made available for download on or by MP3tunes, but also demanded that MP3tunes take action with respect to all of the plaintiffs' copyrighted recordings, even if not included on the representative list. MP3tunes removed the songs identified on the representative list from its websites, but took no action concerning the broader demand to take down other copyrighted recordings.[2487]

MP3tunes brought a counterclaim under Section 512(f) based on the allegation that five or more recordings on the take-down notice were authorized by one of the plaintiff record labels (EMI) for free downloading. The court ruled that MP3tunes was collaterally estopped from bringing the counterclaim based on an earlier ruling in a separate state litigation between the parties. MP3tunes then sought to amend its counterclaim to enumerate additional allegations, including that plaintiff EMI paid third parties to distribute free MP3s over the Internet; at least six of the plaintiffs' record label websites distributed songs for free; and EMI engaged in active marketing of its music directly and through hundreds or thousands of online music partners. The court denied MP3tunes the ability to amend its counterclaim on three grounds. First, the court noted, citing the Diebold case above, that a material misrepresentation for purposes of Section 512(f) is one that affected the infringer or service provider's response to a DMCA letter. Because MP3tunes removed only the songs on the representative list and did not respond to the demand that it remove all links to any of the plaintiffs' copyrighted recordings, the court concluded that the plaintiffs' representation that any link to its copyrighted recording was infringing could not be a "material" misrepresentation. Second, the court noted that MP3tunes had suffered no injury because it took no action other than filing an anticipatory lawsuit. Third, the court held that an allegation of a possibility that some of the songs on the representative list might be non-infringing was too speculative to meet applicable pleading standards, so amendment of the counterclaim would be futile.[2488]

(ix) Brave New Films v. Weiner

In Brave New Films 501(C)(4) v. Weiner,[2489] Brave New Films uploaded to YouTube a video containing footage from The Michael Savage Show in which Savage made disparaging remarks about Muslims. The uploaded video criticized Savage's remarks. The syndicator of Savage's show, Original Talk Radio Network (OTRN), sent a DMCA takedown notice to YouTube, alleging that the video posted by Brave New Films was infringing. Brave New Films

---

[2486] 611 F. Supp. 2d 342 (S.D.N.Y. 2009).

[2487] Id. at 344.

[2488] Id. at 346-47.

[2489] 626 F. Supp. 2d 1013 (N.D. Cal. 2009).

submitted a counter-notice to YouTube and instituted a lawsuit against Savage and OTRN, seeking a declaratory judgment that the video did not infringement copyrights held by OTRN or Savage, and alleging misrepresentation in violation of Section 512(f).[2490]

Savage sought to avoid the Section 512(f) claim against him by arguing that the takedown notice submitted to YouTube by OTRN was defective, in that it did not allege a good faith belief that Brave New Films' use of the video was unauthorized, and that a notice not in compliance with all requirements of Section 512(c)(3)(A) could not form the basis for a Section 512(f) claim. The court rejected Savage's arguments on two grounds. First, OTRN stated in its takedown notice under penalty of perjury that the information in the letter was accurate and that YouTube had posted the video without authorization, which the court held was sufficient to satisfy the "good faith belief" requirement of Section 512(c)(3)(A). Second, the court ruled that the safe harbor provision of Section 512(c)(3)(A) and its attendant requirements are to protect OSPs from liability and cannot be asserted as a defense to Section 512(f) claims.[2491]

(x) Design Furnishings v. Zen Path

In Design Furnishings, Inc. v. Zen Path LLC,[2492] the court ruled that notices to eBay that sales of wicker furniture on the eBay website infringed the Zen Path's copyrights violated Section 512(f). Zen Path's copyright registrations indicated a strong inference that it knew subjectively it did not have a valid copyright infringement claim when it filed its notices of infringement with eBay for two reasons. First, Zen Path's applications for copyright registration claimed its works were sculptures or three dimensional artwork or ornamental designs. However, the pictures of the furniture submitted by Zen Path with the copyright registrations suggested that Zen Path sought protection of the industrial design of the furniture. Second, the applications contained internal contradictions that the court did not elaborate.[2493]

(xi) Amaretto Ranch Breedables v. Ozimals

In Amaretto Ranch Breedables v. Ozimals, Inc.[2494] the court denied a TRO and preliminary injunction barring Linden Research, operator of Second Life, from removing the plaintiff's virtual animal products from its site as a result of takedown notices issued by the defendant. The plaintiff alleged that the notices violated Section 512(f). The court found that the plaintiff had shown insufficient likelihood of success on the merits to support its Section 512(f) claim because the only similarity between the plaintiff's and the defendant's virtual animals was the idea that they each required "food" to "live."[2495]

[2490] Id. at 1014-15.

[2491] Id. at 1017-18.

[2492] 2010 U.S. Dist. LEXIS 112314 (E.D. Cal. Oct. 21, 2010).

[2493] Id. at 8-10.

[2494] 2010 U.S. Dist. LEXIS 141242 (N.D. Cal. Dec. 21, 2010).

[2495] Id. at *2-7.

(xii) Shropshire v. Canning

In Shropshire v. Canning,[2496] the plaintiff, owner of the musical composition "Grandma Got Run Over By A Reindeer," issued a takedown notice to YouTube to remove a video posted by the defendant containing pictures of reindeer with audio of a group called the "Irish Rovers" singing the plaintiff's composition. YouTube removed the video, the defendant then filed a counter-notice, stating that he believed the video constituted fair use of the composition, and YouTube restored the video. The plaintiff asserted a claim that the counter-notice was false under Section 512(f) and the defendant made a motion to dismiss.[2497]

The court granted the motion. The court noted in passing that under Lenz v. Universal Music Corp.,[2498] a complainant filing a takedown notice must evaluate whether the material made fair use of the copyright. But in this instance, the Section 512(f) claim was being brought by the original complainant against the filer of a counter-notice. In any event, the court found the plaintiff had failed to identify a specific misrepresentation in the defendant's counter-notice. Accordingly, the court granted the motion to dismiss with leave to amend the plaintiff's complaint to identify a specific misrepresentation in the counter-notice and explain how that misrepresentation caused the plaintiff injury.[2499]

The plaintiff filed an amended complaint and the defendant again moved to dismiss. This time, the court granted the defendant's motion in part and denied it in part. The court denied the motion in part because the plaintiff had pled sufficient facts to show that the defendant did not have a good faith belief that the video was removed due to mistake or misidentification, as asserted in the counter-notice. The plaintiff had pled that that communications between its representative and the defendant prior to the counter-notice established that the defendant knew the material had not been removed due to a mistake or misidentification. Specifically, the amended complaint alleged that the plaintiff's representative had contacted the defendant several times to inform him that the "Grandma" song video infringed the plaintiff's copyright and that the defendant needed to obtain a license before issuing a counter-notice. The representative had also explained to the defendant the difference between rights to a copyrighted sound recording and a copyrighted composition, thereby clarifying to the defendant how the plaintiff could have a copyright interest in a recording performed by the Irish Rovers. Finally, the defendant had sent an email to the plaintiff stating "[g]o ahead, contact the Video site managers and get my video removed."[2500]

The court, however, granted the defendant's motion to dismiss insofar as it was based on a statement in the counter-notice that "[n]o sound was copied, no visuals were copied." The court found it was clear in context that this statement was referring to the fact that the audio in

---

[2496] 2011 U.S. Dist. LEXIS 4025 (N.D. Cal. Jan. 11, 2011).

[2497] Id. at *1-4.

[2498] 572 F. Supp. 2d 1150, 1154 (N.D. Cal. 2008).

[2499] Shropshire, 2011 U.S. Dist. LEXIS 4025 at *17-18.

[2500] Shropshire v. Canning, 809 F. Supp. 2d 1139, 1141, 1148 (N.D. Cal. 2011).

the defendant's video had been performed by the Irish Rovers and not copied from any video of performance of the Grandma song by the plaintiff. The court also interpreted a related statement in the counter-notice – that "no part of [the] Grandma video is a copy of any original work made by Elmo" – in a similar fashion. Accordingly, the court granted the defendant's motion to dismiss to the extent the Section 512(f) claim was based on these statements.[2501]

(xiii) Rock River Communications v. Universal Music Group

The case of Rock River Communications, Inc. v. Universal Music Group, Inc.[2502] presented an interesting interpretation of the types of takedown demands to which Section 512(f) applies. The plaintiff created in 2006 certain remixed recordings of reggae music originally recorded by Bob Marley and the Wailers between 1969 and 1972. Universal Music Group controlled the rights to a large percentage of Marley's recordings and claimed it had acquired an exclusive interest in the recordings. Universal sent a cease and desist letter to Apple with respect to the sale of the plaintiff's album in Apple's iTunes online store. The plaintiff contended that Universal's letter contained knowing misrepresentations that the album was infringing, and that it was a takedown notice pursuant to Section 512(c)(3) and therefore subject to the prohibitions of Section 512(f).[2503]

The court granted summary judgment to Universal on the Section 512(f) claim on the ground that the cease and desist letter was not a DMCA takedown notice issued pursuant to Section 512(c) because it was not directed against materials posted at the direction of users. Rather, the recordings had been posted on iTunes by Apple, not its users, as Apple chose all recordings that were available through iTunes. Accordingly, because the "notification" at issue was not a notification pursuant to the DMCA, no claim under Section 512(f) could stand.[2504]

Universal also argued that the DMCA was not applicable because Apple received a financial benefit directly attributable to the alleged infringement on the iTunes site and therefore could not qualify for the Section 512(c) safe harbor.[2505] The court rejected this argument, with the following observation: "The Court's conclusion should not be read to imply that an internet service provider's inability to meet all of the safe harbor requirements takes a dispute entirely out of the ambit of the DMCA. Rather, the Court concludes only that where the manner of the alleged infringement is not of any of the types addressed in 17 U.S.C. §512(c), (d), or (e), notice of claimed infringement given is not a section 512(c)(3) notification and therefore not subject to section 512(f)."[2506]

[2501] Id. at 1149.

[2502] 2011 U.S. Dist. LEXIS 46023 (C.D. Cal. Apr. 27, 2011).

[2503] Id. at *2-3, 48-49.

[2504] Id. at *49-50.

[2505] Id. at *51 n.11.

[2506] Id.

(xiv) Smith v. Summit Entertainment

In Smith v. Summit Entertainment LLC,[2507] the court denied the defendant's motion to dismiss the plaintiff's Section 512(f) claim because the plaintiff had adequately pled that the defendant had submitted a DMCA notice to a web site on which the plaintiff had posted a copy of his song falsely alleging that the song infringed the defendant's copyright, when in fact the defendant's complaint was that the song's CD cover violated the defendant's trademark in a series of films called the "Twilight Saga." The plaintiff had stated on the song's CD cover that it was "inspired by the twilight saga." The plaintiff's allegations in his complaint that the defendant had made an unquestionably false assertion in take down notices, and the song was taken down, was sufficient to plead a claim under Section 512(f).[2508]

(xv) Ouellette v. Viacom

In Ouellette v. Viacom Int'l, Inc.,[2509] the plaintiff brought claims under Section 512(f) against Viacom alleging that Viacom improperly issued takedown notices against various videos the plaintiff posted to YouTube containing Viacom programs together with the plaintiff's critiques of those programs. The plaintiff claimed Viacom had failed to evaluate whether the plaintiff's use of its material was fair use before issuing the takedown notices. A magistrate judge recommended that the claims be dismissed with prejudice because the plaintiff (who was pro se) did not plead facts sufficient to show that Viacom had actual knowledge the plaintiff made fair use in posting and critiquing the Viacom videos and that Viacom acted in subjective bad faith in issuing its takedown notices. The magistrate judge also concluded that the plaintiff's allegation that Viacom used scanning software to identify infringing material without human review for fair use was insufficient to support a Section 512(f) claim because no facts were pled that Viacom had actual knowledge of the software's deficiencies.[2510]

Upon objection by the plaintiff to the magistrate judge's recommendations, the district court adopted the findings and recommendations of the magistrate judge in full.[2511] In elaboration of the magistrate's recommendations, the district court noted that the Ninth Circuit had established a high bar for plaintiffs for Section 512(f) claims in the Rossi case,[2512] under which a defendant can be liable only if it knew that the subject material was not infringing when it issued its takedown notices. Without such a standard, copyright owners like Viacom could face limitless lawsuits just by policing its material on the Internet. The district court ruled that, contrary to the plaintiff's argument that interrogatories were the correct means for him to discover Viacom's intent in issuing its takedown notices to YouTube, Section 512(f) required him to allege facts, at the pleading stage, that demonstrate Viacom acted without a good faith

---

[2507] 2011 U.S. Dist. LEXIS 60246 (N.D. Ohio June 6, 2011).

[2508] Id. at *1-3, *7-8.

[2509] 2012 U.S. Dist. LEXIS 33556 (D. Mont. Mar. 13, 2012).

[2510] Id. at *1, 11-13.

[2511] Ouellette v. Viacom Int'l, Inc., 2012 U.S. Dist. LEXIS 68109 (D. Mont. Apr. 25, 2012).

[2512] Rossi v. Motion Picture Ass'n of Am., Inc., 391 F.3d 1000 (9th Cir. 2004).

belief. The court agreed with the magistrate that the plaintiff had not pled any facts meeting the subjective standard or establishing that his videos were fair use of Viacom's copyrighted materials.[2513]

With respect to the plaintiff's allegation that Viacom's use of scanning software violated the good faith requirement, the district court noted that the essence of the plaintiff's objection was that Viacom's history established that it used its software to abuse the takedown process, a form of "Internet bullying." The court ruled that the plaintiff could not satisfy his burden under the DMCA by alleging that Viacom had acted improperly in the past with respect to others. Rather, the Rossi case required him to plead factual allegations that Viacom acted improperly in *his* case by pleading facts that Viacom knew that its scanning software was flagging his non-infringing videos and that Viacom issued takedown notices nonetheless. Because the plaintiff had not done so, he had failed to state a sufficient Section 512(f) claim. The court granted Viacom's motion for judgment on the pleadings.[2514]

(5) Other Provisions

Section 512(g) provides that a Service Provider shall not be liable for the good faith disabling of access to or removal of material or activity claimed to be, or appearing from the facts and circumstances to be, infringing (regardless of whether the material or activity is ultimately determined to be infringing). However, if such removal is taken pursuant to a notice given to the Service Provider pursuant to the provisions of the third safe harbor (which will be referred to herein as the "safe harbor notice"), then Section 512(g)'s limit on liability is conditioned upon compliance with the following. The Service Provider must (i) take reasonable steps to promptly notify the subscriber that it has removed or disabled access to the subscriber's allegedly infringing material; (ii) upon receipt of a counter notification from the subscriber stating under penalty of perjury that it has a good faith belief that the materials were removed or disabled as a result of mistake or misidentification of the material, provide the person who submitted the safe harbor notice with a copy of the counter notification and inform that person that the Service Provider will replace the removed material or cease disabling access to it in ten business days; and (iii) replace the removed material and cease disabling access to it not less than ten, nor more than fourteen, business days following receipt of the counter notification, unless the Service Provider receives notice from the person submitting the safe harbor notice that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the Service Provider's system.

As described in more detail in Section II.G.6(h) above, Section 512(h) sets up a procedure through which a copyright owner may obtain an order through a United States district court directing the Service Provider to release the identity of an alleged direct infringer acting through the Service Provider's system or network.

[2513] Ouellette, 2012 U.S. Dist. LEXIS 68109 at *7-10.

[2514] Id. at *10-11, 13.

Under Section 512(l), failure of a Service Provider to fit into one of the safe harbors does not affect the Service Provider's claim that its conduct is nonetheless noninfringing, or any other defense.

Finally, Section 512(m) clarifies that the safe harbors are not conditioned upon a requirement that the Service Provider monitor its system for infringements, or access, remove or disable access to material where such conduct is prohibited by law (for example, by the Electronic Communications Privacy Act).

(6) Injunctions Against Service Providers

Under Section 512(j), if a Service Provider is subject to injunctive relief other than under the first safe harbor, courts are limited to injunctions that restrain the Service Provider from providing access to infringing material at particular online sites on its service, that restrain it from providing services to a subscriber engaging in infringing activity by terminating the subscriber, or that otherwise are "necessary to prevent or restrain infringement of specified copyrighted material at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose." If the Service Provider is subject to injunctive relief under the first safe harbor, then courts are limited to injunctions that restrain the Service Provider from providing access to a subscriber engaging in infringing activity by terminating the subscriber or by taking reasonable steps specified in the order to block access to a specific, identified, online location outside the United States.

(7) Designation of Agent to Receive Notification of Claimed Infringement

To take advantage of the third safe harbor for innocent storage of infringing information, Section 512(c)(2) requires a Service Provider to designate an agent to receive notifications of claimed infringement by providing contact information for that agent to the Copyright Office and through the Service Provider's publicly accessible website. Section 512(c)(2) requires the Copyright Office to maintain a current directory of designated agents and to make the listing available to the public.

On Nov. 3, 1998, the Copyright Office published interim regulations for the designation of such agents.[2515] Because the DMCA was made effective immediately, the Copyright Office did not have time to conduct rulemaking proceedings. Accordingly, the Office adopted interim regulations, and stated its intent in the next several weeks to publish a notice of proposed rulemaking to seek comments on more comprehensive final regulations governing the designation of agents to receive notification of claimed infringement. Upon the adoption of final rules, Service Providers will have to file new designations that satisfy the requirements of the final regulations.[2516]

[2515] 63 Fed. Reg. 59233 (Nov. 3, 1998).

[2516] Id. at 59234.

Under the Copyright Office's interim rules, the Office does not provide printed forms for filing interim designations of agents. Instead, Service Providers must file a document entitled "Interim Designation of Agent to Receive Notifications of Claimed Infringement," identified as such by a prominent caption or heading. The Interim Designation, which requires a filing fee of $20, must contain the following information: (i) the full legal name and address of the Service Provider; (ii) all names under which the Service Provider is doing business; (iii) the name, full address, telephone number, facsimile number, and electronic mail address of the agent to receive notification of claimed infringement; and (iv) the signature of the appropriate officer or representative of the Service Provider designating the agent, together with the printed name and title of the person signing the designation, and the date of signature.[2517] A suggested format for filing an Interim Designation can be found on the Copyright Office's website at http://lcweb.loc.gov/copyright/onlinesp/agent.pdf. Each Interim Designation may be filed only on behalf of a single Service Provider. Related companies (e.g., parents and subsidiaries) are considered separate Service Providers who would file separate interim designations.[2518]

In the event of a change in the information reported in an Interim Designation, a Service Provider must file an amended Interim Designation containing the current information required for such designations, together with a filing fee of $20. A suggested format for filing an amended Interim Designation can be found on the Copyright Office's website at http://lcweb.loc.gov/copyright/onlinesp/agenta.pdf. Designations and amendments are posted online on the Copyright Office's website at http://www.loc.gov/copyright/onlinesp/list/index.html. If a Service Provider terminates its operations, it must notify the Copyright Office by certified or registered mail.[2519]

(8) Whether the Safe Harbors Apply to Pre-1972 Sound Recordings

Two decisions have concluded that the DMCA safe harbors apply to claims of infringement against service providers with respect to sound recordings fixed prior to February 15, 1972, the date on which sound recordings first became eligible for federal copyright protection. The first was Capitol Records, Inc. v. MP3Tunes, LLC,[2520] for the reasons discussed in Section III.C.6(b)(1)(iii).s above. The second was UMG Recordings, Inc. v. Escape Media Group, Inc.,[2521] largely on the grounds of the persuasiveness of the reasoning of the MP3Tunes decision.[2522]

[2517] Id. at 59234-35.

[2518] Id. at 59234.

[2519] Id. at 59235.

[2520] 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

[2521] 2012 N.Y. Misc. LEXIS 3214 (S.Ct. N.Y. July 10, 2012).

[2522] Id. at *3-12.

7. Limitations of Liability of Online Service Providers under the Communications Decency Act

The Communications Decency Act ("CDA"), 47 U.S.C. § 230, was passed by Congress to create "a federal immunity to any *state law* cause of action that would hold computer service providers liable for information originating with a third party."[2523] Specifically, 47 U.S.C. § 230(c)(1) provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230(e)(3) provides in part that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." One of the main purposes of the CDA immunity was to prevent service providers from being treated as the publisher of defamatory statements posted on or through the service by users.

(a) Stoner v. eBay

Stoner v. eBay Inc.[2524] involved a novel application of the CDA to shield the online auction service provider eBay Inc. from liability under state laws for intellectual property infringements committed through its service. In that case, the plaintiff sought to hold eBay liable for the sale and distribution of illegal copies of sound recordings sold through its auction service, alleging that eBay's participation in the same constituted unfair competition under the California Business and Professions Code § 17200 et seq. The court granted eBay's motion for summary judgment, holding that the CDA's immunity provisions shielded eBay from liability under the asserted state laws.

To establish immunity under the CDA, the court ruled that eBay had to establish the following three elements: "(1) that eBay is an interactive computer services provider; (2) that eBay is not an information content provider with respect to the disputed activity; and (3) that plaintiff seeks to hold eBay liable for information originating with a third-party user of its service."[2525] The parties did not dispute the first element – that eBay was an interactive computer services provider. The court ruled that eBay had established the second element because it was undisputed that the descriptions of the goods and services auctioned over the eBay service were created entirely by the sellers.[2526]

With respect to the third element, the plaintiff argued that the suit did not seek to hold eBay responsible for the publication of information provided by others, but rather for its own participation in selling contraband musical recordings by virtue of its charging fees and advertising for its services, providing insurance for all auctioned items, and providing escrow

---

[2523] Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997) (emphasis added).

[2524] 56 U.S.P.Q.2d 1852 (Cal. Sup. Ct. 2000).

[2525] Id. at 1853.

[2526] Id.

and payment services.[2527] The court ruled that eBay's role did not extend beyond the scope of the federal immunity:

> A principle objective of the immunity provision is to encourage commerce over the Internet by ensuring that interactive computer service providers are not held responsible for how third parties use their services. … To accomplish this objective, the immunity extends beyond the publication of harmful material over the Internet, and encompasses the distribution of such material in transactions effected over the Internet.[2528]

The court noted that, at bottom, the plaintiff's contention was that eBay should be held responsible for failing to monitor the products auctioned over its service when it must have known that illicit recordings were being auctioned. The plaintiff argued that the very description of some recordings (e.g., "bootleg" tapes) identified them as contraband, so that by failing to intervene, eBay must be deemed to have knowingly joined in the unlawful sale.[2529] The court rejected this argument:

> Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products. While such a service may be aware that a fraction of the large volume of data exchanged over its facilities involves unlawful activity, and might be able to detect a certain portion of those, the threat of liability for failing to monitor effectively would, in the judgment of Congress, deter companies such as eBay from making their service available as widely and as freely as possible. … In order for liability to arise and the immunity to be lost, it would be necessary to show actual, rather than constructive, knowledge of illegal sales, and some affirmative action by the computer service, beyond making its facilities available in the normal manner, designed to accomplish the illegal sales. [2530]

Accordingly, the court granted eBay's motion for summary judgment. This case presents an additional weapon of immunity against liability for service providers, at least to the extent that claims are brought against the service provider under state law. Because many states have laws that may be asserted against service providers for infringement committed through their services – such as unfair competition laws and laws that protect sound recordings fixed before 1972 (when Congress added protection of sound recordings to the copyright statute) – the construction of the CDA under Stoner v. eBay, if followed by other courts, could provide a very useful grounds for immunity.

[2527] Id. at 1853-54.

[2528] Id. at 1854.

[2529] Id.

[2530] Id. at 1855.

(b) Perfect 10 v. CCBill

The facts of Perfect 10, Inc. v. CCBill LLC[2531] are set forth in Section III.C.6(b)(1)(i)d. above. In that case, Perfect 10 appealed rulings by the district court that CCBill and CWIE were immune from liability for state law unfair competition and false advertising claims based on the CDA. CCBill and CWIE cross appealed, arguing that the district court erred in holding that the CDA did not provide immunity against Perfect 10's right of publicity claims.[2532]

The Ninth Circuit noted that, although the CDA does not provide service providers with immunity from laws pertaining to intellectual property, it does not contain an express definition of "intellectual property." Because state laws protecting intellectual property are not uniform, and because material on a website may be viewed across many states at a time, the court reasoned that permitting the reach of any particular state's definition of intellectual property to dictate the contours of federal immunity under the CDA would be contrary to Congress' expressed goal of insulating the development of the Internet from the various state-law regimes. Thus, in the absence of a definition from Congress, the court construed the term "intellectual property" in the CDA to mean "federal intellectual property." Accordingly, CCBill and CWIE were eligible for CDA immunity for all of the state claims raised by Perfect 10.[2533]

8. Secondary Liability of Investors

(a) The Hummer Winblad/Bertelsmann Litigation

For a discussion of this litigation, see Section III.C.2(c)(8) above.

(b) UMG Recordings v. Veoh Networks

The plaintiffs, who owned rights to copyrighted sound recordings and musical compositions allegedly used without authorization by users submitting user-generated content to a site operated by Veoh Networks, sought to hold three of Veoh's investors secondarily liable under theories of contributory liability, vicarious liability, and inducement of infringement. In UMG Recordings, Inc. v. Veoh Networks, Inc.,[2534] in a decision designated not for publication, the court dismissed the plaintiff's complaint with leave to amend. With respect to contributory liability, the court held that merely exercising ownership to select a Board of Directors cannot invite derivative liability.[2535] "Nor is there a common law duty for investors (even ones who collectively control the Board) 'to remove copyrighted content' in light of the DMCA."[2536] The court distinguished the Hummer Winblad/Bertelsmann litigation on the ground that the court

---

[2531] 2007 U.S. App. LEXIS 7238 (9th Cir. Mar. 29, 2007).

[2532] Id. at *2.

[2533] Id. at *32-34.

[2534] 2009 U.S. Dist. LEXIS 14955 (C.D. Cal. Feb. 2, 2009), aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

[2535] Id. at *11.

[2536] Id.

there upheld the complaints against the investors in view of the allegation that the investors had specifically ordered that infringing activity take place on the Napster site. With respect to vicarious liability, the court noted there was no direct financial benefit to Veoh's investors in the form of fees from users or advertisers, and mere potential future increase in financial value of the investment was not sufficient. With respect to inducement to infringe, there was no allegation that the investors encouraged Veoh to infringe directly, thereby distinguishing the Grokster case.[2537]

On appeal, the Ninth Circuit affirmed. The plaintiffs argued that even if summary judgment was properly granted to Veoh on the basis of the DMCA safe harbor, the investors could remain potentially liable for their related indirect infringement because the district court did not make a finding regarding Veoh's direct infringement, and the investors did not qualify as services providers who could receive DMCA safe harbor protection. The Ninth Circuit noted that although it might seem illogical to impose greater liability on the investors than on Veoh itself, the court assumed without deciding that the suit against the investors could properly proceed even though Veoh was protected from monetary liability. Reaching the merits of the plaintiffs' secondary liability arguments, however, the court held that the district court properly dismissed the complaint against the investors.[2538]

With respect to contributory liability, the Ninth Circuit agreed with the district court that the plaintiffs had not alleged sufficiently that the investors gave material assistance in helping Veoh or its users accomplish infringement. The plaintiffs acknowledged that funding alone could not satisfy the material assistance requirement, but argued that the investors also directed the spending of the funding on basic operations including hardware, software and employees, which the plaintiffs argued formed the site and facilities for Veoh's direct infringement, analogizing to the Bertelsmann case. The court distinguished the Bertelsmann case, however, on the ground that the investor was Napster's only available source of funding and thus held significant power and control over Napster's operations. In this case, by contrast, there were multiple investors, and none of them could individually control Veoh.[2539]

The plaintiffs attempted to circumvent this distinction by arguing that the three investors together took control of Veoh's operations by obtaining three of Veoh's five board seats. The court noted that, even assuming that such joint control, not typically an element of contributory infringement, could satisfy the material assistance requirement, the complaint nowhere alleged that the investors agreed to work in concert. Although the complaint alleged that he investors sought and obtained board seats as a condition of their investments, the court noted that three investors individually acquiring one seat apiece was not the same as agreeing to operate as a unified entity to obtain and leverage majority control. Unless the three independent investors were on some level working in concert, then none of them actually had sufficient control over the board to direct Veoh in the way the plaintiffs contended. The court found this missing allegation to be critical because finding secondary liability without it would allow plaintiffs to

---

[2537] Id. at *13-18.

[2538] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1045-46 (9th Cir. 2011).

[2539] Id. at 1046.

sue any collection of directors making up 51% of the board on the theory that they constituted a majority, and therefore together controlled the company. In view of the missing allegations, the court affirmed the dismissal of the plaintiffs' contributory infringement claim.[2540]

Based on the same missing allegations, the court also affirmed the district court's dismissal of the plaintiffs' vicarious liability and inducement of infringement claims. The court noted that the plaintiffs' arguments that the investors distributed Veoh's services and had the right and ability to supervise the infringing users were premised on the same unalleged contention that the investors agreed to act in concert, and thus together they held a majority of seats on the board and maintained operational control over the company. Accordingly, the court affirmed the dismissal of the complaint against the investors.[2541]

D. Linking and Framing

The practice of "linking" is another activity that is ubiquitous on the World Wide Web. A "link" is an embedded electronic address that "points" to another Web location. Links may be of at least two different types. The first type, which will be referred to as an "out link," merely provides a vehicle by which a person browsing a Web page can go to another site by clicking on the link. The out link stores the electronic address of the destination site, and clicking on the link sends that address to the browser, which in turn moves the user to the new destination site.

A second type of link, which will be referred to as an "inline link," is a pointer to a document, image, audio clip or the like somewhere on the Web contained in another's Web page which, in effect, pulls in the image, text or audio clip from the other Web page into the current document for display. In other words, a user looking at *A's* Web page will see on that page image, text, or an audio clip that actually was "pulled in" from site owner *B's* Web page.[2542] When material from an inline link is displayed within the "frame" or window border of a page of the linking website, this type of linking is often referred to as "framing."[2543] The linking site is sometimes referred to as a "para-site," with obvious pejorative connotations.

Both out links and inline links raise a number of potential copyright issues. An out link that points to a site containing infringing material may, for example, cause further infringing

---

[2540] Id. at 1047.

[2541] Id.

[2542] I. Trotter Hardy, "Computer RAM 'Copies:" Hit or Myth? Historical Perspectives on Caching As a Microcosm of Current Copyright Concerns," 22 U. Dayton L. Rev. 423, 449 (1997). For example, "[a]n individual at the Massachusetts Institute of Technology for a while kept an inline 7ink to the 'Dilbert' cartoon of the day. The cartoon appears on copyright owner United Media's site, www.unitedmedia.com/comics/dilbert/, but to browser's of the individual's site, the cartoon appeared to be residing 'there.' United Media sent the individual, Dan Wallach, a 'cease and desist' letter, after which Wallach ceased and desisted the in-line linking." Id. at 39 n.82.

[2543] "Frame" technology is a page presentation capability available in both the Netscape Navigator and the Microsoft Internet Explorer browsers that enables the display of multiple, independently scrollable panels on a single screen. Frames may contain many types of elements, including text, hypertext, graphics, scrollable regions, and other frames.

reproductions, public performances, public distributions, public displays, digital performances of sound recordings, and/or importations to occur when the user reaches that site and the infringing material is downloaded, imported and/or performed or displayed to the linking user. Even if material on the destination site is not infringing of its own right, the reproductions, distributions, and displays that occur as a result of the out link may not be authorized, since the out link may have been established (as is generally the case) without the explicit permission of the owner of material on the destination site. Under the WIPO treaties, the result of clicking on the out link may be to generate an unauthorized access and transmission of the destination material. Or the out link itself may be considered to be an unauthorized "making available to the public" of the material on the destination site – the owner of the destination site may wish to retain complete control of how and when information on its site is presented to the public.

It is unclear whether an out link might also be considered the creation of an unauthorized derivative work. Viewed in one way, an out link could be considered nothing more than a reference to another work, much like a citation in a law review article, that should not be considered a derivative work. One could argue that the material on the linked site is neither altered by the link nor "incorporated" into the linking site, but is seen in its original form when the user arrives there as a result of the link.

Viewed a different way, one could treat a site as a virtual collective work comprised of all material available to be viewed by the user in the course of browsing through the site. Links cause an "incorporation" – at least in a virtual sense – of the linked material into this collective work, thereby in some sense creating a derivative work. If the linked site material enhances the value of the linking site, the linked site owner might argue that the linking site is "based upon" the linked site and therefore constitutes a derivative work.[2544]

The fair use or implied license doctrine may apply to many out links, because it is no doubt the case that many site owners will want their material disseminated as widely as possible, and references in to the site through links from other sites will be considered desirable. However, in some instances the linked site owner may argue that out links cause harm, and such harm should defeat a fair use or implied license defense. For example, nonconsensual links may result in burdensome amounts of traffic on the linked site from users the linked site is not targeting. The owner of the linked site could argue that such unwanted traffic prevents the owner from distributing copyrighted material on its site to its desired audience, thereby harming the potential market for its material. Alternatively, if the linking site is undesirable for some reason in the eyes of the linked site, the linked site might allege the linking diminishes the commercial value of its copyrighted material at the linked site. This might be the case, for

[2544] "A 'derivative work' is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted." 17 U.S.C. § 101.

example, if a site distributing pornographic material were to link to a religious site distributing religious material.[2545]

In addition to the issues of direct infringement discussed above, if a linked site contains infringing material, the link may give rise to contributory infringement on the part of the linking site, particularly if the linking site is promoting the copying, transmission, public display or public performance of material at the linked site. As noted in the previous Section, the SPA instituted a complaint against an OSP for contributory infringement based in part on the provision of links to Internet sites where unauthorized copies of the plaintiffs' software could be found. Linking to a site containing infringing material may also give rise to vicarious liability, if the linking site derives financial benefit from the link.

As discussed in Section III.C.6(b) above, the DMCA provides a safe harbor under certain conditions to OSPs who set up out links to infringing material without knowledge of the infringement.

Inline links may provide an even more direct basis for legal liability than out links. An inline link causes a reproduction of the linked material to be "pulled in" to the linking site, and therefore may cause an infringement of the right of reproduction, display, or performance, or may constitute the creation of an unauthorized derivative work, just as if material had been clipped from a printed source and placed in one's own material. An inline link may also cause an infringing access or transmission of copyrighted material under the WIPO treaties.

Although beyond the scope of this paper, both out links and inline links may raise issues of trademark infringement as well as copyright infringement. The trademarks of the linked site are often used as an icon on which the user may click to reach the linked site, and the trademark owner may argue that such use constitutes an infringement. In addition, both out links and inline links may give rise to allegations of false implications of sponsorship or endorsement of the linking site by the company affiliated with the linked site or material, or of confusion as to source of the linked material.

There have been a number of cases challenging linking and framing on copyright grounds:[2546]

[2545] Linking also raises a number of trademark issues. If the link consists of the linked site's company name, trademark or logo, there is a danger of confusing site visitors about the source, affiliation or sponsorship of either the linking or the linked company's goods or services. The language surrounding a link may also imply an endorsement by the linked company. For example, a list of links to "our many satisfied customers" states an endorsement by those customers of the linking site owner's activities. From the opposite end, a linking site should carefully consider any explicit or implied endorsement it makes of the linked site's goods or services over which it has no control. Linking to a site that contains defamatory material might make the linking entity itself liable as a "re-publisher" of the defamatory material by pointing users to the material. See Kopitzke, "Think Links: Web-Page Owners Should Consider Legal Consequences of Hypertext Links to Others' Sites," *San Francisco Daily Journal* (Dec. 20, 1996), at 5.

[2546] In addition to the United States cases discussed in text, in Jan. 2001, an online European recruitment company, StepStone, obtained an injunction in Germany against OFiR, a Danish media group, preventing OFiR from deep linking (bypassing its home pages) to StepStone's web site. The injunction was based on new European laws

1. The Shetland Times Case

A recent case out of Scotland illustrates one type of harm that a linked site owner perceived to result from links to its site. In The Shetland Times Co., Ltd. v. Wills, [2547] the plaintiff, The Shetland Times ("Times"), maintained a website containing copies of articles that appeared in the printed version of its newspaper. Users visiting the site were initially presented with a "front page" containing headlines. Clicking on a headline linked the user to the full text of the article. The Times planned to sell advertising space on the front page.

The defendant, The Shetland New ("News"), also maintained a website. News took verbatim the headlines from Times' site and placed them on News' Web page to allow users at News' site to link directly to the full text of Times' articles, without having to first view Times' front page. This bypassing of Times' front page obviously caused harm to Times' ability to sell advertising on the front page, since those readers of Times' articles who arrived at the articles through links from News' site would never see the ads. Times sued News in the Scotland Court of Sessions, alleging that News' copying of Times' headlines constituted copyright infringement.

The court issued an "interim edict" (a temporary order) pending a full hearing, ruling that the headlines could be considered copyrightable literary works. The court rejected the defendant's argument that the headlines were not the product of sufficient skill or effort, finding that because many of the headlines consisted of eight or so words that imparted information, copying of the headlines might at least in some instances constitute copyright infringement.

The parties subsequently settled their dispute by agreeing that News would be permitted to link to stories on Times' website by means of headlines only in the following manner: each link to any individual story would be acknowledged by the legend "A Shetland Times Story" appearing underneath each headline and of the same or similar size as the headline; adjacent to any such headline or headlines there would appear a button showing legibly the Times masthead logo; and the legend and the button would each be hypertext links to the Times online headline page.

Under United States law, in most instances headlines will probably not be individually copyrightable under the "words and short phrases" doctrine,[2548] which holds that individual words and short phrases such as titles are not copyrightable, although a collection of headlines might be copyrightable as a compilation. Thus, News' verbatim copying of a collection of

---

on database and copyright protection. Jean Eaglesham, "Recruiter Bans Rival's Links," available as of Jan. 18, 2001 at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3YQ8AC2IC.

[2547] Scotland Court of Session, Oct. 24, 1996.

[2548] See, e.g., Hutchins v. Zoll Medical Corp., 492 F.3d 1377 (Fed. Cir. 2007) (copyright does not protect individual words and "fragmentary" phrases when removed from their form of presentation and compilation); Dobson v. NBA Properties, Inc., 1999 Copyr. L. Dec. ¶ 27,891 (S.D.N.Y. 1999) (phrase "Chicago Bulls Repeat Threepeat" was not protectable under the "words and short phrases doctrine" embodied in 37 C.F.R. § 202.1(a)); Acuff-Rose Music, Inc. v. Jostens, Inc., 988 F. Supp 289 (S.D.N.Y. 1997) (phrase "You've got to stand for something or you'll fall for anything" was an unprotectable cliché); Apple Computer, Inc. v. Microsoft Corp., 799 F. Supp. 1006 (N.D. Cal. 1992).

Times' headlines from a single Times newspaper as a basis for News' links to the Times website might also constitute an infringement under United States copyright law. If Times' suit had been brought in the United States, News would no doubt argue that its use of the headlines was a fair use as part of news reporting.[2549] Times would no doubt argue in response that the commercial harm to its advertising revenues from its headlines on its own front page should defeat News' fair use argument. Although it is unclear how such a case would be decided under United States fair use law, the case is a good illustration of the copyright issues that may arise out of the act of linking.

2. The Total News Case

In February of 1997, a number of news service providers (The Washington Post, Cable News Network, Times Mirror, Dow Jones and Reuters New Media) commenced a suit against Total News, Inc. ("Total News") and other defendants who were either providing website design and programming services to Total News or were principals of Total News. The case was the first to challenge framing as a copyright infringement.

The Total News website was a "para-site," designed to make over 1200 news sources from all over the world available at a single site. The Total News home page frame consisted of the totalnews.com URL at the top, a column of rectangular icons with the trademarked names of several of the plaintiffs running down the left margin, and advertising sold by the defendants at the bottom. At the right center portion of the screen was a news window. When the user first logged onto the Total News website, this window was occupied by a "compass" style array of hyperlinks to several of the plaintiffs' websites. Clicking on the links would cause material from the plaintiffs' websites to be displayed in the news window, but still within the Total News "frame." Thus, for example, if a user clicked on the "Washington Post" link, the news window within the Total News frame would fill with an electronic version of *The Washington Post* newspaper linked in from *The Washington Post*'s own website. However, the totalnews.com URL would remain in place at the top of the frame and advertising sold by Total News would remain in place at the bottom of the frame.

Because the news window of the Total News frame was smaller than full screen in size,[2550] the effect of the framing by the defendants was to display only a portion of the original screens of material from the linked sites at any given time, and the user was forced to scroll the news window horizontally or vertically to see all of the original material from the linked sites. Thus, advertisements contained on the original pages of the linked sites were reduced in size, and in some cases were totally obscured by the Total News frame. At the same time, the user was continuously exposed to the advertising contained within the Total News frame:

[2549] "Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as … news reporting … is not an infringement of copyright." 17 U.S.C. § 107.

[2550] The framed used by Total News to display its directory buttons took up slightly more than 15% of the page width. Gahtan, "Inappropriate Use of Frames May Constitute Infringement," *Cyberspace Lawyer*, Apr. 1997, at 2, 2.

> Absent the "framing" by Defendants described above, someone wishing to view the content of Plaintiffs' sites would, upon accessing those sites, see only Plaintiffs' material as Plaintiffs intend for it to be seen. Use of Defendants' website thus results in continuous, prolonged exposure to the logo, URL and advertising of totalnews.com. Defendants have promoted totalnews.com to advertisers and the public based entirely on Defendants' ability to republish the content of Plaintiffs' sites within the totalnews frames, including frames containing advertising.[2551]

The plaintiffs alleged that Total News infringed the copyrights in various materials from the plaintiffs' websites by "republishing" such material through the Total News site. The complaint did not state which specific rights of the copyright holders were infringed, referring instead merely to the plaintiff's "exclusive rights under 17 U.S.C. § 106."[2552] The plaintiffs also alleged claims for misappropriation of news, federal trademark dilution, federal and state trademark infringement, unfair competition, and tortious interference with contractual relations with their advertisers.

At least one of the plaintiffs, CNN, attempted to counteract the deleterious effects of the framing by employing special code in its Web page that checked to see if the content was being viewed from within a frame, and, if so, caused the unauthorized composite page to be replaced with the CNN page on the entire screen. This technical solution had several problems, however. It took up to a minute or more to take effect, and a pop-up window inviting users to return to the Total News site was still able to appear superimposed on the CNN website.[2553]

In June of 1997, the parties settled the case pursuant to a stipulated order of settlement and dismissal.[2554] Under the settlement, Total News agreed to stop framing the plaintiffs' websites. However, the settlement permitted Total News to maintain out links from the Total News website to any of the plaintiffs' websites, provided that the links were only via hyperlinks consisting of the names of the linked sites in plain text; Total News made no use, as hyperlinks or otherwise, of any of the plaintiffs' proprietary logos or other distinctive graphics, video or audio material; and the links were not likely to imply affiliation, endorsement or sponsorship by any plaintiff or otherwise cause confusion, dilution of the plaintiff's marks, or other violations of state or federal law.

3. The Seattle Sidewalk Case

In April of 1997, Ticketmaster Corporation brought an action in federal district court against Microsoft Corporation based on links from Microsoft's "Seattle Sidewalk" website to Ticketmaster's website. In February of 1998, Ticketmaster filed a Second Amended Complaint,

---

[2551] Complaint in The Washington Post Co. v. Total News, Inc., 97 Civ. 1190 (S.D.N.Y. Feb. 20, 1997) at ¶ 35.

[2552] Id. ¶ 72.

[2553] Gahtan, supra note 2550, at 4.

[2554] A copy of the Stipulation and Order of Settlement and Dismissal is available at www.callaw.com/opinions/hotdocs/totalnew.html.

which asserted claims for copyright and trademark infringement, as well as for unfair competition based on various common law and state law theories.

Ticketmaster maintained a website (www.ticketmaster.com) through which it sold and marketed tickets to various entertainment events. The "Seattle Sidewalk" site, one of a number of city guides maintained by Microsoft on The Microsoft Network, offered a guide to entertainment and restaurants available in the Seattle area. Microsoft placed links on the Seattle Sidewalk to the Ticketmaster site so that users of the Seattle Sidewalk could purchase tickets to events of interest online through Ticketmaster. Negotiations between Microsoft and Ticketmaster for an agreement allowing Microsoft to profit from linkage to and association with Ticketmaster's website failed, and Microsoft established the links – which in several instances bypassed the home page of the Ticketmaster site – without permission from Ticketmaster.

Ticketmaster sued Microsoft in federal court. With respect to its trademark claims, Ticketmaster asserted that the unauthorized links wrongfully appropriated, misused, and diluted Ticketmaster's name and trademarks. In particular, Ticketmaster noted in its complaint that it had a business relationship with MasterCard by which Ticketmaster had agreed to give MasterCard prominence over any other credit cards in any advertising. Ticketmaster objected to Microsoft's use of Ticketmaster's name in connection with MasterCard without giving MasterCard prominence. Ticketmaster also asserted that its name and trademark had been buried by Microsoft in metatag code at Microsoft's site in order to attract to Microsoft's Sidewalk websites Internet search engines and Internet users who were seeking information about tickets sold by and available through Ticketmaster. Ticketmaster alleged that this use of its name and trademark in metatags improperly feathered Microsoft's own nest at Ticketmaster's expense.

Ticketmaster also asserted claims of copyright infringement, based on the allegations that (i) in creating links to the Ticketmaster site, Microsoft repeatedly viewed and thus copied onto its own computers the copyrighted contents of Ticketmaster's website, and (ii) in the operation of the links, Microsoft was reproducing, publicly distributing and displaying without permission Ticketmaster's copyrighted website material.

In Microsoft's answer to Ticketmaster's complaint, Microsoft alleged that Ticketmaster could not complain about Microsoft's link to Ticketmaster's home page because Ticketmaster knew when it set up its website that owners of other Web pages would create such links. Microsoft noted that when an event required tickets, Microsoft routinely provided information about how to obtain them, including prices, telephone numbers and, where appropriate, hypertext links to relevant Web pages. Microsoft alleged that such information was freely available to the public and was not proprietary to Ticketmaster. Microsoft asserted numerous defenses, including (i) that Ticketmaster, when it chose to set up Web pages, assumed the risk that others would use its name and URLs; (ii) that Ticketmaster was estopped from complaining about Microsoft's link because Ticketmaster encouraged users to seek out its website and refer others

to the site; and (iii) that Microsoft's presentation of information about Ticketmaster on its Seattle Sidewalk site was commercial speech protected by the First Amendment.[2555]

Microsoft and Ticketmaster ultimately reached a settlement in the lawsuit, pursuant to which Microsoft was permitted to link to the Ticketmaster site, but not through links that bypassed Ticketmaster's home page.

4. The Futuredontics Case

In Sept. of 1997, Futuredontics, Inc., owner of a website relating to its dental referral service, filed a complaint against a defendant that was framing material from Futuredontics' website in the defendant's website. [2556] The frame displaying Futuredontics' website material included the defendant's logo, information on the defendant, and links to the defendant's other web pages. Futuredontics claimed that such framing constituted the creation of an infringing derivative work. The defendant moved to dismiss the complaint for failure to state a claim, arguing that its frame should be viewed as merely a "lens" which enabled Internet users to view the information that Futuredontics itself placed on the Internet. The court denied the defendant's motion, ruling that existing authority did not resolve the legal issue, and Futuredontics' complaint therefore sufficiently alleged a copyright infringement claim.[2557] Interestingly, however, the court had previously denied Futuredontics' motion for a preliminary injunction, ruling that Futuredontics had failed to establish a probability of success.[2558]

On July 23, 1998, in an unpublished opinion, the Ninth Circuit affirmed the district court's denial of the preliminary injunction.[2559] The Ninth Circuit found that Futuredontics had presented no evidence whatsoever of tangible, let alone irreparable, harm from the defendant's framed link to its site. In addition, the Ninth Circuit ruled that "Futuredontics' claim, that the AAI framed link 'falsely implies that AAI – not Futuredontics – is responsible for the success of Futuredontics's dental referral service' even if true, is not tied to any tangible loss of business or customer goodwill."[2560]

5. The Bernstein Case

In Sept. of 1998, a California judge dismissed without comment a copyright infringement lawsuit, Bernstein v. J.C. Penney, Inc.,[2561] in which the plaintiff, a professional photographer, sought to hold liable several defendants who maintained links on their websites that eventually

---

[2555] "Microsoft Answers Ticketmaster's Charges of Electronic Piracy," *Andrews Computer & Online Industry Litigation Reporter* (July 1, 1997) at 24421.

[2556] Futuredontics, Inc. v. Applied Anagramatics, Inc., 45 U.S.P.Q.2d 2005 (C.D. Cal. 1998).

[2557] Id. at 2010.

[2558] Id. at 2006.

[2559] Futuredontics, Inc. v. Applied Anagramatics, Inc., 1998 U.S. App. LEXIS 17012 (9th Cir. July 23, 1998).

[2560] Id. at *3.

[2561] 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998).

led to a Swedish university website where two allegedly infringing photographs of actress Elizabeth Taylor owned by the plaintiff were displayed. Specifically, persons visiting J.C. Penney's website could, through a chain of no less than six links, reach the photographs on the Swedish website.[2562] The plaintiff Bernstein insisted that J.C. Penney deliberately designed its website so that visitors would be able to see the two photographs of Elizabeth Taylor. Bernstein alleged that the defendants had previously licensed one of the photographs, suggesting that the defendants were trying to benefit from the photographs without paying for them.[2563] The defendants labeled the suit as based on a bizarre and unprecedented theory that, if accepted, would destroy the Internet as a means of worldwide communication, and the judge apparently agreed.[2564]

6. The Intellectual Reserve Case

In Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,[2565] the plaintiff was the owner of the copyright in a Mormon Church work titled the "Church Handbook of Instructions" (the "Handbook"). After the defendants were ordered to remove copies of the Handbook from their website, the defendants posted a notice on their website stating that the Handbook was online, and posted three links to other website addresses where the Handbook could be found. The plaintiffs sought to hold the defendants liable for inducement of infringement and contributory infringement.

The court ruled that the defendants were not liable for inducement of infringement, because there was no evidence that the defendants had any direct relationship with the other

---

[2562] Id. at 1063; "Judge Dismisses Copyright Claims Based on Linking," *Andrews Computer & Online Industry Reporter* (Oct. 6, 1998) at 3, 3. Defendant Arden, manufacturer of a perfume called "Passion" that was endorsed by Taylor, recited the chain of links that a user would need to follow from Penny's site to reach the allegedly infringing photographs: from Penney's main home page to (1) "Elizabeth Taylor's Passion," a part of the Penney's site, to (2) "Biography," a part of the "Passion" site containing information about Taylor's life, to (3) "work on screen," which took the user to (4) an Internet Movie Database Ltd. (IMDB) site, a completely separate site with no connection to Penney's, to (5) "FTP," a link on the IMDB site that took the user to the Swedish site, from where the user could (6) access the infringing photographs. Id.

[2563] Id.

[2564] The defendants argued that the plaintiff's theory of infringement by multiple linking would have a devastating impact on the Internet and argued that the claim should be dismissed for three reasons: "(1) a company whose product is merely displayed on another entity's website cannot be held liable for any infringement by the author of that website; (2) linking cannot constitute direct infringement because the computer server of the linking website does not copy or otherwise process the content of the linked-to site; and (3) multiple linking cannot constitute contributory infringement because (a) Internet users viewing of the material at issue is not infringing and thus there was no direct infringement in the United States to which Arden could contribute; (b) linking 'is capable of substantial noninfringing uses' and thus cannot support a claim for contributory infringement; and (c) the Court cannot infer from the facts alleged that [defendants] knew the photos had been posted to [one of the websites in the chain] and multiple linking does not constitute substantial participation in any infringement where the linking website does not mention the fact that Internet users could, by following the links, finding infringing material on another website." Bernstein, 50 U.S.P.Q.2d at 1064 (citations omitted). The court dismissed the complaint without leave to amend without articulating any specific reasons therefor. Id.

[2565] 53 U.S.P.Q.2d 1425 (D. Utah 1999).

websites on which the Handbook was available, nor that the defendants had induced the operators of those websites to post the Handbook.[2566]

The court concluded, however, that the defendants could be liable for contributory infringement. Turning first to whether there was any direct infringement to which the defendants could be contributing, the court concluded that when visitors to the sites on which the Handbook was posted displayed the Handbook, an infringing copy of the Handbook was made in the users' RAM.[2567] The court then concluded that the defendants were contributorily liable for such infringement because they had actively encouraged it,[2568] based on the following facts:

> The defendants posted on their website the comment "Church Handbook of Instructions is back online!" and provided three links to websites containing the Handbook.

The defendants posted e-mail suggesting that the lawsuit against the defendants would be affected by people logging into one of the linked websites and downloading the complete Handbook.

In response to an e-mail stating that the sender had unsuccessfully tried to browse a website containing the Handbook, the defendants gave further instruction on how to browse the material.

At least one of the three linked websites encouraged the copying and posting of copies of allegedly infringing material on other websites.[2569]

Accordingly, the court entered a preliminary injunction enjoining the defendants from, among other things, posting on their website the addresses of other websites that the defendants knew, or had reason to know, contained the material alleged to infringe the plaintiff's copyright.[2570]

7. Ticketmaster v. Tickets.com

Ticketmaster Corporation operated the Ticketmaster web site, through which users could purchase tickets to various events such as concerts and ball games. On the Ticketmaster home page there were instructions and a directory to subsequent pages (one per event) containing a short description of the event, date, time, place, and price, and a description of how to order tickets via the Internet, telephone, mail, or in person. The defendant, Tickets.com, operated a somewhat different ticketing service. Although Tickets.com sold some tickets to certain events

---

[2566] Id. at 1427.

[2567] Id. at 1428, citing MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993) and Marobie-Fl., Inc. v. National Ass'n of Fire Equip. Distrib., 983 F. Supp. 1167, 1179 (N.D. Ill. 1997).

[2568] The court noted that "[l]iability for contributory infringement is imposed when 'one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.'" Intellectual Reserve at 1427 (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

[2569] Intellectual Reserve at 1428.

[2570] Id. at 1429.

on its own, it provided information as to where and how tickets that it did not sell could be purchased and a link that would take users to the appropriate ticket seller on line. Where the exclusive ticket broker was Ticketmaster, Tickets.com would deep link directly to the interior web page of Ticketmaster (bypassing the home page) for the particular event in question, where the customer could buy the tickets from Ticketmaster.[2571]

Ticketmaster alleged that Tickets.com committed copyright infringement by copying its interior web pages in order to extract the basic information on those pages, such as event, place, time, date, and price. (The extracted information was then placed in Tickets.com's format on its own interior web pages.) The court denied a motion by Tickets.com to dismiss the copyright infringement claim, ruling that, although the factual data contained on Ticketmasters' internal pages could not be protected by copyright, the allegation of copying of Ticketmasters' internal web pages in order to extract that factual data was sufficient to state a valid claim for copyright infringement.[2572] The court went on to state, however, that hyperlinking by itself did not constitute copyright infringement:

> [H]yperlinking does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved. The customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently.[2573]

Five months later, the court issued another opinion that denied a motion for a preliminary injunction brought by Ticketmaster. With respect to the copyright claim, the court noted that Ticketmasters' internal web pages were copied only temporarily, for 10-15 seconds, in the course of extracting the factual information from those pages, and the factual information was then presented by Tickets.com to its users in a different format from how that information appeared on Ticketmasters' site.[2574] The court ruled that the plaintiff was not entitled to a preliminary injunction on copyright grounds because the temporary copying for purposes of extracting the factual information from Ticketmasters' internal web pages was likely to be a fair use. The court analogized to the Ninth Circuit's decision in Sony Computer Entertainment, Inc.

[2571] Ticketmaster Corp. v. Tickets.com Inc., 54 U.S.P.Q.2d 1344, 1345 (C.D. Cal. 2000).

[2572] Id. at 1345-46. The court granted, however, the defendant's motion to dismiss the plaintiff's breach of contract claim, which was based on the "terms and conditions" for use of the Ticketmasters website. The court apparently found that the terms and conditions were not enforceable because they did not require clicking to "agree" to them and were not immediately visible to users: "[T]he terms and conditions are set forth so that the customer needs to scroll down the home page to find and read them. Many customers instead are likely to proceed to the event page of interest rather than reading the 'small print.' It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site. The motion is granted with leave to amend in case there are facts showing Tickets' knowledge of them plus facts showing implied agreement to them." Id. at 1346.

[2573] Id. at 1346.

[2574] Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. Aug. 10, 2000), at *9-10.

v. Connectix Corp.,[2575] which the district court characterized as holding that copying for reverse engineering to obtain non-protectable information is permitted by the fair use doctrine in certain circumstances.[2576] The district court observed:

> Reverse engineering to get at unprotected functional elements is not the same process as used here but the analogy seems to apply. The copy is not used competitively. It is destroyed after its limited function is done. It is used only to facilitate obtaining non-protectable data – here the basic factual data. It may not be the only way of obtaining that data (i.e., a thousand scriveners with pencil and paper could do the job given time), but it is the most efficient way, not held to be an impediment in Connectix.[2577]

The court also rejected the plaintiff's argument that the defendant's copying of the URLs of the interior pages of the Ticketmasters site constituted infringement. "The court doubts that the material is protectable because the URL appears to contain functional and factual elements only and not original material."[2578] Accordingly, the court ruled that, because Ticketmaster appeared unlikely to prevail on its copyright infringement claim, a preliminary injunction should not issue.[2579]

After nearly two additional years of litigation, Tickets.com brought a motion for summary judgment on Ticketmaster's copyright claims, which the court granted.[2580] In granting summary judgment, the court ruled that the spider's temporary copying of Ticketmaster's web pages into RAM in order to extract the factual information about events contained on those pages constituted a fair use. "In temporarily downloading [Ticketmaster's] event pages to its RAM

[2575] 203 F.3d 596 (9th Cir. 2000).

[2576] Tickets.com, 2000 U.S. Dist. LEXIS 12987 at *12.

[2577] Id. at *12-13.

[2578] Id. at *13.

[2579] Id.

[2580] Ticketmaster Corp. v. Tickets.com, Inc., 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 7, 2003). Tickets.com also sought summary judgment on Ticketmaster's contract claim, based on a notice placed on the home page of the Ticketmaster site stating that anyone going beyond that point into the interior pages of the web site accepted certain conditions, including that all information obtained from the site was for the personal use of the user and could not be used for commercial purposes. The contract claim had been rejected as a basis for a preliminary injunction in the court's first opinion in 2000, because the notice was placed at the bottom of the home page so that a user without an especially large screen would have to scroll down to read the conditions of use. Subsequently, Ticketmaster moved the notice to a prominent place on the home page with a warning that proceeding further bound the user to the conditions of use. Id. at *6-7. In addition, the court noted that Ticketmaster had submitted evidence that Tickets.com was in fact fully familiar with the conditions Ticketmaster claimed to impose on users, including a letter from Ticketmaster to Tickets.com which quoted the conditions, and a reply by Tickets.com stating that it did not accept the conditions. The court denied Tickets.com's motion for summary judgment on the contract theory, noting that there was sufficient evidence to defeat summary judgment on the contract theory if knowledge of the asserted conditions of use was had by Tickets.com. Id. at *7-8. The court concluded that "a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so." Id. at *9.

through the use of spiders, [Tickets.com] was not exploiting [Ticketmaster's] creative labors in any way: its spiders gathered copyrightable and non-copyrightable information alike but then immediately discarded the copyrighted material. It is unlikely that the spiders could have been programmed to take only the factual information from the [Ticketmaster] web pages without initially downloading the entire page."[2581]

The court also reaffirmed its earlier ruling on Ticketmaster's preliminary injunction motion that the URLs copied by Tickets.com to allow the deep linking were not copyrightable. Ticketmaster contended that, although the URLs were functional, they should be entitled to copyright protection because there were several ways to write the URL and, thus, original authorship was present. The court rejected this argument. "A URL is simply an address, open to the public, like the street address of a building, which, if known, can enable the user to reach the building. There is nothing sufficiently original to make the URL a copyrightable item, especially the way it is used."[2582]

Finally, the court ruled that Tickets.com's deep linking did not cause an infringing public display of the Ticketmaster event pages. The court distinguished the Ninth Circuit's holding in Kelly v. Arriba Soft Corp., discussed in Section II.C.2 above, by noting that in Kelly the plaintiff's images were framed by the defendant's window and thus were surrounded by the defendant web page's text and advertising. In the instant case, whether or not framing occurred depended upon the settings on the user's computer, over which Tickets.com had no control, and framing therefore occurred on some occasions but not on others. However, when users were linked to the Ticketmaster web pages, the user of the Tickets.com site was taken directly to the originating Ticketmaster site, containing all the elements of that particular Ticketmaster event page, and the Ticketmaster event pages were clearly identified as belonging to Ticketmaster. Moreover, the link on the Tickets.com site contained a notice stating "Buy this ticket from another online ticketing company."[2583] Accordingly, the court granted Tickets.com summary judgment on Ticketmaster's copyright claims.[2584]

8. The MP3Board Case

In this case, several RIAA member companies brought claims for contributory and vicarious copyright infringement against MP3Board for operating a web site, located at

---

[2581] Id. at *17-18.

[2582] Id. at *20.

[2583] Id. at *21-23.

[2584] Ticketmaster also brought a trespass to chattels claim against Tickets.com based on Tickets.com's spiders unauthorized entry into the Ticketmaster site. The court granted Tickets.com summary judgment on this claim, ruling that in order to establish a trespass to chattels claim, there must be some evidence of tangible interference with the use or operation of the computer being invaded by the spider. "Since the spider does not cause physical injury to the chattel, there must be some evidence that the use or utility of the computer (or computer network) being 'spiderized' is adversely affected by the use of the spider. No such evidence is presented here. This court respectfully disagrees with other district courts' finding that mere use of a spider to enter a publicly available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels." Id. at *12.

www.mp3board.com, which provided Internet users with resources to enable them to locate MP3 files from publicly available Web sites. No music files were located on the MP3Board web site. Instead, the web site featured an automated search engine that searched for, aggregated and organized links to media files on the Web, and provided a tutorial offering users instruction on how to locate and download such files. The site also featured a message board on which users could post questions or song requests. In response to users' posts, MP3Board personnel personally searched for links to songs and posted the links on the message board, solicited other users to provide the requested works, and obtained and posted passwords to enable users to access certain music files.[2585]

The RIAA sent a number of infringement demand letters relating to MP3Board's activities before filing suit. On Oct. 27, 1999, and again on Apr. 18, 2000, the RIAA sent letters to MP3Board's ISP, identifying artists whose works were being infringed – but no specific song titles – and demanding that the ISP remove or disable access to the MP3Board site or MP3Board's links to infringing works. In response to the second letter, MP3Board's ISP disabled Internet access to the MP3Board web site, but service was restored after MP3Board supplied a counter notification to the ISP asserting that it had removed the infringing material identified in the RIAA's notice. On May 25, 2000, the RIAA wrote directly to MP3Board and demanded that MP3Board remove all infringing links, this time naming 21 artists and 22 song titles which were representative of the titles being infringed. The letter also attached printouts of screen shots of MP3Board's web site on which the RIAA identified 662 links which the RIAA believed to lead to infringing material. MP3Board did not dismantle access to any of the identified links in response. Shortly thereafter, the RIAA filed suit and sought summary judgment on its claims of contributory and vicarious copyright infringement.[2586]

The court denied the RIAA's motion for summary judgment, finding that numerous issues of material fact remained to be resolved. First, although the structure of the MP3Board site and scale of the operation gave rise to a strong inference that users downloaded files containing copyrighted music, the court found that the record companies had not submitted any direct of evidence of infringement to which MP3Board could contribute or be vicariously liable, such as user logs or other technical data showing the downloading of copyrighted and unauthorized files.[2587] The court ruled that, to show the unlawful distribution of a copyrighted work, the plaintiffs needed to show that an unlawful copy was disseminated to the public.[2588] This ruling is in contrast to the Frena, Chuckleberry, Webbworld, and Marobie-FL cases, discussed in Section II.D.1 above, which held that the mere making available of unauthorized works for download by members of the public constituted infringement of the distribution right.

With respect to contributory liability, the court found material issues of fact both concerning the knowledge and the material contribution prongs. With respect to the material

---

[2585] Arista Records, Inc. v. MP3Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002) at *5-6.

[2586] Id. at *7-9.

[2587] Id. at *11-12.

[2588] Id. at *13-14.

contribution prong, the court noted that MP3Board styled itself as a "passive" tool. The court concluded, however, that there was sufficient evidence from which a factfinder could determine that MP3Board materially contributed to the infringement by virtue of its search engine, the site's solicitation of third parties to post links to sites containing audio files, the posting of a link to a third party named Freedrive where users could store audio files online, the posting of a tutorial on how to locate and download audio files via MP3Board using one of the record companies' copyrighted recordings as an example, and the searching by MP3Board personnel for links to requested songs in response to user requests through the MP3Board message boards.[2589]

Concerning knowledge, the court found material issues of fact with respect to whether MP3Board had constructive knowledge of infringement or whether MP3Board's activities were covered by the Sony doctrine and whether the site was capable of commercially significant noninfringing uses. The record companies pointed to a category of links on the site titled "Legal MP3s" as evidence that MP3Board recognized that the other categories contained MP3s which were not legal. In response, MP3Board noted that a third party MP3 supplier had specifically requested the title "Legal MP3s" to describe the category, which contained exclusively content from that third party. MP3Board also contended that there was no evidence it monitored the posting of links, and stated that it did not investigate the links.[2590]

The court found stronger evidence of actual knowledge of infringement. The court noted that the RIAA letters of Oct. 27, 1999 and Apr. 18, 2000 to MP3Board's ISP, which were forwarded on to MP3Board, were insufficient to constitute notice under DMCA Section 512(d)(3). "By solely listing artists' names, and neglecting to specify any infringing links or even particular songs, the letter(s) did not include 'identification of the reference or link, to material or activity claimed to be infringing."[2591] Accordingly, MP3Board's failure to delete any links in response to those letters could not give rise to any liability.[2592] However, the letter of May 25, 2000 complied with DMCA notification requirements because it not only named particular artists along with specified songs, but was accompanied by printouts of screen shots of MP3Board's web site, on which the RIASA highlighted and placed an asterisk next to 662 links which the RIAA believed to infringe upon the record companies' copyrights (although no URL addresses were provided by the RIAA).[2593] Despite the adequacy of notice via the May 25, 2000 letter, the court nevertheless held that issues of material fact existed regarding MP3Board's knowledge of infringing activity.[2594]

With respect to vicarious liability, the court similarly found that issues of material fact concerning MP3Board's right and ability to control infringing activity, and whether it had a direct financial interest in the activity, precluded summary judgment. It also found material

---

[2589] Id. at *17-18.

[2590] Id. at 21-23.

[2591] Id. at *26 (quoting Section 512(d)(3)).

[2592] Id. at *27.

[2593] Id. at *28-29.

[2594] Id. at *30.

issues of fact concerning whether MP3Board qualified as a "service provider" for purposes of the Section 512(d) safe harbor, thereby at least implicitly recognizing that the Section 512(d) safe harbor could apply to vicarious liability. With respect to the issue of control, the court curiously found issues of material fact, even though it stated, citing the Ninth Circuit's Napster I decision, that a defendant's ability to block infringers' access to a particular environment for any reason constitutes proof of its right and ability to supervise and control the infringing activities. The court further noted as evidence of control that MP3Board could delete links from its database and thus prevent them from being displayed in response to user queries, and that it had in fact removed offending links from the site and banned repeat offenders of its rules from posting any additional links.[2595]

With respect to the issue of financial benefit, the court again curiously found issues of material fact, despite the fact that it cited only evidence from which direct financial benefit could be inferred. Specifically, the court, against citing Napster I, noted that infringement which increases a defendant's user base or otherwise acts as a draw for customers constitutes a direct financial interest. It also cited testimony from MP3Board's principals that the revenue MP3Board received from banner advertisements on the site was directly tied to the number of users who were exposed to those ads.[2596] In view of the material issues of fact cited by the court, it denied the plaintiffs' motion for summary judgment.[2597]

9. Kelly v. Arriba Soft

One of the most important linking cases is that of Kelly v. Arriba Soft Corp.[2598] That case and its significance are discussed in detail in Section II.C.2 above.

10. Batesville Services, Inc. v. Funeral Depot, Inc.

In Batesville Services, Inc. v. Funeral Depot, Inc.,[2599] the plaintiff Batesville sold caskets and was the owner of the copyrights in a number of advertising photographs used to market its caskets. The defendant, although not an authorized dealer of Batesville, operated a web site that sold caskets, including Batesville caskets. The defendant displayed some of Batesville's casket photographs on its web site. In response to a cease and desist letter, the defendant removed the photographs from its web site, but approached the Veterans Society, an authorized Batesville dealer, and reached an agreement that the defendant would pay the expenses of modifying the Veterans Society web site so that digitized versions of images of Batesville caskets would be

---

[2595] Id. at *33-34.

[2596] Id. at *35-36.

[2597] The court denied a counter-motion for summary judgment filed by MP3Board that its activities of identifying links where information could be found were protected by the First Amendment. The court cited authority from the Second Circuit that the fair use doctrine encompasses all claims under the First Amendment in the copyright field, and noted that MP3Board had not asserted that its activities constituted fair use, nor could it succeed on such an assertion under the applicable factors of the fair use doctrine. Id. at *37-40.

[2598] No. 00-55521 (9th Cir. Feb. 6, 2002).

[2599] 2004 Copyr. L. Dec. ¶ 28,901 (S.D. Ind. 2004).

displayed on the site. The defendant then modified its own web site so that small, low resolution thumbnail images of Batesville caskets were linked to the appropriate casket pages on the Veterans Society website. When a shopper on the defendant's site clicked on a thumbnail image, the shopper was linked to a much larger image on a casket page on the Veterans Society web site, which in turn displayed the defendant's phone number. The casket web pages on the Veterans Society site also had a link labeled "Back to Main Gallery" that would return the viewer to the defendant's web site.[2600]

The plaintiff contended that both the previous and the modified arrangements violated their copyrights in the photographs in question. The defendant argued, among other things, that the Veterans Society, as an authorized Batesville dealer, had an implied license to display the photographs, and that in any event the use of links on the Internet could never amount to copyright infringement. Both sides moved for summary judgment.[2601]

With respect to the implied license argument, the court noted that Batesville had supplied the photographs to the Veterans Society as an authorized dealer, and that like any other Batesville dealer, the Veterans Society was authorized to use those photographs for at least some purposes. Batesville argued, however, that the Veterans Society had exceeded the scope of its implied license by posting the photographs on its web site to promote a business other than its own. The court rejected this argument, noting that there was no evidence that Batesville had even asked the Veterans Society to change its arrangements or had ever communicated to the Veterans Society its internal policy that its photographs were to be used to promote only the authorized dealer's business to whom the photographs were supplied. Batesville could have revoked at any time the implied license to the Veterans Society or insisted that it revise its web site in a way that satisfied Batesville, but had not done so. Accordingly, the factual record could lead a reasonable jury to find that the Veterans Society's implied licensed allowed the disputed use of the images in question, and the court ruled that neither Batesville nor the defendant was entitled to summary judgment on the implied license defense.[2602]

Turning to the defendant's linking defense, the court rejected the defendant's argument, based on the Ticketmaster Corp. v. Tickets case and the Bernstein case, discussed respectively in Sections III.D.7 and III.D.5 above, that links can never amount to a copyright violation. The court noted that those two cases suggest that the host of a web site who establishes a link to another site that may be interesting to the host's web site visitors does not undertake any general duty to police whether the linked sites contain any material infringing the copyrights of others. Those two cases, however, did not support a sweeping per se rule that links can never give rise to infringement.[2603]

[2600] Id. at pp. 37,694-95.

[2601] Id. at 37,695.

[2602] Id. at 37,697-98. The court also rejected the defendant's argument that its use of the Batesville photographs was a fair use. Id. at 37,698-701.

[2603] Id. at 37,701.

The court cited the Intellectual Reserve case, discussed in Section III.D.6 above, for the proposition that, in extreme cases, even encouraging browsing of infringing web sites can violate the copyright laws.[2604] "From that conclusion, it is easy to allow room for liability for defendants who deliberately encourage use of infringing web sites by establishing links to those sites. This is not a case where Funeral Depot merely found some useful material elsewhere on the internet and encouraged its shoppers to link to those sites. Instead, Funeral Depot actively secured control of the contents of the Veterans Society website and modified the website to use it for its own purposes."[2605]

The court noted that the "casket gallery" on the Veterans Society web site did not exist until the defendant created those web pages, that it had designed and paid for them, it still controlled changes to them, and they displayed the defendant's phone number. The defendant's control of the web pages was so complete that the owner of the Veterans Society was not aware of any changes to the casket portion of its web site.[2606] "These facts are unusual enough to take this case out of the general principle that linking does not amount to copying. These facts indicate a sufficient involvement by Funeral Depot that could allow a reasonable jury to hold Funeral Depot liable for copyright infringement or contributory infringement, if infringement it is. The possibility of copyright infringement liability on these unusual facts showing such extensive involvement in the allegedly infringing display should not pose any broad threat to the use of hyperlinks on the internet."[2607]

11. Live Nation Sports v. Davis

The facts of Live Nation Motor Sports, Inc. v. Davis,[2608] are discussed in Section II.B.3 above. The court granted a preliminary injunction enjoining the defendant from providing Internet links to the plaintiff's webcasts of its motorcycle racing events or otherwise displaying or performing the plaintiff's webcasts.[2609] With almost no analysis, the court ruled that the plaintiff had a likelihood of success on its copyright claim because "the unauthorized 'link' to the live webcasts that [the defendant] provides on his website would likely qualify as a copied display or performance of [the plaintiff's] copyrightable material."[2610] The court found a threat of irreparable harm to the plaintiff because the defendant's links would cause the plaintiff to lose its ability to sell sponsorships or advertisements on the basis that its website was the exclusive source of the webcasts.[2611] Although the unclear facts of this case make its reach uncertain, it could potentially imply that any unauthorized link that causes material available on another site

---

[2604] Id. at 37,701-02.

[2605] Id. at 37,702.

[2606] Id.

[2607] Id.

[2608] 2006 U.S. Dist. LEXIS 89552 (N.D. Tex. Dec. 11, 2006).

[2609] Id. at *18.

[2610] Id. at *12.

[2611] Id. at *15.

to be streamed through an unauthorized site could constitute an infringing public display or performance.

12. Perfect 10 v. Google (aka Perfect 10 v. Amazon)

The case of Perfect 10 v. Google involved some important rulings in the context of framing of content taken from third party sites. That case is discussed extensively in Section II.C.4 above.

E. Streaming and Downloading

"Streaming" is the digital transmission of a work, usually a musical work, over a network that results in an immediate playing of the work at the recipient's end, without storage of a permanent copy at the recipient's end. If a permanent copy of a work is stored at the recipient's end as a result of a transmission, the act of transmission is usually referred to as "downloading" and the resultant copy is referred to as a "download." A "limited download" refers to a download that can be played only for a limited period of time or a limited number of plays.

Streaming potentially implicates at least two rights of the copyright holder in both the sound recording being transmitted and the musical work embodied in the sound recording – the right of public performance and the right of reproduction. The right of public performance is potentially implicated because Section 101 of the copyright statute defines the public performance of a work to include the following: "to transmit or otherwise communicate a performance ... of the work … to the public, by means of any device or process, whether the members of the public capable of receiving the performance … receive it in the same place or in separate places and at the same time or at different times."[2612] The right of reproduction is potentially implicated because interim whole or partial copies of the work are made in various RAM memories in the course of transmission of the work through the Internet.[2613] In addition, copies of the works available for streaming generally must be stored on one or more servers operated by the streaming vendor.

Significant legal disputes have arisen over the application of the rights of public performance and reproduction, as well as the compulsory statutory licenses afforded by the copyright statute, to streaming and limited downloads. The nature of these disputes, and the cases decided to date with respect to them, are discussed below.

1. The Digital Performance Right – The Section 114(d)(1) Exemption and Streaming by FCC-Licensed Broadcasters

Section 106(4) of the copyright statute grants the owner of copyright in a work the exclusive right to perform the work publicly. The right does not apply, however, to sound recordings,[2614] except with respect to certain public performances by digital transmission. In

[2612] 17 U.S.C. § 101.

[2613] See the analysis in Sections I.A.1 & I.A.2 above.

[2614] 17 U.S.C. § 114(a).

particular, the Digital Performance Right in Sound Recordings Act of 1995 (DPRA)[2615] created as of February 1, 1996 a limited right to perform a sound recording by means of a "digital audio transmission."[2616]

Certain digital transmissions of performances are exempt from this right under Section 114(d)(1). Specifically, the performance of a sound recording publicly by means of a digital audio transmission (i) as part of a "nonsubscription broadcast transmission,"[2617] (ii) as part of a retransmission of a nonsubscription broadcast transmission (subject to certain limitations in the case of a retransmission of a radio station's broadcast transmission),[2618] or (iii) as part of certain other narrowly defined incidental transmissions or transmissions within or to a business establishment for use in the ordinary course,[2619] is exempt from the digital performance right, provided in each case that it is not "part of an interactive service." The copyright statute defines an "interactive service" as a service "that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient."[2620] Nonexempt digital audio transmissions that are not part of an "interactive service" are subject to a statutory license as provided in Section 114(d)(2) of the copyright statute, as discussed further in subsection 2 below. Those wishing to engage in digital audio transmissions as part of an interactive service must negotiate individual licenses with the relevant copyright holders.

In the late 1990's, a controversy arose over whether FCC-licensed broadcasters, which are exempt from paying royalties to sound recording copyright holders for traditional radio broadcasting of those recordings, should remain exempt when streaming the same broadcast over the Internet. The broadcasters argued such streaming should be classified as an exempt "nonsubscription broadcast transmission" under Section 114(d)(1)(A) of the copyright statute. On Dec. 11, 2000, the Copyright Office issued a final rule determining that AM/FM broadcast signals transmitted simultaneously over a digital communications network such as the Internet

---

[2615] Pub. L. No. 104-39, 109 Stat. 336 (codified at 17 U.S.C. §§ 106, 114, 115).

[2616] See 17 U.S.C. § 106(6). Section 114(j)(5) of the copyright statute defines a "digital audio transmission" to mean "a digital transmission as defined in section 101, that embodies the transmission of a sound recording. This term does not include the transmission of any audiovisual work." Section 101 defines "digital transmission" as "a transmission in whole or in part in a digital or other non-analog format."

[2617] 17 U.S.C. § 114(d)(1)(A). A "broadcast" transmission is "a transmission made by a terrestrial broadcast station licensed as such by the Federal Communications Commission." Id. § 114(j)(3). A "nonsubscription" transmission is "any transmission that is not a subscription transmission." Id. § 114(j)(9). A "subscription" transmission is "a transmission that is controlled and limited to particular recipients, and for which consideration is required to be paid or otherwise given by or on behalf of the recipient to receive the transmission or a package of transmissions including the transmission." Id. § 114(j)(14).

[2618] Id. § 114(d)(1)(B).

[2619] Id. § 114 (d)(1)(C).

[2620] Id. § 114(j)(7).

were not exempt under Section 114(d)(1)(A), and thus were subject to the digital performance right of the DPRA.[2621]

In its ruling, the Copyright Office determined that the exemption for "broadcast transmission[s]" was limited to over-the-air transmissions by FCC-licensed broadcasters and thus did not cover streaming.[2622] The Copyright Office also amended its regulatory definition of a "Service" for purposes of the Section 114 statutory license to clarify that transmissions of a broadcast signal over a digital communications network such as the Internet are not exempt from copyright liability under Section 114(d)(1)(A) of the Copyright Act. The broadcasters challenged the Copyright Office's ruling in federal court.

In Bonneville Int'l Corp. v. Peters,[2623] the Third Circuit affirmed a district court's ruling upholding the Copyright Office's ruling. The Third Circuit noted that, for AM/FM webcasting to be exempt under Section 114(d)(1)(A) from the digital audio transmission performance copyright, it must be 1) noninteractive, 2) nonsubscription and 3) broadcast. Because the parties agreed that AM/FM webcasting was not part of an interactive service and was a nonsubscription transmission, the issue was whether AM/FM webcasting is a "broadcast transmission."[2624]

The court concluded form the statutory language and the legislative history that AM/FM webcasting is not a broadcast transmission. With respect to the statutory language, Section 114(j)(3) defines a broadcast transmission as "a transmission made by a terrestrial broadcast station licensed as such by the Federal Communications Commission." The court gave "terrestrial" its "natural and logical meaning of earthbound."[2625] The parties disputed, however, whether a "broadcast station" should be read to refer to the broadcaster as a business entity that operates broadcasting facilities, or to the broadcasting facilities themselves (and by extension the mode of transmission). The court adopted the latter interpretation, noting that the former interpretation would lead to anomalous consequences. One such consequence would be that any entity that operated at least one FCC-licensed radio station would have carte blanche to digitally perform recordings via any conceivable transmission medium (in a noninteractive, nonsubscription manner) without limitation or copyright liability.[2626]

Another anomalous consequence would be that the meaning of the modifier "terrestrial" would become absurd. Specifically, under the interpretation in question, a terrestrial broadcast station would mean a business entity that is earthbound, in contrast, presumably, to one that is space-borne. The court noted that such an interpretation made no sense given that no space-borne business entities exist. On the other hand, an interpretation limited to earthbound

---

[2621] 65 Fed. Reg. 77292 (Dec. 11, 2000).

[2622] Id. at 77301.

[2623] 68 U.S.P.Q.2d 1545 (3d Cir. 2003).

[2624] Id. at 1549.

[2625] Id. at 1550.

[2626] Id.

broadcasting *facilities*, as opposed to broadcasting done through satellites, would be entirely plausible.[2627] Accordingly, the court concluded that a

> "broadcast station licensed as such by the [FCC]," as the term is used in Section 114(j)(3), refers to the physical radio station facility that broadcasts radio signals over the air, and not to the business entity that operations the radio station. A "broadcast transmission" under § 114(d)(1)(A) would therefore be a radio transmission by a radio station facility operated subject to an FCC license and would not include a webcast. AM/FM webcasting does not meet the definition of a "nonsubscription broadcast transmission" and does not, therefore, qualify under § 114(d)(1)(A) for an exemption from the digital audio transmission performance copyright of § 106(6).[2628]

The court noted that the legislative history was consistent with its interpretation. In the 1995 Senate Report, accompanying the legislation that first established a digital performance right for sound recordings, Congress stated that the "classic example of [an exempt transmission under section 114(d)(1)(A)] is a transmission to the general public by a free *over-the-air* broadcast station, such as a traditional radio or television station, and the Committee intends that such transmissions be exempt regardless of whether they are in a digital or nondigital format, in whole or in part."[2629] Thus, the court found it clear that the original 1995 exemption for broadcast transmissions was limited to over-the-air transmissions, and Congress did not contemplate protecting AM/FM webcasting, which did not exist at the time. Because the DMCA amendments in 1998 to the broadcast transmission exemptions were silent on AM/FM webcasting, the court found no affirmative grounds to believe that Congress intended to expand the protections contemplated by the original 1995 legislation.[2630]

Accordingly, the Third Circuit concluded that Section 114(d)(1)(A)'s nonsubscription broadcast transmission exemption implicates only over-the-air radio broadcast transmissions, and does not cover the Internet streaming of AM/FM broadcast signals.[2631]

As discussed in detail in Section III.E.2(a) below, in May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA agreed on a proposal for royalty rates to be paid for Internet streaming of AM/FM broadcasts for the period from 1998 through Dec. 31, 2004, and submitted the proposal to the Copyright Office for possible adoption without a CARP. On May 20, 2003, the Copyright Office published the proposal for comment.[2632]

[2627] Id.

[2628] Id. at 1552.

[2629] S. Rep. No. 104-128, at 19 (1995).

[2630] Id. at 1555.

[2631] Id.

[2632] 68 Fed. Reg. 27506 (May 20, 2003).

With respect to the related issue of royalties to owners of the copyrights in underlying musical works that are streamed online, in Nov. 2001, a federal district court in New York approved an interim agreement reached between radio stations and music-licensing agency Broadcast Music Inc. (BMI). Under that agreement, radio stations agreed to pay 1.065% of revenues generated by online music streaming, the same rate that radio stations pay for rights to broadcast the musical compositions over the airwaves.[2633]

Similarly, in Oct. 2004, a federal district court in New York approved a license agreement negotiated between the American Society of Composers, Authors and Publishers (ASCAP) and the Radio Music License Committee (RMLC), representing most of the nearly 12,000 U.S. commercial radio stations, for rights to perform ASCAP music over the air and via simultaneous streaming. The agreement governed the period Jan. 1, 2001 through Dec. 31, 2009.[2634]

2. The Digital Performance Right – Statutory Licenses Under Section 114 for Certain Nonsubscription and Subscription Services

Section 114 of the copyright statute provides statutory licenses for the performance of sound recordings publicly by both nonsubscription and subscription digital services, again provided in each case that such transmissions are "not part of an interactive service."[2635] Under Section 114(d)(2), the statutory licenses cover transmissions by the following means:[2636]

Subscription Digital Audio Transmissions: by means of subscription digital audio transmissions that are not exempt under Section 114(d)(1). A "subscription" transmission is "a transmission that is controlled and limited to particular recipients, and for which consideration is required to be paid or otherwise given by or on behalf of the recipient to receive the transmission or a package of transmissions including the transmission."[2637]

All nonexempt digital subscription transmission services are eligible for the statutory license, provided that they are non-interactive and comply with the terms of the license.

[2633] Kevin Featherly, "Judge OKs Interim Online-Radio Music Royalty Rate" (Nov. 28, 2001), available as of Feb. 2, 2002 at www.newsbytes.com/news/01/172509.html.

[2634] "Music Publishers Sign Deal on Web Radio" (Oct. 18, 2004), available as of Oct. 19, 2004 at www.washingtonpost.com/wp-dyn/articles/A41418-2004Oct.18.html. The court's order approving the license agreement was available as of May 1, 2005 at www.ascap.com/licensing/radio/ORDER.pdf. The license sets forth the total amount of industry-wide fees that will be collected by ASCAP during each of the applicable years of the agreement, and allocates each local radio station's share of the annual license payment in accordance with a license fee allocation formula set forth in Exhibit B to the license. A copy of the license was available as of May 1, 2005 at www.ascap.com/licensing/radio/RMLC_License.pdf (main body of license) and www.ascap.com/licensing/radio/FeeMethodology.pdf (allocation formula).

[2635] 17 U.S.C. § 114(d)(2)(A)(i).

[2636] The statutory license was expanded by the Digital Millennium Copyright Act of 1998 (DMCA), Pub. L. No. 105-304, to expressly cover non-exempt eligible non-subscription transmissions and non-exempt transmissions made by preexisting satellite digital audio radio services. See 17 U.S.C. § 114(f).

[2637] 17 U.S.C. § 114(j)(14).

Although the statutory provisions are quite complex, Section 114 generally requires that the service not violate the "sound recording performance complement,"[2638] not publish in advance a schedule of the programming to be performed, not cause any receiving device to switch from one program channel to another, include in each transmission certain identifying information encoded in each sound recording, pay the royalty fees, and comply with the associated terms and with any recordkeeping requirements promulgated by the Copyright Office.[2639]

The statute distinguishes between two types of subscription digital audio transmissions: (1) a "preexisting subscription service," which is a non-interactive subscription service performing audio-only digital audio transmissions that was in existence and was making such transmissions to the public for a fee on or before July 31, 1998;[2640] and (2) a "new subscription service," which is a non-interactive subscription service performing digital audio transmissions and that is not a preexisting subscription service or a "preexisting satellite digital audio radio service" (defined in the third bullet below).[2641]

Eligible Nonsubscription Transmissions (Webcasting): by means of an "eligible nonsubscription transmission," which is defined as "a noninteractive nonsubscription digital audio transmission not exempt under subsection (d)(1) that is made as part of a service that provides audio programming consisting, in whole or in part, of performances of sound recordings, including retransmissions of broadcast transmissions, if the primary purpose of the service is to provide to the public such audio or other entertainment programming, and the primary purpose of the service is not to sell, advertise, or promote particular products or services other than sound recordings, live concerts, or other music-related events."[2642] The conditions for the statutory license for eligible nonsubscription transmissions are very similar to those of nonexempt digital subscription transmissions noted above.

[2638] Section 114(j)(13) provides: "The 'sound recording performance complement' is the transmission during any 3-hour period, on a particular channel used by a transmitting entity, of no more than-

(A) 3 different selections of sound recordings from any one phonorecord lawfully distributed for public performance or sale in the United States, if no more than 2 such selections are transmitted consecutively; or

(B) 4 different selections of sound recordings-

(i) by the same featured recording artist; or

(ii) from any set or compilation of phonorecords lawfully distributed together as a unit for public performance or sale in the United States,

if no more than three such selections are transmitted consecutively:

Provided, That the transmission of selections in excess of the numerical limits provided for in clauses (A) and (B) from multiple phonorecords shall nonetheless qualify as a sound recording performance complement if the programming of the multiple phonorecords was not willfully intended to avoid the numerical limitations prescribed in such clauses."

[2639] 17 U.S.C. §§ 114(d)(2)(A)-(C) & 114(f)(2)-(4).

[2640] Id. § 114(j)(11).

[2641] Id. § 114(j)(8).

[2642] Id. § 114(j)(6).

Preexisting Satellite Digital Audio Radio Services: by means of a "preexisting satellite digital audio radio service" (not exempt under Section 114(d)(1)), which is defined as "a subscription satellite digital audio radio service provided pursuant to a satellite digital audio radio service license issued by the Federal Communications Commission on or before July 31, 1998, and any renewal of such license to the extent of the scope of the original license, and may include a limited number of sample channels representative of the subscription service that are made available on a nonsubscription basis in order to promote the subscription service."[2643] To be eligible for the statutory license, the service must not exceed the sound recording performance complement and must not publish in advance a schedule of the programming to be performed.[2644]

Pursuant to its statutory authority, the Copyright Office conducted a number of Copyright Arbitration Royalty Panel (CARP) proceedings[2645] to establish the royalty rates to be paid for the statutory license. For example, on May 8, 1998, the Librarian of Congress issued an initial determination of rates and terms for the statutory license to be paid by nonexempt subscription digital transmission services, imposing a royalty rate of 6.5% of gross revenues from U.S. residential subscribers.[2646]

The Copyright Office subsequently initiated separate CARP proceedings to set rates and terms for transmissions made by "eligible nonsubscription services" and those transmissions made by "pre-existing satellite digital audio radio services."[2647] The latter proceeding was also to establish rates and terms for transmissions made during the period Jan. 1, 2001, to Dec. 31, 2002, by "preexisting subscription services" (i.e., the three subscription services in existence prior to the passage of the DMCA, as discussed in the next subsection). Neither proceeding considered rates and terms for transmissions made by "new subscription services." The manner in which rates have subsequently been set for the various categories of services are enumerated in the following subsections.

[2643] Id. § 114(j)(10).

[2644] Id. § 114(d)(2)(B).

[2645] The Copyright Royalty Tribunal Reform Act of 1993, Pub. L 103-198, 107 Stat. 2304, eliminated the Copyright Royalty Tribunal (CRT) and replaced it with a system of ad hoc Copyright Arbitration Royalty Panels (CARPs) administered by the Librarian of Congress and the Copyright Office. The CARPs adjust royalty rates and distribute royalties collected under the various compulsory licenses and statutory obligations of the copyright statute.

[2646] 63 Fed. Reg. 25394 (May 8, 1998). The determination was appealed by the RIAA. The D.C. Circuit affirmed the rates, although it remanded the matter of certain payment terms to the Librarian for further proceedings. Recording Industry Ass'n of Am. v. Librarian of Congress, 176 F.3d 528 (D.C. Cir. 1999).

[2647] 66 Fed. Reg. 1700 (Jan. 9, 2001). A "pre-existing satellite digital audio radio service" is "a subscription satellite digital audio radio service provided pursuant to a satellite digital audio radio service license issued by the Federal Communications Commission on or before July 31, 1998, and any renewal of such license to the extent of the scope of the original license, and may include a limited number of sample channels representative of the subscription service that are made available on a nonsubscription basis in order to promote the subscription service." 17 U.S.C. § 114(j)(10).

(a) Preexisting Subscription Services

In early 2003, three preexisting subscription services (Music Choice, DMX Music Inc., and Muzak LLC) reached agreement with the RIAA, American Federation of Television and Radio Artists, and American Federation of Musicians of the United States and Canada on what the terms and rates should be for the use of sound recordings by the preexisting subscription services under the Section 114 statutory license. On Jan. 30, 2003, the Copyright Office published the proposed rates and terms for comment on their possible adoption without the convening of a CARP. The proposal covered rates and terms for the period Jan. 1, 2002 through Dec. 31, 2007. SoundExchange would be the agent designated to receive the royalty payments.[2648] On July 3, 2003, having received no objections, the Copyright Office adopted the proposed rates and terms as final. Licensees were required to pay 7% of monthly gross revenues from residential services in the United States for the period Jan. 1, 2002 through Dec. 31, 2003, and 7.25 % for Jan. 1, 2004 through Dec. 31, 2007. In addition, an advance payment of $100,000 was required each year, due by Jan. 20 of each year.[2649]

On Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004 ("CRDRA")[2650] was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with a Copyright Royalty Board (CRB) comprised of three permanent Copyright Royalty Judges (CRJs).

On Jan. 9, 2006, the CRB announced commencement of a proceeding to determine rates and terms of royalty payments under Sections 114 and 112 for preexisting subscription services and preexisting satellite digital audio radio services ("SDARS").[2651] SoundExchange, Music Choice, Muzak, XM, Sirius, Royalty Logic Inc. and THP Capstar Acquisition dba DMX Music, all filed petitions in response. DMX and Sirius asserted that they qualified as preexisting subscription services and were thus eligible for the earlier, below-market rates established by the CARP in May 1998 and revised in July 2003. SoundExchange challenged this assertion, arguing that they did not qualify as a preexisting service under Section 114(j)(11) because neither had provided digital audio transmissions on or before July 31, 1998. On Aug. 21, 2006, the CRB referred this question to the Register of Copyrights for a ruling.[2652]

In November of 2006, in response to the CRB's request, the Copyright Office published in the Federal Register a memorandum opinion concluding that

> eligibility for a preexisting subscription service license is limited to subscription services that satisfy the definition of 17 U.S.C. § 114(j)(11), which includes being in operation on July 31, 1998 and continuously operating since that time. In 1998, Congress identified

---

[2648] 68 Fed. Reg. 4744 (Jan. 31, 2003).

[2649] 68 Fed. Reg. 39837 (July 3, 2003).

[2650] Pub. L. No. 108-419, 118 Stat. 2341 (2004).

[2651] 71 Fed. Reg. 1455 (Jan. 9, 2006).

[2652] "Copyright Royalty Board Sets New Rates for Satellite Radio Providers XM and Sirius," *BNA's Patent, Trademark & Copyright Journal* (Dec. 14, 2007) at 160.

> those entities which satisfied the definition and were eligible at that time as being DMX, Music Choice and the DiSH Network. Therefore, today, those same services are the only ones that may qualify as being preexisting subscription services, since they are the only ones which can satisfy the requirement of being in operation as of July 31, 1998. Moreover, for purposes of participating in a rate setting proceeding, the term 'preexisting subscription service' is best interpreted as meaning the business entity which operates under the statutory license. A determination of whether DMX is the same service that was identified by the legislative history in 1998 and has operated continuously since that time requires a factual analysis that is beyond the scope of the Register's authority for questions presented under 17 U.S.C. § 802(f)(1)(B).[2653]

Over the next year, various parties either entered into independent settlement arrangements with SoundExchange, were dismissed by the CRB, or withdrew from the proceedings, leaving only Sirius and XM to proceed as SDARS.[2654] In June 2007, SoundExchange and Music Choice entered into an agreement that was submitted to the royalty judges pursuant to 17 U.S.C. § 801(b)(7)(A). On Oct. 31, 2008, the CRB published a Notice of Proposed Rulemaking requesting comment on the proposed rates and terms submitted to the CRB. Having received no objections from a party that would be bound by the proposed rates and terms, the CRB adopted them in its final regulations on Dec. 19, 2007, effective Jan. 1, 2008.[2655] The rates stipulated that from 2008 through 2011, the royalty fees would be 7.25% of the licensee's monthly gross revenues resulting from residential services in the United States, and for 2012 the fee would be 7.25% of monthly gross revenues. These rates also include a minimum, non-refundable, annual fee of $100,000, credited against royalties due in that year.[2656] The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.[2657]

On Jan. 10, 2008, the CRB issued its decision setting the statutory royalty rate that XM and Sirius must pay to artists and record labels through 2012 as follows: 6.0% for 2007 and 2008; 6.5% for 2009; 7.0% for 2010; 7.5% for 2011; and 8.0% for 2012. The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but again declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.[2658]

[2653] 71 Fed. Reg. 64639, 64640 (Nov. 3, 2006).

[2654] "Copyright Royalty Board Sets New Rates for Satellite Radio Providers XM and Sirius," *BNA's Patent, Trademark & Copyright Journal* (Dec. 14, 2007) at 160-61.

[2655] 72 Fed. Reg. 71795 (Dec. 19, 2007); "Fees, Terms Set for Transmission Of Sound Recordings by Preexisting Services," *BNA's Patent, Trademark & Copyright Journal* (Jan. 04, 2008) at 222.

[2656] 72 Fed. Reg. 71795, 71796 (Dec. 19, 2007).

[2657] Id.

[2658] 73 Fed. Reg. 4080, 4102 (Jan. 24, 2008).

These decisions were cast in doubt, however, when the Register of Copyrights issued a determination on Feb. 19, 2008 stating that the CRB had committed clear legal error by failing to set separate values for the Section 112 and Section 114 licenses, and failing to include a minimum fee for the Section 112 license. The Register found the failure to set separate values to be problematic because the beneficiaries of each license may not be identical, as the Section 112 statutory license applies to reproductions and the Section 114 statutory license applies to public performances.[2659]

The impact of the Register's determination was initially unclear. Although Section 802(f)(1)(D) allows the Register to issue a decision correcting legal errors made by the CRB after a final determination has issued, the CRB may revise final determinations only to correct "technical or clerical errors," or to modify the "terms but not the rates… in response to unforeseen circumstances that would frustrate the proper implementation of such determination."[2660] While the Register's determination is binding on the CRB in subsequent proceedings, it was unclear if it would have an effect on the rates already set through 2012.[2661]

A partial answer came in the form of SoundExchange, Inc. v. Librarian of Congress,[2662] in which SoundExchange contested the CRB's 2008 rate-setting decision, arguing that the rates should be closer to 13% of royalties. The court rejected this argument, noting that the CRB's decision was not arbitrary and capricious. However, the court agreed with the Register's determination that the conflation of Section 112 and 114 rates was improper, but found that the evidence in the record was insufficient for it to set a rate, and so remanded the case to the CRB to set a royalty rate that disaggregated the Section 112 and 114 royalties.[2663]

The CRB then adopted a final rule on rates and terms for preexisting subscription services and satellite digital audio radio services, effective March 5, 2010, establishing monthly royalties for the performances equal to the following percentages of monthly gross revenues resulting from residential services in the U.S.:

6.0% for 2007 and 2008
6.5% for 2009
7.0% for 2010

[2659] 73 Fed. Reg. 9143, 9146 (Feb. 19, 2008) ("Royalties collected under section 114 are paid to the performers and the copyright owners of the sound recordings, i.e., usually the record companies; whereas, the royalties collected pursuant to the section 112 license are not paid to performers."); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

[2660] 17 U.S.C. § 803(c)(4); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 447.

[2661] "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

[2662] 571 F.3d 1220 (D.C. Cir. 2009).

[2663] SoundExchange, Inc. v. Librarian of Congress, 571 F.3d 1220, 1225-26 (D.C. Cir. 2009); "Copyright Royalty Judges' Rate Determination for Satellite Radio Performances Stands," *Bloomberg Law Reports – Intellectual Property*, Vol. 3, No. 30 (July 27, 2009) at 1-2.

7.5% for 2011
8.0% for 2012

Additionally, royalties for ephemeral recordings made in connection with such performances were set at 5% of the total royalties for the transmissions that they are made to facilitate (thereby differentiating the Section 112 and 114 royalties).[2664]

(b) Eligible Nonsubscription Services (Webcasters)

While the CARP proceedings for eligible nonsubscription services were pending, the major record labels and representatives of various FCC-licensed broadcasters reached an agreement in Dec. 2001 on royalty rates to be paid by FCC-licensed broadcasters when they simultaneously stream their AM/FM broadcasts during the period from Oct. 28, 1998 through Dec. 31, 2008.[2665] The settling parties submitted a request to the Copyright Office to withdraw from the CARP, further requesting that the Copyright Office withdraw the issue of AM/FM streaming from the CARP and publish the settled rates in the Federal Register for public comment after the CARP had delivered its report on the remaining issues in the proceeding. They requested that, if there were no objections to the published settled rates, the Librarian of Congress adopt those rates. The settling parties insisted, however, that the settled rates not be revealed to the CARP before the CARP's determination of the royalty rates that should apply to nonsubscription digital audio transmissions other than AM/FM streaming (i.e., webcasting).[2666]

The Copyright Office rejected the settling parties' requests, noting that neither the copyright statute nor existing regulations provided for negotiation and settlement of generally applicable royalty rates after a CARP has been empaneled. The Copyright Office therefore ruled that the AM/FM streaming rate would have to be resolved in the CARP proceeding, and further noted that the parties were free to make a joint submission to the CARP urging that it adopt the rates upon which they had agreed.[2667]

The CARP issued its ruling on Feb. 20, 2002, setting the recommended performance fees at 0.14 cents per performance for webcasting to Internet listeners for free and at 0.07 cents per performance for simultaneous webcasting of AM/FM broadcasts by traditional FCC-licensed broadcasters.[2668] The CARP's recommendations were reviewed by the Copyright Office, which recommended to the Librarian of Congress that the Librarian reject the rates set forth in the CARP's report. On June 20, 2002, the Librarian published his final decision on the matter, which abandoned the CARP's two-tiered rate structure of 0.14 cents per performance for Internet-only transmissions and 0.07 cents for each retransmission of a performance in an AM/FM radio broadcast, deciding instead that the rate of 0.07 cents should apply to both types of transmission.

[2664] 75 Fed. Reg. 5513 (Feb. 3, 2010).

[2665] Order, Docket No. 2000-9 CARP DTRA 1&2 (Jan. 7, 2002), at 1.

[2666] Id.

[2667] Id. at 1-2.

[2668] The CARP Report was available online as of Feb. 20, 2002 at www.loc.gov/copyright/carp/webcasting_rates.html.

The foregoing rates applied for the period from Oct. 28, 1998 through Dec. 31, 2002.[2669] The Register of Copyright's rationale for rejection of the CARP rates, together with the Librarian's order adopting the Register's recommendation, were published on July 8, 2003 at 67 Fed. Reg. 45239. The D.C. Circuit rejected various challenges to the Librarian's decision, allowing it to stand.[2670]

On Jan. 30, 2002, the Copyright Office announced the initiation of the next voluntary six-month negotiation period for determining reasonable rates and terms for eligible nonsubscription services for the 2003-2004 period.[2671] No settlements were reached and the Copyright Office on Nov. 20, 2002 requested interested parties to file notices of intent to participate in, and written comments and proposals for the scheduling of, a CARP proceeding.[2672]

On Dec. 4, 2002, President Bush signed into law the Small Webcaster Settlement Act of 2002 ("SWSA"), Pub. L. 107-321, 116 Stat. 2780, which amended the royalty rates to be paid for the Section 112 and Section 114 statutory licenses by an "eligible small webcaster" and by noncommercial webcasters. The SWSA is the legislative embodiment of an agreement negotiated between small webcasters and the RIAA.[2673] Among other things, the SWSA allows SoundExchange, the Receiving Agent designated by the Librarian of Congress in his June 20, 2002 order for collecting royalty payments made by eligible nonsubscription transmission services under the Section 112 and Section 114 statutory licenses,[2674] to enter into agreements on behalf of all copyright owners and performers to set rates, terms and conditions for eligible small webcasters operating under those statutory licenses.

Section 8(f) of the SWSA defines an "eligible small webcaster" as "a person or entity that has obtained a compulsory license under 17 U.S.C. 112 or 114 and the implementing regulations therefor to make eligible nonsubscription transmissions and ephemeral recordings that–

> (1) For the period beginning on October 28, 1998, and ending on December 31, 2002, has gross revenues during the period beginning on November 1, 1998, and ending on June 30, 2002, of not more than $1,000,000;
>
> (2) For 2003, together with its affiliates, has gross revenues during 2003 of not more than $500,000; and

---

[2669] Librarian of Congress, "Webcasting Determination," available as of June 21, 2002 at www.copyright.gov/carp/webcasting_rates_final.html.

[2670] Beethoven.com LLC v. Librarian of Congress, 394 F.3d 939 (D.C. Cir. 2005).

[2671] 67 Fed. Reg. 4472 (Jan. 30, 2002).

[2672] 67 Fed. Reg. 70093 (Nov. 20, 2002).

[2673] The agreement is published at 67 Fed. Reg. 78510 (Dec. 24, 2002).

[2674] See 67 Fed. Reg. 45239 (July 8, 2002).

(3) For 2004, together with its affiliates, has gross revenues plus third party participation revenues and revenues from the operation of new subscription services during 2004 of not more than $1,250,000."[2675]

The SWSA governed the period from Oct. 28, 1998 through Dec. 31, 2004. During that period, eligible small webcasters could elect to pay the royalty rates established by the SWSA rather than the statutory rates determined by any other applicable method, such as a CARP proceeding. To be eligible for the SWSA rates, an eligible small webcaster was required to submit a completed and signed election form to SoundExchange by no later than the first date on which the webcaster would have to make a royalty payment under the SWSA. Subject to certain minimum annual fees, the royalty rates under the SWSA for Oct. 28, 1998 through Dec. 31, 2002 were 8 percent of a webcaster's gross revenues or 5 percent of its expenses, whichever is greater. For 2003 and 2004, the royalty rates were 10 percent of the webcaster's first $250,000 in gross revenues and 12 percent of any gross revenues in excess of $250,000 during the applicable year, or 7 percent of the webcaster's expenses during the applicable year, whichever is greater.[2676] Under Section 5 of the SWSA, the minimum annual fees ranged from $500 to $5,000, depending upon the year and the gross revenues of the webcaster.[2677]

In June of 2003, the RIAA and educational and other tax exempt institutions reached an agreement under which college radio stations and other educational broadcast stations staffed substantially by students enrolled and the educational institution could pay even further discounted license fees for webcasting in the amount of a flat fee of $200 annually for the years 1998 and 1999, $250 annually for the years 2000 through 2003, and a fee of $500 for 2004, except that educational institutions having fewer than 10,000 students could continue to pay only $250 in 2004. The agreement allowed noncommercial webcasters at other tax exempt institutions to pay an annual fee of between $200 and $500, depending upon whether the webcasting is done through a single or multiple channels. The agreement applied retroactively to October 28, 1998 and lasted through the end of 2004.[2678]

In May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA, acting under the provisions of the SWSA, agreed on a proposal for royalty rates to be paid by eligible non-subscription services for the 2003 and 2004 statutory licensing period and by new subscription services from 1998 through Dec. 31, 2004 (the "SWSA Agreement"), and submitted the proposal to the Copyright Office for possible adoption without a CARP. The agreement also established proposed rates for Internet streaming of AM/FM broadcasts. On May 20, 2003, the Copyright Office published the proposal for comment, which would establish the

---

[2675] Id. at 78513.

[2676] Id. at 78511.

[2677] Id. at 78512.

[2678] 68 Fed. Reg. 35008 (June 11, 2003).

royalty rates for each of the three categories of services set forth in the table below.[2679] On Feb. 6, 2004, the Copyright Office adopted the proposal as a final rule.[2680]

Eligible Non-subscription Services	Option of paying royalties as follows: Per Performance Option – 0.0762 cents per performance for digital audio transmissions Aggregate Tuning Hour Option – 1.17 cents per aggregate tuning hour for all channels and stations except channels and stations where the programming consists of non-music programming, such as news, talk, sports or business programming. For such non-music channels and stations, the licensee must pay 0.0762 cents per aggregate tuning hour. Minimum Annual Fee: $2,500 Ephemeral Recordings: These rates will be deemed to include the royalties payable for ephemeral recordings
New Subscription Services	Options of paying royalties as follows: Per Performance Option – 0.0762 cents per performance for digital audio transmissions Aggregate Tuning Hour Option – 1.17 cents per aggregate tuning hour for all channels and stations except channels and stations where the programming consists of non-music programming, such as news, talk, sports or business programming. For such non-music channels and stations, the licensee must pay 0.0762 cents per aggregate tuning hour. Percentage of Subscription Revenues Option – 10.9% of subscription service revenue, but in no event less than 27 cents per month for each person who subscribes. Minimum Annual Fee: $2,500 Ephemeral Recordings: These rates will be deemed to include the royalties payable for ephemeral recordings
Internet Streaming of AM/FM Broadcasts	Streaming: 0.88 cents per aggregate tuning hour Ephemeral Recordings: The rate for ephemeral recordings by business establishment services is 10% of gross proceeds.

Webcasters wishing to take advantage of the SWSA Agreement were required to submit a completed and signed election form to SoundExchange no later than 30 days after the publication of the rates and terms in the Federal Register, or for those webcasters who had not yet made a digital audio transmission as of such publication, no later than the first date on which they would be obligated to make royalty payments.

[2679] 68 Fed. Reg. 27506 (May 20, 2003).

[2680] 69 Fed. Reg. 5693 (Feb. 6, 2004).

On August 21, 2003, the Copyright Office published proposed rates and terms for noncommercial webcasters who elected not to operate under the rates and terms set under the SWSA Agreement.[2681] Those proposed rates and terms were the same as those that were set for the period ending December 31, 2002 in the Order of the Librarian of Congress published July 8, 2002 at 67 Fed. Reg. 45239. On Feb. 6, 2004, the Copyright Office adopted the proposed rates and terms as a final rule for the 2003 and 2004 statutory licensing period.[2682]

On June 18, 2003, the Copyright Office issued a final rule governing SoundExchange as the authorized agency to collect and distribute the statutory royalties for subscription digital transmission services and webcasting, including small webcasters.[2683] The rules governing the collection, distribution, and audit of royalties by SoundExchange may be found at 37 C.F.R. §§ 260.3 & 260.6.

As noted earlier, on Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004 ("CRDRA")[2684] was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with a Copyright Royalty Board (CRB) comprised of three permanent Copyright Royalty Judges (CRJs). The Act also reformed the way webcasters participate in the rate setting process. Webcasters must file a petition to participate, which costs $150 to file, but parties with similar interests may split the cost by filing a joint petition. The CRJs provide a list of participants to all parties, who then have three months to negotiate their own royalty rates. If the parties are unable to agree, the CRJs will accept written comments for four to five months. These comments may include witness statements, testimony and exhibits to be presented in the proceeding, as well as other information necessary to establish terms and rates. The comment period is followed by a 60-day discovery period. Finally, the parties have one more opportunity to negotiate their own settlement at a settlement conference scheduled by the CRJs to take place outside the presence of the CRJs. Only then will the CRJs begin proceedings to set the rates.[2685]

The Act also terminated the voluntary negotiation proceeding initiated by the Copyright Office in January 2004 to set rates for the 2005-2006 period for eligible nonsubscription services.[2686] On Feb. 8, 2005, as required by the Act, the Copyright Office published a notice that the rates and terms for the statutory licenses in effect on Dec. 31, 2004, for new subscription services, eligible nonsubscription services, and services exempt under Section 114(d)(1)(C)(iv), as well as the rates and terms for small webcasters published in the Federal Register under the authority of the SWSA for the years 2003-2004, would remain in effect for at least 2005.[2687] On

---

[2681] 68 Fed. Reg. 50493 (Aug. 21, 2003).

[2682] 69 Fed. Reg. 5693 (Feb. 6, 2004).

[2683] 68 Fed. Reg. 36469 (June 18, 2003).

[2684] Pub. L. No. 108-419, 118 Stat. 2341 (2004).

[2685] Allison Kidd, "The Beginning of the End of the Internet Radio Royalty Dispute," *Journal of Internet Law*, Oct. 2005, at 15, 22.

[2686] 69 Fed. Reg. 689 (Jan. 6, 2004).

[2687] 70 Fed. Reg. 6736 (Feb. 8, 2005).

Feb. 16, 2005, again as required by the Act, the Copyright Office published a notice initiating a proceeding, and requesting petitions to participate therein, to establish or adjust rates and terms for the statutory licenses for new subscription services and eligible nonsubscription services for the period commencing Jan. 1, 2006 through Dec. 31, 2010.[2688]

After two years of testimony, on May 1, 2007, the CRB published in the Federal Register its final rule and order setting forth its decision as to the royalties that "Commercial Webcasters" (i.e., non-interactive new subscription services and eligible nonsubscription services, including simultaneous digital audio retransmissions of over-the-air AM or FM radio broadcasts) must pay to stream copyrighted music over the Internet. The new rates abandoned the existing percentage-of-revenue scheme in favor of an annual flat per-station rate structure up to a specified cap, coupled with a per-performance rate for services that exceed the cap, where "performance" is defined as the streaming of one song to one listener. The annual per-channel and per-station rate for non-commercial webcasters not exceeding 159,140 aggregate tuning hours per month and for Commercial Webcasters was set at $500 per year. The per-performance rates for transmissions in excess of that limit by non-commercial webcasters, and for any transmissions by Commercial Webcasters, retroactive to Jan. 1, 2006, were set at:

$0.0008 for 2006
$0.0011 for 2007
$0.0014 for 2008
$0.0018 for 2009
$0.0019 for 2010

These rates were inclusive of both the Section 114 license fees and the royalty payable under Section 112 for ephemeral recordings used solely to facilitate transmissions for which it paid royalties.[2689]

The CRB's decision caused great controversy and protest, particularly among small webcasters, who claimed the rates were so high that they would put the webcasters out of business. Several bills were introduced in Congress and negotiations with SoundExchange took place to reduce the rates for small webcasters. On May 22, 2007 SoundExchange announced that it would extend for another three years (through 2010) the previous, lower rates under the SWSA for small webcasters (i.e., 10% of gross revenue up to $250,000 and 12% of revenue exceeding that amount).[2690] On Aug. 21, 2007, SoundExchange set out certain conditions that

---

[2688] 70 Fed. Reg. 7970 (Feb. 16, 2005).

[2689] 72 Fed. Reg. 24084, 24111 (May 1, 2007). The CRB's decision was initially set forth in a report published on its web site on Mar. 2, 2007. Representatives of the Intercollegiate Broadcasting System Inc., DiMA, National Public Radio, the Radio Broadcasters, Royalty Logic Inc., WHRB (FM), SoundExchange, and many small commercial webcasters filed a series of motions seeking a rehearing on the royalty scheme. On April 16, 2007, the CRB rejected the motions. On July 11, 2007, the U.S. Court of Appeals for the D.C. Circuit denied a petition filed by webcasters seeking to stay the CRB's determination. "SoundExchange Offers Webcasters Reprieve After D.C. Court Denies Petition to Stay," *BNA's Patent, Trademark & Copyright Journal* (July 20, 2007) at 345.

[2690] Id.

had to be met by a small webcaster to qualify for the favorable rates – the webcaster had to earn less than $1.2 million in total annual revenue and could not exceed a total of 5 million aggregate tuning hours each month. Should the threshold be exceeded, the webcaster would be required to pay the CRB's published rates. SoundExchange announced that the agreement would apply only to performance royalties collected on behalf of the 20,000 recording artists and 3,500 record labels represented by the collective – royalties due to other artists and labels would be payable under the CRB's rates. Interested webcasters had until Sept. 14, 2007 to accept the offer.[2691]

On Aug. 23, 2007, SoundExchange also announced an accord on the amount of fees some large webcasters would pay – specifically, that a $50,000 cap would replace the $500 per-station minimum fee set by the CRB. In return for the cap, the signatory webcasters agreed within six months to begin collecting and reporting census information on all songs streamed over the Internet. SoundExchange and DiMA also agreed to form a committee designed to analyze the issue of audio stream-ripping and technological solutions that might be available. The agreement did not, however, disturb the CRB's per-performance royalty fees.[2692]

On Aug. 10, 2007, the Copyright Office, acting under the provisions of the CRDRA, formally terminated all open proceedings under the old CARP system.[2693]

On Oct. 16, 2008, President Bush signed into law the Webcaster Settlement Act of 2008 ("WSA 2008"), Pub. L. 110-435, 122 Stat. 4974, in order to provide more time for SoundExchange and webcasters to come up with an agreement on royalty rates. Modifying Section 114(f)(5), the WSA 2008 granted SoundExchange the authority to make settlements until Feb. 15, 2009, and allowed any agreement reached to have terms in force until the end of 2016. It also eliminated all mentions of "small webcaster," replacing it with simply "webcaster," thereby allowing webcasters of any size to enter into negotiated agreements. The WSA 2008 further allowed the parties to agree that their alternative rates may be drawn on as precedent in future rate-setting proceedings, and also made optional the requirements for what shall be included in such agreements.[2694]

In January 2009, the Corporation for Public Broadcasting and SoundExchange came to an agreement establishing royalties to be paid on behalf of public radio systems for streaming sound recordings on about 450 public radio web sites from 2005 thorugh 2010. The agreement provides SoundExchange with a single up-front payment of $1.85 million, along with consolidated usage and playlist information to assist with the process of compensating individual artists. Additionally, National Public Radio agreed to withdraw its appeal of a May 2007 CRB

[2691] "SoundExchange Agrees to Separate Royalty Deals Between Large and Small Webcasters," *BNA's Patent, Trademark & Copyright Journal* (Aug. 31, 2007) at 530.

[2692] Id. at 529.

[2693] 72 Fed. Reg. 45071 (Aug. 10, 2007).

[2694] "Congress Votes to Allow Webcasters To Negotiate Rates With Sound Exchange," *BNA's Patent, Trademark & Copyright Journal* (Oct. 3, 2008) at 753.

rate decision.[2695] Several weeks later, in February, the National Association of Broadcasters also reached an agreement with SoundExchange to lower the Internet broadcasting rates for participating radio stations by about 16% in 2009 and 2010, with stations paying an annual fee of $500 for each channel and a per-performance royalty rate of $0.0008 in 2006, increasing to $0.0025 in 2015, with a ceiling of $50,000.[2696] A group of small webcasters, including Attention Span Radio, Blogmusik, Born Again Radio, Music Justice, My Jazz Network, and Voice of Country, also came to an agreement with SoundExchange that covered 2006 though 2015. Under the agreement, transmissions cannot exceed 5 million tuning hours per month, and the rates are calculated as either:

> (1) the greater of 10% of the webcaster's first gross revenue in excess of $250,000, or 12% of any annual gross revenue exceeding $250,000; or
>
> (2) 7% of the webcaster's annual expenses. For transmissions exceeding 5 million tuning hours per month, the rates are either those set by the CRB's 2007 determination, or whichever rates are then applicable under Sections 112(e) and 114.[2697]

The Webcaster Settlement Act of 2008 was amended in 2009 to extend the negotiation period, and President Obama signed it into law on June 30, 2009. After two years of negotiations, on July 7, 2009, SoundExchange and "pureplay" webcasters (businesses whose primary form of business is streaming sound recordings under a government license) came to an agreement on music royalties. Web sites with revenue below $1.25 million agreed to pay 12-14% of their revenue in royalties annually, along with an annual $25,000 fee (applied to the royalties owed). The agreement covers the period of 2006 through 2015 for large web sites, or 2006 through 2014 for small web sites.[2698]

The CRB's 2007 determination of rates was challenged in Intercollegiate Broadcast Systems Inc. v. Copyright Royalty Board.[2699] The court largely upheld the determination, ruling that the CRB's interpretation of Section 114 was not unreasonable for failing to assume a perfectly competitive market; that commercial webcasters had failed to show that the rates were "crushing and disproportionate" (and therefore arbitrary and capricious); and that the CRB was justified in determining a per performance rate, rather than a percentage of revenue fee structure for small webcasters. However, because webcasters' services could arguably be seen as offering thousands of channels, the court remanded the question of whether the CRB should cap minimum annual fees for a single licensee, rather than basing such fees on a per-channel-per-

---

[2695] "Public Broadcasters Agree to Web Music Royalties" (Jan. 15, 2009), available as of Aug. 1, 2012 at http://www.lexisnexis.com/community/copyright-trademarklaw/blogs/newsheadlines/archive/2009/01/16/public-broadcasters-agree-to-web-music-royalties.aspx.

[2696] Rachel Metz, "Agreement Reached on Internet Music Royalty Rates," *The Washington Post*, Feb. 17, 2009; 74 Fed. Reg. 9293, 9300 (Mar. 3, 2009).

[2697] 74 Fed. Reg. 9293 (Mar. 3, 2009).

[2698] Nathan Pollard, "SoundExchange and 'Pureplay' Webcasters Reach Royalty Agreement," *BNA News* (July 9, 2009).

[2699] 571 F.3d 69 (D.C. Cir. 2009).

station basis. The court also remanded the issue posed by the $500 minimum fees for noncommercial webcasters, because the court said it was not supported by sufficient evidence in the record.[2700]

Following Intercollegiate Broadcast Systems, the CRB established a comment period in November 2009 for the parties to reach an agreement regarding the remanded minimum annual fee issue, and on Dec. 2 SoundExchange and DiMA submitted a settlement. The settlement was published for comment on Dec. 23,[2701] and soon after adopted as final, setting the minimum annual fee for commercial webcasters at $500 for 2006-2010.[2702] The second issue on remand, concerning the $500 fee for noncommercial broadcasters, was settled by the CRB in a Sept. 17 decision in favor of upholding the fee. The CRB ruled that the evidence presented on remand supported at least a $500 minimum fee for noncommercial webcasters, and that the industry demonstrated an acceptance of these minimum fees, as evidenced in the agreements that industry representatives have entered into pursuant to the Webcaster Settlement Acts of 2008 and 2009.[2703]

In U.S. v. American Society of Composers, Authors and Publishers,[2704] the U.S. District Court for the Southern District of New York set the licensing rates and terms that AOL, RealNetworks, and Yahoo! would have to pay in order to publicly perform ASCAP songs over the Internet. The three companies had applied to ASCAP for a blanket license to perform ASCAP-reperatory music over the Internet, but were unable to reach an agreement, so ASCAP petitioned the court for a determination of reasonable royalty rates. Although ASCAP initially claimed that royalty rates should apply to both streaming music and downloads, an earlier proceeding determined that royalty rates should apply only to streaming music because downloads invoke the copyright holder's reproduction right, not the public performance right.[2705] The final rates involved a three-step computation, starting with a calculaton of each company's domestic revenue. Because AOL and Yahoo! offer a variety of services, the domestic revenue figure is then reduced by a "music-use-adjustment" fraction (the total number of hours music is streamed to users by that company, divided by the total number of hours that visitors utilize the site, as determined by the third-party traffic measurement firm comScore Media Metrix). Finally, a 2.5% royalty rate is applied to the remaining revenue figure, producing the royalty rate.[2706]

[2700] Id. at 76-82.

[2701] 74 Fed. Reg. 68214 (Dec. 23, 2009).

[2702] 75 Fed. Reg. 6097 (Feb. 8, 2010).

[2703] 75 Fed. Reg. 56873 (Sept. 17, 2010).

[2704] 559 F. Supp. 2d 332 (S.D.N.Y. 2008).

[2705] U.S. v. American Society of Composers, Authors and Publishers, 485 F. Supp. 2d 438 (S.D.N.Y. 2007); "Court Sets Music Royalty Rate, Terms Through 2009 for Three Online Services," *BNA's Electronic Commerce & Law Report* (May 7, 2008) at 623.

[2706] "Court Sets Music Royalty Rate, Terms Through 2009 for Three Online Services," *BNA's Electronic Commerce & Law Report* (May 7, 2008) at 623-4.

(c) New Subscription Services

On Feb. 12, 2001, the Copyright Office announced the initiation of the six-month statutory voluntary negotiation period for determining reasonable rates and terms for the statutory license for new subscription services.[2707] No agreements were reached. After the close of the negotiation period, the Copyright Office received petitions requesting that a CARP be convened to establish terms and rates for the statutory license covering new subscription services. The petitioners also requested that the Copyright Office consolidate the proceeding for new subscription services with the proceeding for pre-existing satellite digital audio radio services and pre-existing subscription services.[2708] As discussed in the previous subsection, in May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA agreed on a proposal for royalty rates to be paid by new subscription services for the period from 1998 through Dec. 31, 2004, and submitted the proposal to the Copyright Office for possible adoption without a CARP. On May 20, 2003, the Copyright Office published the proposal for comment.[2709] On Feb. 6, 2004, the Copyright Office adopted the proposal as a final rule.[2710]

As noted in the previous subsection, on Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004[2711] was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with three permanent Copyright Royalty Judges. In addition, the Act terminated the voluntary negotiation proceeding initiated by the Copyright Office in February 2004 to set rates for the 2005-2006 period for new subscription services.[2712] On Feb. 8, 2005, as required by the Act, the Copyright Office published a notice that the rates and terms for the statutory licenses in effect on Dec. 31, 2004, for new subscription services, eligible nonsubscription services, and services exempt under Section 114(d)(1)(C)(iv), as well as the rates and terms for small webcasters published in the Federal Register under the authority of the SWSA for the years 2003-2004, would remain in effect for at least 2005.[2713] On Feb. 16, 2005, again as required by the Act, the Copyright Office published a notice initiating a proceeding, and requesting petitions to participate therein, to establish or adjust rates and terms for the statutory licenses for new subscription services and eligible nonsubscription services for the period commencing Jan. 1, 2006.[2714]

After two years of testimony, on May 1, 2007, the CRB published in the Federal Register its final rule and order setting forth its decision as to the royalties that non-interactive new

---

[2707] 66 Fed. Reg. 9881 (Feb. 12, 2001).

[2708] 66 Fed. Reg. 58180 (Nov. 20, 2001).

[2709] 68 Fed. Reg. 27506 (May 20, 2003).

[2710] 69 Fed. Reg. 5693 (Feb. 6, 2004).

[2711] Pub. L. No. 108-419, 118 Stat. 2341 (2004).

[2712] 69 Fed. Reg. 5196 (Feb. 3, 2004).

[2713] 70 Fed. Reg. 6736 (Feb. 8, 2005).

[2714] 70 Fed. Reg. 7970 (Feb. 16, 2005).

subscription services must pay to stream copyrighted music over the Internet for the period 2006 through 2010. The details of that decision are set forth in the preceding subsection.

On Oct. 31, 2005, XM Satellite Radio, Inc., filed a Petition to Initiate and Schedule Proceeding for a "new type of subscription service [which] performs sound recordings on digital audio channels programmed by the licensee for transmission by a satellite television distribution service to its residential customers, where the audio channels are bundled with television channels as part of a 'basic' package of service and not for a separate fee."[2715] The CRB published a notice in the Federal Register on Dec. 5, 2005 announcing commencement of the proceedings to set rates and terms for the royalty payments under Sections 112 and 114 for the activities of the new subscription service described in the XM Petition and soliciting interested parties to participate.[2716] Sirius Satellite Radio, Inc. ("Sirius"), XM, MTV Networks ("MTV"), and SoundExchange, Inc petitioned to participate, and the parties reached a settlement, with the proposed rates and terms filed on Oct. 30, 2007.[2717] On Nov. 9, 2007, the CRB published a Notice of Proposed Rulemaking requesting comment on the proposed rates and terms submitted to the CRB, and adopted the proposed rates and terms in its final regulations on Dec. 20, 2007.[2718]

The final rates for stand-alone contracts[2719] are the greater of 15% of revenue, or the following monthly minimum payment per subscriber:

$0.0075 from inception through 2006
$0.0075 for 2007
$0.0075 for 2008
$0.0125 for 2009
$0.0150 for 2010

For bundled contracts,[2720] the final rates are the greater of 15% of revenue allocated to reflect the objective value of the licensee's service, or the following monthly minimum payment per subscriber:

$0.0220 from inception through 2006
$0.0220 for 2007
$0.0220 for 2008

[2715] 72 Fed. Reg. 72253 (Dec. 20, 2007).

[2716] 70 Fed. Reg. 72471 (Dec. 05, 2005).

[2717] 72 Fed. Reg. 72253 (Dec. 20, 2007).

[2718] Id.

[2719] "Stand-alone contracts" mean contracts between the licensee and a cable or satellite television provider in which the service is the only content licensed by the licensee to the provider. See 72 Fed. Reg. 72253, 72255 (Dec. 20, 2007).

[2720] "Bundled contracts" mean contracts between the licensee and a cable or satellite television provider in which the service is not the only content licensed by the licensee to the provider. 72 Fed. Reg. 72253, 72255 (Dec. 20, 2007).

$0.0220 for 2009
$0.0250 for 2010

These rates also include a minimum, non-refundable, annual fee of $100,000, credited against royalties due in that year. The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.[2721]

As mentioned above in the section on preexisting subscription services, the Register of Copyrights issued a determination on Feb. 19, 2008 that stated that the CRB had committed clear legal error by failing to set separate values for the Section 112 and Section 114 licenses, and including a minimum fee for the Section 112 license.[2722] Soon after, in SoundExchange, Inc. v. Librarian of Congress,[2723] the court agreed with the Register's determination that the conflation of Section 112 and 114 rates was improper, but found that the evidence in the record was insufficient for it to set a rate, and so remanded the case to the CRB to set a royalty rate that disaggregated the Section 112 and 114 royalties.[2724]

In January 2009, the CRB commenced another rate determination process for new subscription services for the license period 2011-2015,[2725] and petitions to participate were received from SoundExchange, Royalty Logic, and Sirius XM Radio. The parties reached a settlement in late 2009, and on Jan. 22, 2010, the CRB published a notice seeking comments on the rates proposed by the settlement.[2726] Having received no comments or objections, the CRB adopted the proposed rates as final, amending 37 CFR 383.[2727] The final rates for stand-alone contracts are the greater of 15% of revenue, or the following monthly minimum payment per subscriber:

$0.0155 for 2011
$0.0159 for 2012
$0.0164 for 2013
$0.0169 for 2014
$0.0174 for 2015

[2721] Id.

[2722] 73 Fed. Reg. 9143, 9146 (Feb. 19, 2008) ("Royalties collected under section 114 are paid to the performers and the copyright owners of the sound recordings, i.e., usually the record companies; whereas, the royalties collected pursuant to the section 112 license are not paid to performers."); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

[2723] 571 F.3d 1220 (D.C. Cir. 2009).

[2724] SoundExchange, Inc. v. Librarian of Congress, 571 F.3d 1220 (D.C. Cir. 2009); "Copyright Royalty Judges' Rate Determination for Satellite Radio Performances Stands," *Bloomberg Law Reports – Intellectual Property*, Vol. 3, No. 30 (July 27, 2009) at 1-2.

[2725] 74 Fed. Reg. 319 (Jan. 5, 2009).

[2726] 75 Fed. Reg. 3666 (Jan. 22, 2010).

[2727] 75 Fed. Reg. 14074, 14075 (Mar. 24, 2010).

For bundled contracts, the final rates are the greater of 15% of revenue allocated to reflect the objective value of the licensee's service, or the following monthly minimum payment per subscriber:

$0.0258 for 2011
$0.0265 for 2012
$0.0273 for 2013
$0.0281 for 2014
$0.0290 for 2015

In response to the Register of Copyrights' Feb. 19 2009 decision requiring that Section 112 and 114 royalties be disaggregated, the new rates also state that the royalty for Section 112(e) constitutes 5% of the total royalty payments under this agreement.[2728] Finally, the recordkeeping provisions of this agreement do not require licensees to report their performances.[2729]

3. The Digital Performance Right – What Constitutes an "Interactive" Service

The Section 114 statutory license does not apply to an "interactive service." Section 114(j)(7) defines an "interactive service" as a service "that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient." Section 114(j)(7) further provides that the "ability of individuals to request that particular sound recordings be performed for reception by the public at large, or in the case of a subscription service, by all subscribers of the service, does not make a service interactive, if the programming on each channel of the service does not substantially consist of sound recordings that are performed within 1 hour of the request or at a time designated by either the transmitting entity or the individual making such request. If an entity offers both interactive and noninteractive services (either concurrently or at different times), the noninteractive component shall not be treated as part of an interactive service."

As might be expected, considerable controversy has arisen over the application of the definition of "interactive service." A number of lawsuits have been filed involving the issue:

– On May 24, 2001, ten recording companies sued Launch Media, Inc. for copyright infringement, alleging that Launch's LAUNCHcast service created an interactive radio station by providing users with the ability to select specific artists, to rate artists and recordings, to select certain music that the user had or had not previously rated, to permanently block particular recordings, to skip the current recording and move on to the next one, and to pause the current

[2728] Id.

[2729] Id. at 14076.

recording and resume from the same point later.[2730] This lawsuit eventually led to a decision by the Second Circuit on the meaning of an "interactive" service, discussed in subsection (a) below.

– On June 1, 2001, Launch and other online webcasters, acting through the Digital Media Association (DiMA), filed a declaratory judgment action against the RIAA, seeking a declaration that their webcasting services were eligible for the statutory license because the songs played "ultimately are generated by a computer in a manner designed to ensure compliance with the DMCA's statutory license provision"; users "do not determine the particular sound recordings or the particular artists which become the basis of the transmission; and [they] have no ability to select or obtain advance knowledge as to the particular songs that are streamed on the stations"; "[a]rtist identification on the services is representative only"; the "skip" function on the services operates only forward and users "can never know which song they are 'skipping forward to'"; and "[i]n all cases the consumer-influenced situations are available to every member of the general public."[2731] The United States District Court for the Southern District of New York denied the parties' cross-motions for dismissal under F.R.C.P. 12(b)(6) and summary judgment.[2732] Launch was later acquired by Yahoo, and settled with a number of the record companies.[2733]

– On June 8, 2001, the record companies responded with three lawsuits against XACT Radio, Musicmatch, Inc., and MTVi Group, each of which provided consumers with access to streamed music over the Internet, asserting against each the same basic allegations as contained in the complaint against Launch. The complaint asserted that the use of the "skip" button by users will cause the defendants to exceed the performance complement restrictions.[2734] Musicmatch subsequently settled its lawsuit with the record companies.

Previously, on April 17, 2000, DiMA had sought to resolve the issues in the Copyright Office, filing a rulemaking petition that sought adoption of the following proposed rule concerning the definition of a "Service" for purposes of the statutory license:

> A Service making transmissions that otherwise meet the requirements for the section 114(f) statutory license is not rendered "interactive," and thus ineligible for the statutory license, simply because the consumer may express preferences to such Service as to the musical genres, artists and sound recordings that may be incorporated into the Service's music programming to the public. Such a Service is not "interactive" under section 114(j)(7), as long as: (i) Its transmissions are made available to the public generally; (ii) the features offered by the Service do not enable the consumer to determine or learn in advance what sound recordings

---

[2730] Hillel Parness, "Internet Radio: As RIAA and DiMA Prepare to Do Battle over 'Interactivity,' Questions Resurface About ISP Liability," *Cyberspace Lawyer*, July/August 2001, at 2, 4.

[2731] Id.

[2732] See Arista Records, LLC v. Launch Media, Inc., 578 F,3d 148, 150 (2d Cir. 2009).

[2733] Brad King, "Yahoo Launches Into Web Music" (June 28, 2001), available as of Feb. 22, 2002 at www.wired.com/news/mp3/0,1285,44884,00.html.

[2734] Parness, supra note 2730, at 4.

will be transmitted over the Service at any particular time; and (iii) its transmissions do not substantially consist of sound recordings performed within one hour of a request or at a time designated by the transmitting entity or the individual making the request.[2735]

The Copyright Office denied the petition, ruling, among other things, that "[i]n light of the rapidly changing business models emerging in today's digital marketplace, no rule can accurately draw the line demarcating the limits between an interactive service and a noninteractive service. Nor can one readily classify an entity which makes transmissions as exclusively interactive or noninteractive."[2736] The Office concluded that the determination of whether a particular activity is "interactive" must be determined on a case by case basis upon a full evidentiary record.[2737]

(a) Arista Records v. Launch Media

In Arista Records, LLC v. Launch Media, Inc.,[2738] the Second Circuit, affirming a jury determination, held that the LAUNCHcast webcasting service was not an "interactive" service within the meaning of Section 114(j)(7) as a matter of law,[2739] and Launch Media could therefore rely on the statutory license for public performances via digital audio transmissions. The LAUNCHcast service enabled a user to create "stations" that played songs within a particular genre or similar to a particular artist or song the user selected. Specifically, upon registering with the service, the user would select artists whose music she preferred. The user would then list genres the user enjoyed and rate them on a scale. The user was also asked the percentage of songs the user had not previously rated the user would like to incorporate into the user's station (the "unrated quota"). The minimum unrated quota was 20%. Once LAUNCHcast began playing music based on the user's preferred artists and genres, the user would rate the songs, artists, and albums played between zero and 100. Below the rating field were hyperlinks termed "history," "share," and "buy." The history hyperlink allowed the user to see a list of the songs previously played, and the buy hyperlink facilitated the user's purchase of the songs. The share hyperlink allowed the user to share the station with other users. That feature facilitated the subscription of one user to another user's station. While a song played, the user had the ability to pause the song, skip the song, or delete the song from the station by rating it zero. The user was not able to go back to restart a song that was playing, or to repeat any of the previously played songs in the playlist.[2740]

Each time the user logged into the LAUNCHcast service and selected a station, the service generated a playlist of 50 songs selected from a hashtable of potential songs that could be

---

[2735] 65 Fed. Reg. 77330, 77331 (Dec. 11, 2000).

[2736] Id. at 77332-33.

[2737] Id. at 77332.

[2738] 578 F.3d 148 (2d Cir. 2009), cert. denied, 2010 U.S. LEXIS 810 (Jan. 25, 2010).

[2739] The court ruled that the issue of interactivity presents an issue of law. Id. at 151-52.

[2740] Id. at 157-58.

put into the playlist. The hashtable was generated using a very complicated algorithm that took into account numerous variables, only some of which included the user's preferred artists and genres and unrated quota.[2741] Although the playlist generated each time a user selected a radio station was unique to that user at that particular time, the Second Circuit determined that the playlist was not "specially created for the recipient" via an interactive service within the meaning of Section 114(j)(7). Based on an extensive review of the legislative history of Section 114(j)(7), the court noted that Congress' primary concern both in creating a performance right in digital audio transmissions and in excluding interactive services from the statutory performance license was to protect sound recording copyright holders from diminution in record sales. Congress believed that interactive services, by providing predictability based on choices by the user, could approximate the predictability the music listener seeks when purchasing music, thereby diminishing music sales. The Second Circuit therefore concluded that the touchstone of an interactive service is whether it is generating playlists specially created for the recipient that have sufficient predictability to the user that the user's willingness to purchase music will be diminished.[2742]

The Second Circuit decided that the methodology used to select the playlists did not provide the user sufficient control to make the playlists so predictable that the user would choose to listen to the webcast in lieu of purchasing music:

> First, the rules governing what songs are pooled in the hashtable ensure that the user has almost no ability to choose, let alone predict, which specific songs will be pooled in anticipation for selection to the playlist. At least 60% of the songs in the hashtable are generated by factors almost entirely beyond the user's control. The playlist – a total of fifty songs – is created from a pool of approximately 10,000 songs, at least 6,000 of which (1,000 of the most highly rated LAUNCHcast songs among all users and 5,000 randomly selected songs) are selected without any consideration for the user's song, artist, or album preferences. The user has control over the genre of songs to be played for 5,000 songs, but this degree of control is no different from a traditional radio listener expressing a preference for a country music station over a classic rock station. LAUNCHcast generates this list with safeguards to prevent the user from limiting the number of songs in the list eligible for play by selecting a narrow genre. Also, no more than 20% of the songs the user rates – marked by LAUNCHcast as explicitly rated – can be pooled in the hashtable, and no more than three times the number of explicitly rated songs divided by the total number of rated songs can be in the hashtable. This ensures that a limited number of explicitly rated songs will eventually be selected for the playlist. Ironically, this effectively means that the more songs the user explicitly rates, the less the user can predict which explicitly rated songs will be pooled in the hashtable and played on the playlist.

[2741] Id. at 158-59.

[2742] Id. at 161.

> Second, the selection of songs from the hashtable to be included in the playlist is governed by rules preventing the user's explicitly rated songs from being anywhere near a majority of the songs on the playlist. At minimum, 20% of the songs played on the station are unrated – meaning the user has never expressed a preference for those songs. If the user attempts to increase her chances of hearing a particular song by rating only a small number of songs – making the user's list of explicitly and implicitly rated songs smaller than 100 – 90% of the songs LAUNCHcast selects for the playlist will be unrated, flooding the playlist with songs for which the user has never expressed a preference.[2743]

The court further noted that even the ways in which songs were rated included variables beyond the user's control. For example, the ratings by all of the user's subscribed-to stations were included in the playlist selection process. When the user rated a particular song, LAUNCHcast then implicitly rated all other songs by that artist, subjecting the user to many songs the user may have never heard or did not even like. In addition, a user who heard a song she liked and wanted to hear again could not do so by logging off and back on to reset the station to disable the restriction against playing the same song twice on a playlist. Even if the user logged off then back on and selected the same station, the user would still hear the remainder of the playlist to which she had previously been listening with its restrictions still in operation, at least until the user had listened to at least 42 of the playlist's songs. LAUNCHcast also did not enable the user to view the unplayed songs in the playlist, ensuring that a user could not sift through a playlist to choose the songs the user wished to hear. In short, the only thing a user could control was to ensure not hearing a particular song on a particular station again by rating it zero. But the court noted that the ability not to listen to a particular song was not a violation of a copyright holder's right to be compensated when the sound recording was played.[2744] Accordingly, the court ruled that, as a matter of law, the LAUNCHcast service was not an interactive service.[2745]

4. The Reproduction Right – Mechanical Licenses and Streaming/Downloading

An area of great controversy has been whether streaming implicates the reproduction right of the copyright holder at all and, if so, whether the compulsory mechanical license of Section 115 of the copyright statute applies to streaming. As discussed in Sections I.A.1 and I.A.2 above, the right of reproduction is potentially implicated when a work is streamed over the Internet because interim whole or partial copies of the work are made in various RAM memories in the course of transmission of the work. Entities that conduct streaming have sought to avoid having to pay a separate royalty under the right of reproduction based on such interim copies, in addition to a public performance royalty. In addition, controversy has arisen over what royalty rates should apply to copies made in the course of limited downloads, as opposed to full downloads.

[2743] Id. at 162-63 (footnotes omitted).

[2744] Id. at 163-64.

[2745] Id. at 150.

Section 115(a) of the copyright statute provides for a compulsory license (referred to in the industry as a "mechanical license") to make copies of a nondramatic musical work as embodied in phonorecords or digital phonorecord deliveries ("DPDs"), provided that phonorecords of the musical work have been distributed to the public in the U.S. under authority of the copyright owner. Section 115(d) defines a "digital phonorecord delivery" to mean

> each individual delivery of a phonorecord by digital transmission of a sound recording which results in a specifically identifiable reproduction by or for any transmission recipient of a phonorecord of that sound recording, regardless of whether the digital transmission is also a public performance of the sound recording or any nondramatic musical work embodied therein. A digital phonorecord delivery does not result from a real-time, non-interactive subscription transmission of a sound recording where no reproduction of the sound recording or the musical work embodied therein is made from the inception of the transmission through to its receipt by the transmission recipient in order to make the sound recording audible.

The last sentence of this definition might be read to exclude streaming from the definition of DPDs, an issue which has been the subject of considerable controversy, as discussed further below.

Section 115(c)(3)(A) provides that the compulsory license includes the right to distribute "a phonorecord of a nondramatic musical work by means of a digital transmission which constitutes a digital phonorecord delivery, regardless of whether the digital transmission is also a public performance of the sound recording under section 106(6) … or of any nondramatic musical work embodied therein under section 106(4)."

As in the case of the digital performance right with respect to sound recordings, the copyright statute provides for royalty rates for the compulsory mechanical license to be set through voluntary negotiation proceedings noticed by the Copyright Office and, if such proceedings fail to reach agreements, through CARP proceedings.[2746] The copyright statute provides that, in setting the terms and rates for the compulsory license, the CARP "shall distinguish between (i) digital phonorecord deliveries where the reproduction or distribution of a phonorecord is incidental to the transmission which constitutes the digital phonorecord delivery [usually referred to as "incidental DPDs"], and (ii) digital phonorecord deliveries in general [usually referred to as "general DPDs"]."[2747] Voluntary negotiation and/or CARP proceedings are generally to be repeated in each fifth calendar year after 1997.[2748] A CARP proceeding, Docket No. 99-4 CARP DPRA, relating to DPDs was initiated and remained open for many years, but was terminated by the Copyright Office on Aug. 6, 2007 pursuant to the Royalty and Distribution Reform Act of 2004, which eliminated the CARP system and replaced it with the

[2746] 17 U.S.C. § 115(c)(3)(C) & (D).

[2747] Id. § 115(c)(3)(D).

[2748] Id. § 115(c)(3)(F).

CRB. The Copyright Office noted that subsequent proceedings regarding the rates for Section 115 must be initiated under the new CRB system.[2749]

Because Congress did not define what constitutes an incidental DPD, much controversy has arisen with respect to them:

- Whether streaming constitutes a DPD at all;
- If so, whether streaming involves incidental DPDs or general DPDs;
- Whether limited downloads should be classified as incidental DPDs or general DPDs;
- Whether the interim copies generated in the course of streaming or limited downloads constitute a fair use or instead require a mechanical license;
- Whether the interim copies produced in the course of streaming and limited downloads are subject to the compulsory mechanical license of Section 115; and
- What royalties should be paid for the copies of works generated in the course of streaming and limited downloads.

The foregoing issues came to the fore with the rise of online music distribution systems, both "free" services such as Napster, Music City, Grokster, and Kazaa, as well as the various nascent subscription online music services such as Pressplay, MusicNet, Listen.com, and MP3.com. The issues have been fought in a variety of forums, as described in the next subsections.

(a) Applicability of the Section 115 Compulsory License to Streaming

Only one case to date has addressed the issue of whether the compulsory mechanical license of Section 115 applies to streaming. In Rodgers & Hammerstein Org'n v. UMG Recordings, Inc.,[2750] a number of songwriters and music publishers brought an action for copyright infringement against the defendants, UMG Recordings, Inc. and The Farm Club Online, Inc., for copyright infringement. The Farm Club was a subsidiary of UMG that streamed recordings over the Internet. The plaintiffs alleged that such streaming was being conducted without proper licenses under the musical composition copyrights held by the plaintiffs. The defendants claimed that, if a mechanical license were required at all for streaming, they were entitled to the compulsory license under Section 115.[2751]

[2749] 72 Fed. Reg. 45071, 45072 (Aug. 10, 2007).

[2750] 60 U.S.P.Q.2d 1354 (S.D.N.Y. 2001).

[2751] Id. at 1355-57.

The court ruled that the Section 115 compulsory mechanical license did not permit the defendants to stream the copyrighted works at issue over the Internet.[2752] The court pointed to Section 115(a)(1), which provides that a "person may obtain a compulsory license only if his or her primary purpose in making phonorecords is to distribute them to the public for private use." The court noted that the defendants did not fall within this language because they did not sell copies of records to their users, but rather merely placed copies of recordings on their servers to allow users to listen to songs on those records via streaming.[2753] Nor did the copies stored by the defendants on their servers trigger applicability of the compulsory mechanical license:

> Thus the Defendants' server copies of the copyrighted works are not analogous to master recordings made in the course of the process of making phonorecords to be distributed to the public. Defendants concede that their server copies themselves are not for distribution to the public. Since Defendants' server copies are neither intended for distribution to the public nor part of a process for distributing digital copies of the existing phonorecords, Section 115 would not give the Defendants a right to a compulsory license for the server copies.[2754]

Accordingly, the court denied the defendants' motion for summary judgment that they were licensed to stream the works.[2755]

The court also granted the plaintiffs' cross motion for partial summary judgment. The court stated:

> While Defendants have been less than candid with the Court, it is clear that what Defendants are attempting to do is to limit the payments due from them for the streaming of recordings of copyrighted works to their customers to the licensing fee that would be applicable when a radio station sends a recording over the airwaves. It is obvious that Defendants do not want to pay the Plaintiffs the license fee for a record every time one of their customers listens to recording on the Internet. However, the only license that Defendants rely on here is one that is limited to the distribution of records to the public for which there is an established fee. Defendants choice is to obtain a license for that purpose and pay the fee or cease their infringing activity.[2756]

It is unclear what precisely the "infringing activity" was that the court was referring to. It does not seem to be the distribution of copies, for the court found the defendants were not distributing digital copies of phonorecords (and thus Section 115 did not apply). It therefore must have been

---

[2752] The court also held that an existing license from the Harry Fox Agency (HFA) held by the defendants did not cover the streaming because that license was limited by its terms to a specific phonorecord number, and the HFA license did not constitute a compulsory license under Section 115. Id. at 1357-59.

[2753] Id. at 1360.

[2754] Id. (citation omitted).

[2755] Id. at 1361.

[2756] Id.

the public performance of the compositions via streaming for which the defendants required a license.

(b) The Copyright Office's Position – The 2001 DMCA Report and Comment Proceedings

As discussed in Section II.G.6(a) above, Section 104 of the DMCA requires the Register of Copyrights and the Assistant Secretary for Communications and Information of the Commerce Department to study and report to Congress within two years of enactment of the DMCA with respect to the DMCA's impact on, among other things, "the relationship between existing and emergent technology" and Sections 109 and 117 of the copyright statute. The report required under Section 104 was issued in August of 2001 and is available online at www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.

The report concluded that the making of temporary copies of a work in RAM in the course of streaming implicates the reproduction right of the copyright holder so long as the reproduction persists long enough to be perceived, copied, or communicated.[2757] The report noted considerable uncertainty in the industry concerning the legal status of buffer copies and the exposure of webcasters to demands for additional royalty payments from the owners of streamed sound recordings. The report expressed the belief "that there is a strong case that the making of a buffer copy in the course of streaming is a fair use," based largely on the fact that buffer copies do not supersede or supplant the market for the original works and the effect on the actual or potential market for the works appears to minimal or nonexistent.[2758] Because the sole purpose for making the buffer copies is to permit an activity that is licensed by the copyright owner and for which the copyright owner receives a performance royalty, the report concluded that copyright owners appeared "to be seeking to be paid twice for the same activity."[2759]

Accordingly, the report recommended:

> that Congress enact legislation amending the Copyright Act to preclude any liability arising from the assertion of a copyright owner's reproduction right with respect to temporary buffer copies that are incidental to a licensed digital transmission of a public performance of a sound recording and any underlying musical work.
>
> The economic value of licensed streaming is in the public performances of the musical work and the sound recording, both of which are paid for. The buffer copies have no independent economic significance. They are made solely to enable the performance of these works. The uncertainty of the present law potentially allows those who administer the reproduction right in musical works

---

[2757] See Section III.B.2.a of the Executive Summary of the report, which may be found online at www.loc.gov/copyright/reports/studies/dmca/dmca_executive.html.

[2758] Id. Section III.B.2.b.

[2759] Id.

to prevent webcasting from taking place – to the detriment of other copyright owners, webcasters and consumers alike – or to extract an additional payment that is not justified by the economic value of the copies at issue. Congressional action is desirable to remove the uncertainty and to allow the activity that Congress sought to encourage through the adoption of the section 114 webcasting compulsory license to take place.

Although we believe that the fair use defense probably does apply to temporary buffer copies, this approach is fraught with uncertain application in the courts. This uncertainty, coupled with the apparent willingness of some copyright owners to assert claims based on the making of buffer copies, argues for statutory change.[2760]

On Mar. 9, 2001, prior to issuance of the 2001 DMCA report, and in response to a petition by the RIAA for rulemaking or to convene a CARP, the Copyright Office initiated a request for public comments on the interpretation and application of the mechanical and digital phonorecord compulsory license to certain digital music services, including webcasting.[2761] The RIAA petition focused on two types of digital music deliveries:

– "On-Demand Stream," defined as an "on-demand, real-time transmission using streaming technology such as Real Audio, which permits users to listen to the music they want when they want and as it is transmitted to them"; and

– "Limited Download," defined as an "on-demand transmission of a time-limited or other use-limited (i.e. non-permanent) download to a local storage device (e.g. the hard drive of the user's computer), using technology that causes the downloaded file to be available for listening only either during a limited time (e.g. a time certain or a time tied to ongoing subscription payments) or for a limited number of times."[2762]

[2760] Id. Section III.B.2.c. The report also acknowledged a "symmetrical difficulty" faced in the online music industry relating to digital performances that are incidental to digital music downloads:

"Just as webcasters appear to be facing demands for royalty payments for incidental exercise of the reproduction right in the course of licensed public performances, it appears that companies that sell licensed digital downloads of music are facing demands for public performance royalties for a technical 'performance' of the underlying musical work that allegedly occurs in the course of transmitting it from the vendor's server to the consumer's computer.

Although we recognize that it is an unsettled point of law that is subject to debate, we do not endorse the proposition that a digital download constitutes a public performance even when no contemporaneous performance takes place. If a court were to find that such a download can be considered a public performance within the language of the Copyright Act, we believe that the arguments concerning fair use and the making of buffer copies are applicable to this performance issue as well. It is our view that no liability should result from a technical 'performance' that takes place in the course of a download."Id.

[2761] 66 Fed. Reg. 14099 (Mar. 9, 2001).

[2762] Id. at 14100.

Music publishers had taken the position that both On-Demand Streams and Limited Downloads implicated their reproduction (mechanical license) rights. The RIAA requested the Copyright Office to determine whether On-Demand Streams are incidental DPDs and, if so, to convene a CARP to set rates for those incidental DPDs. With respect to Limited Downloads, the RIAA suggested that they may be either incidental DPDs or more in the nature of record rentals, leases or lendings.[2763] In either case, the RIAA believed that the compulsory license of Section 115 should apply, but asked the Copyright Office to conduct a rulemaking proceeding with respect to the issues:

> In sum, RIAA asserts that it is unclear whether the section 115 license permits all of the activities necessary to make On-Demand Streams or Limited Downloads, and if so, at what royalty rates. Consequently, RIAA petitions the Office to determine (1) whether On-Demand Streams are incidental DPDs covered by the license; (2) whether the license includes the right to make server copies or other copies necessary to transmit On-Demand Streams and Limited Downloads; and (3) the royalty rate applicable to On-Demand Streams (if they are covered by the license) and Limited Downloads.[2764]

The Copyright Office sought public comment on these issues and other related issues, including the following:

– "Is it possible to define 'incidental DPD' through a rulemaking proceeding?"[2765]

– "Are some or all the copies of a musical work made that are necessary to stream that work incidental DPDs?"[2766]

– "Aren't incidental DPDs subject to section 115's definition of digital phonorecord deliveries? If so, does the requirement that a DPD result in a 'specifically identifiable reproduction' by or for a transmission recipient rule out some of the copies discussed above from consideration as incidental or general DPDs?"[2767]

(c) The NMPA/HFA/RIAA Agreement of 2001

While the public comment proceedings were ongoing, the RIAA and music publishers, acting through the National Music Publishers Association (NMPA) and the Harry Fox Agency (HFA), announced on Oct. 9, 2001 a breakthrough agreement on the licensing of musical works for new subscription services over the Internet. According to a joint statement filed by NMPA, HFA and RIAA with the Copyright Office on Dec. 6, 2001, the agreement applies to subscription digital music services that include among their offerings "On-Demand Streams" (defined as "an

---

[2763] Id.

[2764] Id. at 14100-101.

[2765] Id. at 14101.

[2766] Id.

[2767] Id. at 14102.

on-demand, real-time transmission of a song to a consumer who requests that song using streaming technology") and/or "Limited Downloads" (defined as "a download that can be played for a limited period of time or a limited number of plays").[2768]

Under the agreement, the parties agreed that a mechanical license under Section 115 for On-Demand Streams and Limited Downloads is available (contrary to the holding of the Rodgers and Hammerstein case discussed in Section III.E.4(a) above) through HFA to all RIAA member companies and to any digital music service that is majority owned by one or more RIAA members. The rights under any such license can be extended to any service authorized by a licensee to make On-Demand Streams and/or Limited Downloads of a licensed musical work. In addition, NMPA and HFA publicly announced that it is their policy to license not only RIAA members but also other digital music services that wish to negotiate comparable agreements.[2769]

The agreement provides that a mechanical license obtained under it includes all reproduction and distribution rights for delivery of On-Demand Streams and Limited Downloads. The agreement confirms that a mechanical license for these services includes the right to make server copies, buffer copies and other related copies used in the operation of the services. The license does not include performance rights, which are licensable separately through performing rights organizations such as ASCAP, BMI and SESAC.[2770] The agreement does not establish specific royalty rates. The parties to the agreement committed to negotiate those rates pursuant to the procedures of Sections 115(c)(3)(B),(C), and (F) of the copyright statute (described in the opening paragraphs to Section III.E.4 above). If negotiations are not successful, the applicable rates are to be determined through CARP proceedings.[2771]

Finally, under the agreement the parties agreed to the following legal points: (1) that the process of making On-Demand Streams and Limited Downloads, from the making of server copies to the transmission and local storage of the stream or download, viewed in its entirety, involves the making and distribution of a DPD; (2) that a compulsory license is available under Section 115 for On-Demand Streams and Limited Downloads; and (3) radio-style and other non-interactive webcasting that would qualify for a statutory license under Section 114(d)(2) does not involve the making or distribution of a DPD and thus does not require a mechanical license.[2772]

On Dec. 14, 2001, the Copyright Office sought public comments on the effect of the RIAA/NMPA/HFA agreement on the issues identified in its public comment proceedings

---

[2768] Joint Statement of The Recording Industry Association of America, Inc., National Music Publishers' Association, Inc. and The Harry Fox Agency, Inc., *In re Matter of Mechanical and Digital Phonorecord Delivery Compulsory License*, Docket No. RM 2000-7 (Dec. 6, 2001), at 3 (available as of Feb. 9, 2002 at www.loc.gov/copyright/carp/10-5agreement.pdf).

[2769] Id. at 3-4.

[2770] Id. at 4.

[2771] Id. at 5.

[2772] Id. at 6.

initiated on Mar. 9, 2001.[2773] The period for comment on the RIAA/NMPA/HFA agreement was extended to Feb. 6, 2002, with reply comments due on Feb. 27, 2002.[2774]

On June 22, 2004, the Copyright Office amended its regulations governing the content and service of notices on the copyright owner required to take advantage of the compulsory license of Section 115. The purpose of the amended regulations was to simplify the notice process for digital music services wishing to take advantage of the compulsory license for a broad spectrum of musical works embodied in sound recordings.[2775]

(d) The Interactive Streaming and Limited Download Agreement of 2008

On Jan. 7, 2008, DiMA requested pursuant to Section 802(f)(1)(B) that the CRB refer to the Register of Copyrights the question of whether interactive streaming constituted a DPD. Copyright Owners objected to the request, and after holding oral arguments on the question, the CRB denied the request, stating that the question of what is "interactive streaming" is a question of fact, not a question of law as required by Section 802(f)(1)(B).[2776]

On September 22, 2008, a royalty agreement was announced between DiMA, the RIAA, the national Music Publishers' Association (NMPA), the Nashville Songwriters Association International (NSAI), and the Songwriters Guild of America (SGA). The agreement proposed mechanical royalty rates for interactive streaming and limited downloads, inclusive of subscription and ad-supported services, and generally called for rates of 10.5% of revenue, minus amounts owed for performance royalties. The parties also confirmed that reproduction or distribution licenses are not required from copyright owners for non-interactive, audio-only streaming services.[2777] The agreement was published on Oct. 1 with a request for comments.[2778] After releasing its Initial Determination on Oct. 2, the CRB issued its Final Determination of Rates and Terms in the Matter of Mechanical and Digital Phonorecord Delivery Rate Determination Proceeding on Nov. 24, and published it on Jan. 26, 2009.[2779]

On Jan. 8, 2009 the Register solicited comments from the participants regarding potential legal errors in the CRB's Final Determination, and received responses from the RIAA, Copyright Owners, and DiMA. Concurrent with the publication of the Final Determination on Jan. 26, the

---

[2773] 66 Fed. Reg. 64783 (Dec. 14, 2001).

[2774] 67 Fed. Reg. 4694 (Jan. 31, 2002).

[2775] 69 Fed. Reg. 34578 (June 22, 2004).

[2776] See 74 Fed. Reg. 4537, 4538 (Jan. 26, 2009).

[2777] Brendan Pierson, "Music Groups Strike Deal on Internet Royalties" (Sept. 24, 2008), available as of Aug. 1, 2012 at http://www.law360.com/ip/articles/70323; DiMA, "Major Music Industry Groups Announce Breakthrough Agreement" (Sept. 23, 2008), available as of Aug. 1, 2012 at http://www.digmedia.org/component/content/article/40-press-releases/128-press-releases-9-23-08.

[2778] 73 Fed. Reg. 57033 (Oct. 1, 2008).

[2779] 74 Fed. Reg. 4510 (Jan. 26, 2009).

Register issued a decision ruling that some elements of the Final Determination were in error, and rejecting the CRB's earlier conclusion that it lacked authority to review the legality of the terms of the agreements.[2780] In particular, the Register identified four erroneous provisions: (1) the definition of "interactive stream" was erroneous because it altered the provisions of the Section 115 license regarding what constitutes a DPD; (2) the promotional royalty rate for interactive streams and limited downloads constituted retroactive rulemaking; (3) the timing of royalty payments provision violated 17 U.S.C. § 115(c)(5); and (4) the Register cannot prescribe regulations on statements of account, as directed in the Final Determination.[2781] In response, the CRB deleted from the Final Determination the four provisions that the Register identified, but did not add any new provisions to correct the errors.[2782] In doing so, the CRB noted that although the Register's decision is binding as precedent only on subsequent proceedings, the CRB chose to exercise its ability to modify the terms (but not the rates) of an agreement, so as to avoid potential confusion for users of the license at issue.[2783]

(e) 2008 Interim Regulation re Compulsory DPD License

Following a notice of proposed rulemaking, the Copyright Office announced on Nov. 7, 2008 an interim regulation concerning the Section 115 mechanical license for making and distributing DPDs. Initially, the proposed rule defined a DPD as including all buffer copies made in the course of streaming, meaning that all music streaming would therefore have been included in the scope of the mechanical license. However, in light of comments and testimony, as well as uncertainties created by the Cartoon Network LP v. CSC Holdings, Inc.[2784] decision, the resulting Interim Regulation backtracked. The Interim Regulation "takes no position on whether or when a buffer copy independently qualifies as a DPD, or whether or when it is necessary to obtain a license to cover the reproduction or distribution of a musical work in order to engage in activieties such as streaming."[2785] Instead, the Interim Regulation simply clarifies that "(1) whenever there is a transmission that results in a DPD, all reproductions made for the purpose of making the DPD are also included as part of the DPD, and (2) limited downloads qualify as DPDs."[2786] As explained below, the Interim Regulation also does not define the duration threshold at which a DPD occurs for the purposes of "fixation."[2787]

The issue of fixation vexed the Copyright Office because Cartoon Network indicated that if a reproduction was not fixed for a sufficient duration then it did not qualify as an infringement of the right of reproduction. However, Cartoon Network provided no clear answers as to the

---

[2780] 74 Fed. Reg. 4537 (Jan. 26, 2009).

[2781] Id.

[2782] 74 Fed. Reg. 6832 (Feb. 11, 2009).

[2783] Id. at 6833.

[2784] 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 2009 U.S. LEXIS 4828 (2009).

[2785] 73 Fed. Reg. 66173, 66174 (Nov. 7, 2008).

[2786] Id.

[2787] Id.

minimum duration that still constituted fixation. After considering Cartoon Network's determination that a buffer that held a work for not more than 1.2 seconds is not "fixed," and contrasting it with the ruling in MAI Sys. Corp. v. Peak Computer, Inc.,[2788] which held that a duration of several minutes was sufficiently fixed, the interim regulation concluded that Cartoon Network did not provide guidance as to the minimum duration sufficient for fixation.

Because of this uncertainty, the interim regulation declined to address whether streaming music that invovlves making buffer copies (but makes no other copies) is included in the Section 115 mechanical license.[2789] Nonetheless, the Interim Regulation did respond to Cartoon Network by altering 37 CFR 201.18 to include the requirement that a DPD be "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."[2790] Although the Regulation noted that some, if not many, such buffer copies constitute DPDs, it left it to the marketplace to decide the issue, noting that most licenses that are made pursuant to Section 115 are not actually mechanical licenses, but rather are voluntary licenses that mirror the rates for mechanical licenses. Providing some clarification, however, the Interim Regulation did state that cached copies on users' hard drives that are created by streaming services do satisfy the fixation/reproduction requirement and thereby qualify as DPDs.[2791] It further resolved a disagreement over who must be able to perceive a copy in order for it to be "specifically identifiable" and therefore qualify under one of the requirements for DPDs, stating that copies that are identifiable by *any* human or computer are thereby "specifically identifiable."[2792]

The Interim Regulation declined to comment on what differentiates an "incidental DPD" from an ordinary DPD, noting that the distinction is not often important because both are included under the Section 115 license, and stating that if a differentiation was ever required in a particular case, it could be made in the context of a factual analysis before the CRB. The Interim Regulation did, however, state that limited downloads qualify as DPDs, citing the fact that they are delivered, they are phonorecords, and they are specifically identifiable.[2793] According to the interim regulation, any copy of a phonorecord made in the process of making and distributing a DPD is covered unter the Section 115 license, even if the copy is not delivered to the recipient. However, "server and intermediate copies that are the source of a transmission that does not result in the making and distribution of a DPD would not fall within the scope of the [Section 115 mechanical] license."[2794]

[2788] 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

[2789] Id. at 66177.

[2790] Id. at 66181.

[2791] Id.

[2792] Id. at 66178.

[2793] Id. at 66178-79.

[2794] Id. at 66180.

(f) Applicability of the Section 115 Compulsory License to Ringtones

In October of 2006, in response to a request by the Copyright Royalty Board for a ruling, the Copyright Office issued a memorandum opinion concluding that ringtones qualify as DPDs eligible for the statutory license of Section 115. Specifically, the Copyright Office ruled as follows:

> We find that ringtones (including monophonic and polyphonic ringtones, as well as mastertones) are phonorecords and the delivery of such by wire or wireless technology meets the definition of DPD set forth in the Copyright Act. However, there are a variety of different types of ringtones ranging from those that are simple excerpts taken from a larger musical work to ones that include additional material and may be considered original musical works in and of themselves. Ringtones that are merely excerpts of a preexisting sound recording fall squarely within the scope of the statutory license, whereas those that contain additional material may actually be considered original derivative works and therefore outside the scope of the Section 115 license. Moreover, we decide that a ringtone is made and distributed for private use even though some consumers may purchase them for the purpose of identifying themselves in public. We also conclude that if a newly created ringtone is considered a derivative work, and the work has been first distributed with the authorization of the copyright owner, then any person may use the statutory license to make and distribute the musical work in the ringtone.[2795]

In Recording Industry Ass'n of America, Inc. v. Librarian of Congress,[2796] the D.C. Circuit held that the Copyright Royalty Board's imposition under the Section 115 compulsory license of a 1.5% per month late fee and a 24 cent royalty for every ring tone sold using copyrighted work were fair measures to compensate copyright owners when their work is copied absent a negotiated license agreement and were therefore not arbitrary and capricious.

5. The Section 111 Compulsory License for Cable Systems

Section 111 of the Copyright Act makes available a statutory license permitting cable systems to publicly perform and retransmit signals of copyrighted television programming to its subscribers, provided they pay royalties at government-regulated rates and abide by the statute's procedures. However, the Section 111 statutory license has been ruled not applicable to retransmission of broadcast programming via Internet streaming.

[2795] 71 Fed. Reg. 64303, 64304 (Nov. 1, 2006).

[2796] 608 F.3d 861 (D.C. Cir. 2010).

(a) WPIX v. ivi

In WPIX, Inc. v. ivi, Inc.[2797] the defendant ivi captured and retransmitted the plaintiff WPIX's copyrighted television programming live and over the Internet to paying ivi subscribers who had downloaded ivi's "TV player" on their computers for a monthly subscription of $4.99. For an additional $0.99 per month, subscribers were able to record, pause, fast-forward, and rewind ivi's streams. In response to a lawsuit for copyright infringement, ivi claimed that it was a cable system entitled to the compulsory license under Section 111. A district court in New York rejected that argument and issued a preliminary injunction against ivi. On appeal, the Second Circuit affirmed, concluding (in accordance with the Copyright Office) that the compulsory license of Section 111 applies only to localized retransmission services regulated as cable systems by the FCC, and that Internet retransmission services are not cable systems and accordingly do not qualify for that license.[2798]

6. International Licensing Efforts

In November of 2003, the International Federation of the Phonographic Industry (IFPI), a global trade body representing major and independent music labels, announced a "one-stop" international license for webcasters. IFPI expected collection agencies in 30 to 40 countries to sign up to the single license agreement by the end of 2003. Webcasters would pay a national body a fee for songs broadcast into each individual country. The agreement would be for radio-style broadcasts only. Internet companies would still need to secure individual licensing agreements to sell permanent song downloads.[2799]

F. First Sales in Electronic Commerce

The "first sale doctrine" of copyright law is codified in Section 109 of the copyright statute. That section provides, "Notwithstanding the provisions of section 106(3) [the exclusive distribution right], the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord."[2800] The applicability of the first sale doctrine to "sales" through online commerce is uncertain.

Section 109 pertains to the sale or disposal of "the possession of [a] copy or phonorecord." The statute was, of course, originally drafted with tangible copies in mind. An immediate issue concerns whether an initial "sale" accomplished by an online *transmission*, rather than the physical distribution of a material object, constitutes a sale of a "copy" that would trigger the application of the doctrine at all. At least one commentator has argued that it does

---

[2797] 2012 U.S. App. LEXIS 18155 (2d Cir. Aug. 27, 2012).

[2798] Id. at *4, 18-23.

[2799] "Music Industry Trumpets Global Webcast License" (Nov. 11, 2003), available as of Nov. 11, 2003 at http://uk.news.yahoo.com/031111/80/edmp0.html.

[2800] 17 U.S.C. § 109(a).

not,[2801] and the NII White Paper notes that the issue is uncertain.[2802] However, it seems plausible to analogize a transmission in which a complete authorized copy of a work ends up in permanent storage at the recipient's site (i.e., other than a transitory copy in RAM) as the distribution of a "copy" for purposes of the first sale doctrine, at least where it was intended that the recipient "own" the received copy.[2803] Such a transaction seems highly analogous to a traditional sale of a copy, except for the distribution vehicle.

One could readily argue that in such instances the first sale doctrine should apply by analogy to permit a purchaser to further transmit his or her copy to a third party, so long as the purchaser deletes his or her original copy from storage, because in that instance, as in the case of traditional distributions of physical copies, no more total "copies" end up in circulation than were originally sold by or under authority of the copyright owner. As one commentator has noted:

> [The first sale doctrine's] balance was gauged over the years …. Neither the copyright owner nor the copy owner receives all that it might desire. The balance could be recut today for cyberspace, but no clear reasons exist to do so. Absent that, this balance governs treatment of digital works, whether on the Internet or a diskette. Applying it is relatively simple. A purchaser who acquires a digital product that is not subject to a license has a right to retransfer the copy, make copies essential to use the work, and otherwise act as owner of the copy. If the "copy" is transferred, the transferor must relinquish all copies it possesses. Otherwise, it would in effect be making multiple copies inconsistent with the balance between copy and copyright owners.[2804]

Although this argument makes sense in many instances, such as where a buyer has purchased a copy of a book that is delivered electronically, in other instances the policy choices with respect to whether the first sale doctrine should be applied by analogy seem less clear. One such example comprises works that are made available for on-demand usage, such as movies. The copyright owner clearly intends to make such works available only for one time use by the recipient, and any further retransmission or distribution of the work to third parties would cut into the owner's on-demand market for the work. Yet depending upon the transmission technology used, a "copy" of the work may be made in whole or in part at the recipient's end. Indeed, under the MAI case, even the data stored in RAM at the recipient's computer would constitute a "copy." It seems less clear that such "copy" should trigger the first sale doctrine and permit the recipient to further distribute that "copy," even if the recipient does not retain a copy.

[2801] K. Stuckey, Internet and Online Law § 6.08[3][b], at 6-54 (2008).

[2802] NII White Paper at 43-44.

[2803] In the case of computer programs, copyright owners often distribute copies of the program subject to a license agreement which states that the copy is being licensed, not sold, to the user as a vehicle to avoid the applicability of the first sale doctrine to the transaction.

[2804] R. Nimmer, Information Law ¶ 4.08[2][b], at 4-32 to 4-33 (2001).

As currently codified in Section 109, the first sale doctrine is drafted as an exception to the *distribution* right of the copyright holder. However, as discussed earlier, the new rights of transmission and access under the WIPO treaties are seemingly broader than the current distribution right under United States law. An issue therefore arises as to whether the first sale doctrine should prevail over these new rights of transmission and access, in addition to the right of distribution. Both WIPO treaties contain provisions stating that nothing in them shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of rights afforded by the treaties will apply after the first sale or other transfer of ownership of the original or a copy of a work with the authorization of the owner.[2805] The WIPO treaties thus seem to contemplate that the interplay between the doctrine of first sale and the new rights of transmission and access will ultimately be resolved through implementing legislation.

Although the implementing legislation in the United States afforded Congress the opportunity to resolve the ambiguities in the scope of the first sale doctrine as applied to the Internet, the DMCA does not address the issue. One of the proposed bills to implement the WIPO treaties, H.R. 3048, would have added the following new subsection (f) to Section 109 of the copyright statute with respect to applicability of the first sale doctrine to works in digital format:

> (f) The authorization for use set forth in subsection (a) applies where the owner of a particular copy or phonorecord in a digital format lawfully made under this title, or any person authorized by such owner, performs, displays or distributes the work by means of transmission to a single recipient, if that person erases or destroys his or her copy or phonorecord at substantially the same time. The reproduction of the work, to the extent necessary for such performance, display, distribution, is not an infringement.

This provision seems to have been drafted to apply to the paradigm situation, discussed above, in which the original sale of a work via transmission in digital format results in a complete copy of the work residing in permanent storage at the purchaser's site. So long as the original purchaser erases his or her copy at substantially the same time, new subsection (f) permits the purchaser to transmit that copy to a third party without liability (including any reproductions, displays or performances that are attendant thereto).

The applicability of this provision to the case of on-demand transmissions for simultaneous viewing or other usage by the original purchaser (such as movies or online games) is not clear. In those instances, as discussed above, it is unclear whether the purchaser should be treated as the "owner of a particular copy or phonorecord in a digital format" by virtue of the initial on-demand download of the work in order to trigger application of the new subsection (f). In any event, this provision was not adopted in the DMCA.

The European Copyright Directive appears to take the position that obtaining a copy of a copyrighted work through an online service does not exhaust the copyright owner's rights in a

---

[2805] See Article 6(2) of the WIPO Copyright Treaty and Articles 8(2) and 12(2) of the WIPO Performances and Phonograms Treaty.

way that would allow resale or retransmission of such copy. Specifically, paragraph 29 of the recitals to the Directive states the following:

> "The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorization where the copyright or related right so provides."

G. Pop-Up Advertising

1. The Gator Litigations

In June of 2002, a number of publishing companies and other entities operating their own web sites sued Gator Corporation for copyright infringement, trademark infringement, unfair competition and other causes of action based on Gator's causing unauthorized pop-up advertising to appear on the sites of the plaintiffs. Gator widely distributed a software application called "Gator" that acted as a digital wallet to provide users with a mechanism for storing personal information about themselves, passwords, user identification numbers and names and other data that consumers routinely need to input on electronic forms when shopping on the Internet. Gator bundled with the digital wallet software another program called "OfferCompanion," which, once installed, would automatically launch whenever a user initiated a browser-based Internet connection, observe the sites visited by the user, and whenever the user visited certain websites, display one or more unauthorized pop-up advertisements directly over such websites, obscuring a portion of the content of the website.[2806]

Gator sold its pop-up advertising services to various clients, who in many instances would engage the Gator service to cause the clients' pop-up ads to appear when users visited competitor's sites. For example, a Gator pop-up advertisement for hotjobs.com would appear on the home page of the plaintiff Dow Jones' CareerJournal.com web site, a classified recruitment advertising site that competed with hotjobs.com.[2807] The plaintiffs sought a preliminary injunction against Gator on the grounds, among others, that the unauthorized display of Gator ads on the plaintiffs' sites infringed the plaintiffs' exclusive right of distribution under copyright law and constituted the making of unauthorized derivative works.

With respect to the distribution right, the plaintiffs argued that each of their web sites were governed by a "terms and conditions of use" that granted site visitors a license to use and

---

[2806] Memorandum in Support of Plaintiffs' Motion for Preliminary Injunction, Washingtonpost.Newsweek Interactive Co. v. The Gator Corporation, Civil Action 02-909-A (E.D. Va. June 25, 2002), at 8-10 (copy on file with the author).

[2807] Id. at 10.

display the copyrighted content of the site but not to alter the site or change its appearance. Because Gator's pop-up advertising altered the appearance of the plaintiffs' web sites by covering a portion of the content of the web page on which the ads appeared, the ads caused the site visitors to generate an infringing altered display of the web sites, and Gator was secondarily liable for contributing to such infringing displays.[2808] The plaintiffs further argued that the altered displays constituted the creation of unauthorized derivative works for which Gator was directly liable.[2809]

On July 16, 2002, the district court entered a preliminary injunction, without written opinion, enjoining Gator from causing its pop-up advertisements to be displayed on any web site owned by or affiliated with the plaintiffs without their express consent, and from altering or modifying, or causing any other entity to alter or modify, any part of such websites or the display thereof.[2810] In February of 2003, Gator reached a settlement with 16 publishers, the terms of which were confidential.[2811]

A number of other lawsuits against Gator were filed. During 2002, Six Continents Hotels Inc. and Inter-Continental Hotels Corp. sued Gator in Atlanta for copyright and trademark infringement, unfair competition, and computer trespass, and Extended Stay America Inc. (ESA) sued Gator in South Carolina on similar grounds. Gator, in turn, sued ESA for declaratory relief in federal court in San Jose, California.[2812] In May 2003, LendingTree Inc. sued Gator for copyright and trademark infringement, asking for statutory damages of $150,000 for each infringement.[2813] As of the writing of this paper, these suits were pending.

2. The WhenU Litigations

Several lawsuits have been brought against WhenU.com, distributor of a pop-up ad program called "SaveNow," alleging copyright and trademark infringement. Although the cases

---

[2808] Id. at 23-25.

[2809] Id. at 25-26. The plaintiffs also argued that Gator's activities constituted trademark infringement because the plaintiffs' trademarks were clearly visible beside Gator pop-up advertisements, creating an unauthorized association between the two, and because of a likelihood of confusion as to sponsorship of the ads. The plaintiffs submitted a consumer survey in which 66% of respondents stated they believed that pop-up advertisements are sponsored by or authorized by the web site in which they appear, and 45% believed that pop-up advertisements have been pre-screened and approved by the web site on which they appear. Id. at 19-21.

[2810] Order granting preliminary injunction, Washingtonpost.Newsweek Interactive Co. v. The Gator Corporation, Civil Action 02-909-A (E.D. Va. July 16, 2002) (copy on file with the author). The court also enjoined Gator from infringing the plaintiffs' trademark or service mark rights, and from making any designations of origin, descriptions, representations or suggestions that the plaintiffs were the source, sponsor or in any way affiliated with Gator's advertisers or their web sites, services and products.

[2811] "Settlement Reportedly Reached in Dispute Over Pop-Up Advertisements," *Mealey's Litigation Report: Intellectual Property* (Feb. 17, 2003), at 22.

[2812] Lisa Shuchman, "Search and Destroy" (Jan. 16, 2003), available as of Jan. 18, 2003 at www.law.com/jsp/article.jsp?id=1039054570236.

[2813] Jen Zoghby, "LendingTree Suit Pops Pop-Ups" (May 19, 2003), available as of Oct. 26, 2003 at http://famulus.msnbc.com/famuluscom/bizjournal05-19-010109.asp.

reached similar results on the copyright claims, they reached different results on the trademark claims.

(a) U-Haul v. WhenU.com

In U-Haul Int'l Inc. v. WhenU.com, Inc.,[2814] U-Haul alleged that WhenU's SaveNow pop-up ad program constituted copyright and trademark infringement and unfair competition. SaveNow was generally bundled for distribution with other software programs, such as screensaver programs. It was distributed with a clickwrap license agreement. Utilizing a directory of commonly used search phrases, commonly visited web addresses, and various keyword algorithms, the SaveNow program scanned the user's Internet activity to determine whether any of the terms, web addresses, or content matched the information in its directory. Upon detecting a match, the program identified an associated product or service category, and then caused a pop-up advertisement to be selected from WhenU's clients which matched the category of the user's activity. The ads appeared in a separate "WhenU window" on top of all other windows visible on the computer's screen, including the window of the user's selected destination web site.[2815]

The court rejected U-Haul's arguments that SaveNow infringed its exclusive rights of display and derivative works. With respect to the display right, U-Haul argued that SaveNow unlawfully caused its web site to be displayed together with WhenU's pop-up ads. The court rejected this argument, noting that the user, not SaveNow, was the one who called up the U-Haul website. The SaveNow program did not alter U-Haul's web page in any manner, and the SaveNow window in which the ad appeared bore no physical relationship to the window in which the U-Haul web page appeared.[2816]

With respect to the derivative works right, U-Haul argued that the SaveNow program created an infringing derivative work by retrieving the U-Haul web page, placing its own advertisement on that Web page, then displaying it to the user. The court ruled that no derivative work of the U-Haul web page was created. First, the WhenU window was a "distinct occurrence" from the U-Haul web page, rather than a single integrated work, and the appearance of a WhenU ad on the user's computer screen at the same time as a U-Haul web page was "a transitory occurrence that may not be exactly duplicated in that or another user's computer."[2817] Second, although the pop-up ad altered the user's computer display, the alteration was not infringing. "To conclude otherwise is untenable in light of the fact that the user is the one who controls how items are displayed on the computer, and computer users would infringe copyrighted works any time they opened a window in front of a copyrighted Web page that is simultaneously open in a separate window on their computer screens."[2818]

[2814] 2003 WL 22071556 (E.D. Va. 2003).

[2815] Id. at *2.

[2816] Id. at *6.

[2817] Id. at *7.

[2818] Id.

Accordingly, WhenU was entitled to summary judgment on U-Haul's claim of copyright infringement.[2819] The court also rejected U-Haul's trademark claim on the ground, among others, that the appearance of WhenU's ads on a user's computer screen at the same time as the U-Haul web page was a result of how applications operate in the Windows environment and therefore did not constitute a "use" of U-Haul's trademarks under the Lanham Act. Neither did inclusion of the U-Haul URL or the word "U-Haul" in the SaveNow program constitute "use" under the Lanham Act, particularly since WhenU did not sell the U-Haul URL to its customers or cause the U-Haul URL or name to be displayed to the computer user when the ads popped up.[2820] Finally, the court found no unfair competition because the user had consented, by accepting the clickwrap license and downloading the software, to the display of the ads on his or her screen.[2821]

(b) Wells Fargo v. WhenU.com

Similar claims of copyright and trademark infringement were brought against WhenU in the case of Wells Fargo & Co. v. WhenU.com, Inc.[2822] The court denied a motion for a preliminary injunction, finding that the plaintiffs had not shown a likelihood of success on the merits of either the copyright or the trademark claims. With respect to the copyright claims, the plaintiffs argued that the SaveNow program caused infringing derivative works of their websites to be created. The court ruled that, to support a claim of direct derivative works infringement against WhenU, the plaintiffs would need to prove that WhenU incorporated the plaintiffs' websites into a new work. The court ruled that the plaintiffs could not establish such proof, because WhenU merely supplied a software product that did not access the plaintiffs' websites and therefore did not incorporate them into a new work. Accordingly, the plaintiffs' claim for copyright infringement could, at best, be a claim for contributory infringement based on an allegedly infringing derivative work created by users of the WhenU software.[2823]

The court concluded that SaveNow users did not create infringing derivative works either. Use of the SaveNow program to display ads did not alter the plaintiffs' websites, nor did the WhenU ad window have any physical relationship to the plaintiffs' websites or alter the content displayed in any other open window.[2824] Even if the presence of an overlapping window could be said to change the appearance of the underlying window on a computer screen, the court held that such alteration was not an infringement by analogy to the case of Lewis Galoob Toys v. Nintendo of Am.[2825] That case held that the "Game Genie" device, which attached to the Nintendo game console and allowed players to temporarily alter certain attributes of video

---

[2819] Id.

[2820] Id. at 4.

[2821] Id. at *1.

[2822] 293 F. Supp. 2d 734 (E.D. Mich. 2003).

[2823] Id. at 769.

[2824] Id.

[2825] 780 F. Supp. 1283 (N.D. Cal. 1991), aff'd, 964 F.2d 965 (9th Cir. 1992).

games, did not create a fixed derivative work because once the Game Genie was detached or the power turned off, the changes disappeared and the video game revered to its original form.[2826]

By analogy, the court ruled that WhenU's program only temporarily changed the way the plaintiffs' websites were viewed by users, and as soon as the ad windows were closed or minimized, the plaintiffs' websites reverted to their original form.[2827] The court also rejected the plaintiffs' argument that an unauthorized derivative work was formed because the WhenU ads modified the pixels on the user's screen display. The court concluded that the pixels "are owned and controlled by the computer user who chooses what to display on the screen" and the plaintiffs' did not have any property or copyright interest in those pixels.[2828] The court also noted that because the pixels on a computer screen are updated every 1/70th of a second, the "alteration of pixels is therefore far too transitory an occurrence to form a basis for a copyright violation."[2829] The court therefore ruled that the WhenU advertisements did not create a work sufficiently permanent to be independently copyrightable, and therefore did not create a derivative work.[2830]

With respect to the plaintiffs' trademark claims, the court rejected three arguments made by the plaintiffs as to why WhenU should be found to "use" the plaintiffs' trademarks in commerce, as required to establish a violation of the Lanham Act. First, the plaintiffs argued that WhenU hindered Internet users from accessing their websites by potentially diverting them to other sites when the user entered the URL of their websites, and such diversion constituted a "use" of their trademarks. The court rejected this argument, noting that WhenU used the plaintiffs' trademarks only in its software directory, to which the typical consumer did not have access, and entry of the plaintiffs' URLs in fact directed them to the plaintiffs' web sites.[2831]

Second, the plaintiffs argued that WhenU positioned its pop-up ads in such a way that consumers would see one display containing WhenU's ads and the plaintiffs' websites and trademarks. This positioning, the plaintiffs argued, created the impression that the pop-up was affiliated with or approved by the plaintiffs. The court rejected this argument, finding that it was apparent to the user that what was appearing on his or her screen was two distinct sources of material. The court noted that the plaintiffs' marks were neither displayed nor appeared to be displayed on WhenU's windows, and the fact that WhenU's ads appeared on a computer screen at the same time the plaintiffs' web pages were visible in a separate window was not a "use" in

---

[2826] Id. at 1288, 1291.

[2827] Wells Fargo, 293 F. Supp. 2d at 770.

[2828] Id. at 770-71.

[2829] Id. at 771.

[2830] Id.

[2831] Id. at 758-59.

commerce of the plaintiffs' marks.[2832] Instead, the court concluded it was a form of legitimate comparative advertising.[2833]

Finally, the plaintiffs argued that the inclusion of their trademarks in WhenU's software directory was a use in commerce. The court rejected this argument as well, finding that the directory entries were used only to identify the category of material a user was interested in, and to dispatch a contextually relevant ad to that user. The ad did not display the plaintiffs' trademarks, and WhenU did not use the plaintiffs' trademarks to indicate anything about the source of the products and services it advertised.[2834]

(c) 1-800 Contacts v. WhenU.com

A third opinion in the various litigations against WhenU was issued just one month after the Wells Fargo opinion. In the case of 1-800 Contacts, Inc. v. WhenU.com,[2835] the district court reached the same conclusion as the U-Haul and Wells Fargo courts on the copyright claims, but reached an opposite conclusion on the trademark claims, although its trademark ruling was later reversed on appeal to the Second Circuit. In this case, claims were brought against both WhenU and one of its advertising customers, Direct Vision, a competitor of the plaintiff 1-800 Contacts. In addition to the copyright and trademark claims, the plaintiff asserted a violation of the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).

With respect to its claim of copyright infringement, the plaintiff argued that, by delivering pop-up ads to a SaveNow user's computer while the user was viewing the plaintiff's website, the defendants created a new screen display that incorporated the plaintiff's copyrighted work, thereby infringing the plaintiff's exclusive right of display.[2836] The court rejected this argument, finding that it would prove way too much were it accepted:

> For this court to hold that computer users are limited in their use of Plaintiff's website to viewing the website without any obstructing windows or programs would be to subject countless computer users and software developers to liability for copyright infringement and contributory copyright infringement, since the modern computer environment in which Plaintiff's website exists allows users to obscure, cover, and change the appearance of browser windows containing

---

[2832] Id. at 759-61.

[2833] Id. at 761.

[2834] Id. at 762. The court also ruled that the plaintiffs had not demonstrated a likelihood of success on the issue of confusion. The court found a number of flaws in the survey conducted by the plaintiffs' expert, in that it did not approximate actual market conditions, did not survey the appropriate population, contained questions that were unclear and leading, and contained no control questions. Id. at 765-69. In March of 2003, plaintiffs Wells Fargo and Quicken Loans settled their lawsuit against WhenU.com and filed a stipulated order of dismissal. See "Wells Fargo Settles WhenU.com Pop-Up Ads Case," *BNA's Electronic Commerce & Law Report* (Mar. 30, 2005) at 329.

[2835] 309 F.Supp.2d 467 (S.D.N.Y. 2003).

[2836] Id. at 485.

> Plaintiff's website. Without authority or evidence for the claim that users exceed their license to view the copyrighted 1-800 Contacts website when they obscure the website with other browser windows (including pop-up ads generated by the SaveNow program), Plaintiff has little basis for its claim that Defendants have infringed its display right.[2837]

The court also rejected the plaintiff's argument that the defendants were creating unauthorized derivative works by adding to or deleting from its copyrighted website, thereby "transforming" or "recasting" the website.[2838] Similar to the holdings in the U-Haul and Wells Fargo cases, the court found that no derivative work satisfying the fixation requirement was created by the SaveNow program, in view of the fact that the pop-up ads could be moved, obscured, or closed entirely, thus disappearing from perception, with the single click of a mouse.[2839] In addition, to the extent the pop-up ads constituted "transmitted images," they were not fixed works since there was no evidence that a fixation was made "simultaneously with" the pop-up ads' "transmission," as required by the definitions in section 101 of the copyright statute.[2840] Finally, the court ruled that the defendants had not recast or transformed the plaintiff's website because its website remained intact on the computer screen. Although the defendants' pop-up ads might obscure or cover a portion of the website, they did not change it.[2841]

> Moreover, if obscuring a browser window containing a copyrighted website with another computer window produced a "derivative work," then any action by a computer user that produced a computer window or visual graphic that altered the screen appearance of Plaintiff's website, however slight, would require Plaintiff's permission. A definition of "derivative work" that sweeps within the scope of the copyright law a multi-tasking Internet shopper whose word-processing program obscures the screen display of Plaintiff's website is indeed "jarring," and not supported by the definition set forth at 17 U.S.C. § 101.[2842]

The district court, however, reached an opposite conclusion to the U-Haul and Wells Fargo courts on the issue of trademark infringement, expressly noting that it disagreed with those courts.[2843] Unlike those courts, the 1-800 Contacts court found that the defendants were making "use" of the plaintiff's trademarks in commerce for several reasons. First, SaveNow users that typed in the plaintiff's web site address or its 1-800 CONTACTS trademark in a search were exhibiting a prior knowledge of the plaintiff's website or goods and services, and the court found that pop-up ads that capitalized on that knowledge were "using" the plaintiff's marks that

---

[2837] Id.

[2838] Id. at 486.

[2839] Id. at 487.

[2840] Id.

[2841] Id.

[2842] Id. at 487-88.

[2843] Id. at 490 n.43.

appeared on its website.[2844] Second, the court found that by including the plaintiff's URL, www.1800contacts.com, in its software directory of terms that triggered pop-up ads, WhenU was "using" a version of the plaintiff's 1-800 CONTACTS mark.[2845] Thus, the court concluded that, by delivering ads to a SaveNow user when the user directly accessed the plaintiff's website, the SaveNow program allowed the defendant Vision Direct, to profit from the goodwill and reputation in the plaintiff's website that led the user to access the plaintiff's website in the first place.[2846]

With respect to the issue of confusion, although the court found the survey of the plaintiff's expert, which was the same expert as the Wells Fargo case, to be flawed for many of the same reasons the Wells Fargo court noted, the court nevertheless held that the plaintiff had established a sufficient showing of likelihood of harm from both "initial interest confusion" and "source confusion" to support a Lanham Act claim.[2847] The court also ruled that, by registering the domain name www.www1800Contacts.com, the defendant Vision Direct had violated the Anticybersquatting Consumer Protection Act.[2848]

Accordingly, based on the trademark and anticybersquatting claims, the court entered a preliminary injunction against the defendants, enjoining them from (1) including the 1-800 CONTACTS mark, and confusingly similar terms, as elements in the SaveNow software directory, and (2) displaying the plaintiff's mark in the advertising of Vision Direct's services, by causing "Vision Direct's pop-up advertisements to appear when a computer user has made a specific choice to access or find Plaintiff's website by typing Plaintiff's mark into the URL bar of a web browser or into an Internet search engine."[2849]

On interlocutory appeal of the preliminary injunction, the Second Circuit reversed, ruling that as a matter of law WhenU did not "use" the plaintiff's marks within the meaning of the Lanham Act when it included the plaintiff's URL in its software directory or when it caused separate, branded pop-up ads to appear either above, below, or along the bottom edge of the plaintiff's website window.[2850] With respect to inclusion of the URL in WhenU's directory, the Second Circuit ruled that the URL transformed the plaintiff's trademark into a word combination that functioned more or less like a public key to the plaintiff's website. The only place WhenU reproduced the address was in its directory, which was not accessible to users and could therefore not create a possibility of visual confusion with the plaintiff's mark. In addition, a WhenU pop-up ad could not be triggered by a computer user's input of the 1-800 trademark or the appearance of that trademark on a web page accessed by the user. Accordingly, the court

---

[2844] Id. at 489.

[2845] Id.

[2846] Id. at 490.

[2847] Id. at 490-505.

[2848] Id. at 505-07.

[2849] Id. at 510.

[2850] 1-800 Contacts, Inc. v. Whenu.com, Inc., 414 F.3d 400, 403 (2d Cir.), cert. denied, 126 S. Ct. 749 (2005).

ruled that WhenU's inclusion of the 1-800 web address in its directory did not infringe on the plaintiff's trademark.[2851]

With respect to the pop-up ads, the court noted that they appeared in a separate window prominently branded with the WhenU mark and had no tangible effect on the appearance or functionality of the plaintiff's website. Nor was the appearance of the ads contingent upon or related to the plaintiff's trademark, the trademark's appearance on the plaintiff's website, or the mark's similarity to the plaintiff's web address. Rather, the display of the ads was the result of the happenstance that the plaintiff chose to use a mark similar to its trademark as the address to its web page. Nor did WhenU's activities divert or misdirect computer users away from the plaintiff's website. Finally, the court noted that WhenU did not sell keyword trademarks to its customers or otherwise manipulate which category-related ad would pop up in response to any particular terms on the internal directory. Accordingly, the ads did not represent a "use" in commerce of the plaintiff's trademarks.[2852]

3. The MetroGuide Litigation

In January 2003, MetroGuide.com sued Hotels.com in Florida for violations of copyright and unfair competition laws for its practice of causing pop-up ads for Hotels.com to appear over MetroGuide's web sites. The complaint alleges that the pop-up ads obscured the plaintiff439brand and content underneath them, enticing customers to book rooms directly with Hotels.com.[2853]

4. The D Squared Litigation

In Oct. 2003, the Federal Trade Commission instituted litigation against D Squared Solutions in federal district court in Maryland.[2854] D Squared co-opted a network administration feature of Microsoft Windows known as "Messenger Service," which was designed to enable computer network administrators to provide instant information to network users such as the need to log off, to send a stream of repeated pop-up advertisements that appeared on the screens of computer users connected to the Internet at 10- to 30-minute intervals. The pop-up messages instructed consumers to visit one of the defendants' web sites to purchase software that would cause the pop-up ads to stop.[2855] The FTC sued D Squared, alleging that its business methods

---

[2851] Id. at 408-09.

[2852] Id. at 410-12.

[2853] "MetroGuide.com Sues Hotels.com; Seeks Damages for Copyright Infringement and Predatory Advertising" (Jan. 27, 2003), available as of Jan. 28, 2003 at www.businesswire.com/cgi-bin/f_headline.cgi?bw.012703/230272653.

[2854] Complaint, Federal Trade Commission v. D Squared Solutions, LLC, 03 CV 31 08 (D. Md. Oct. 30, 2003), available as of Jan. 17, 2004 at www.ftc.gov/os/2003/11/0323223comp.pdf.

[2855] Id. ¶¶ 9-10.

constituted unfair competition, and secured a temporary restraining order against the defendants.[2856]

On Dec. 16, 2003, the court, after a hearing on an order to show cause why the court should not enter a preliminary injunction, denied the FTC's request for a preliminary injunction, vacated the temporary restraining order, and directed counsel to commence discovery immediately. A non-jury trial was calendared for Mar. 8-10, 2004. Because the court rendered its ruling on the record, no opinion was issued giving the court's reasons. However, the court apparently noted that it was unclear whether the pop-up ads had caused substantial injury to consumers.[2857] As of the writing of this paper, the litigation was ongoing.

5. International Decisions

In March of 2004, a the Court of First Instance in Cologne, Germany, issued a preliminary injunction against Claria (formerly known as Gator) that prohibited the company's pop-up and pop-under ads from appearing over Hertz's German rental car web site. The court concluded that Claria had violated various sections of a German unfair competition law.[2858]

H. Harvesting of Web Data

Harvesting of web data using robots and subsequent use or posting of the harvested data is a common occurrence on the Web and can be expected to generate much litigation in the future over claims of copyright infringement and the DMCA. A number of cases are beginning to emerge:

1. The FatWallet Dispute

Shortly before Thanksgiving of 2002, FatWallet.com posted on its web site a list of products and prices scheduled to appear in advertisements on "Black Friday" (the day after Thanksgiving, when by urban legend retailers go "in the black" and start to make money). The products and prices had apparently been harvested from web sites of various retailers. Wal-Mart, one of the companies whose data had been harvested, wrote a letter to FatWallet demanding the takedown under the DMCA of its product and pricing data on the ground that such data constituted a copyrighted compilation. Wal-Mart's attorneys also issued a subpoena under Section 512(h) of the DMCA asking for "information sufficient to identify the individual who posted the infringing material." Wal-Mart backed down on its demands after the Samuelson

---

[2856] The temporary restraining order was available as of Jan. 17, 2004 at www.ftc.gov/os/2003/11/0323223tro.pdf.

[2857] "FTC Denied Injunction Against Software Firm's Intrusive Pop-Up Ads" (Dec. 15, 2003), available as of Jan. 17, 2004 at http://24hour.startribune.com/24hour/technology/story/1089101p-7607955c.html.

[2858] Dawn Kawamoto, "German Court: Pop-Ups Need Permission" (Mar. 26, 2004), available as of Mar. 29, 2004 at www.news.com.com/2100-1024_3-5180240.html.

Law, Technology & Public Policy Clinic at Boalt Hall School of Law agreed to represent FatWallet and fight the subpoena.[2859]

2. Nautical Solutions Marketing v. Boats.com

Boats.com operated a web site, Yachtworld.com, on which subscribing yacht brokers posted listings of yachts for sale. Nautical Solutions Marketing (NSM) opened a competing web site known as Yachtbroker.com. NSM offered two services that Boats.com alleged were infringing of its copyrights. First, NSM used an Internet spider called Boat Rover to extract public yacht listing data from Yachtworld.com and other sites, such as manufacturer, model, length, year of manufacture, price, location, and URL of the web page containing the yacht listing. Boat Rover extracted the facts by momentarily copying the HTML of the web page containing the yacht listing and then collecting the prescribed facts, entering the facts into a searchable database, and then discarding the HTML.[2860]

Second, NSM offered a "valet service" under which, with the permission of a yacht broker who owned a yacht listing on another web site, it would move, delete or modify the yacht broker's listing. Under this service, Yachtbroker.com copied and pasted certain content, including pictures and descriptions (but not the HTML for the entire web page), from yacht listings on Yachtworld.com and posted the content on Yachtbroker.com in a different format. Although the copied content posted on Yachtbroker.com contained many of the same descriptive headings as the original listings on Yachtworld.com, the court found that the headings were the industry standard for yacht listings on yacht brokering web sites.[2861]

NSM filed an action for a declaratory judgment that its two services did not infringe Boats.com's copyrights, which the court granted. The court ruled that Boats.com's copyright of Yachtworld.com's public web pages in order to extract from yacht listings facts unprotected by copyright law constituted a fair use.[2862] The court further ruled that the copyrights in the pictures and descriptions of yachts copied by the valet service were owned by the individual yacht brokers, not Boats.com, and such copying was therefore not infringing. Nor was copying of the headings an infringement, because the headings, being industry standards, were not protected by copyright.[2863] Boats.com also claimed a copyright in the look and feel of the Yachtworld.com web site that it alleged had been copied by Yachtbroker.com. The court rejected this claim, finding that the two web sites were quite dissimilar in appearance.[2864] Finally, the court rejected a claim of infringement in a compilation copyright over the yacht listings on Yachtworld.com.

[2859] Declan McCullagh, "Wal-Mart Backs Away from DMCA Claim" (Dec. 5, 2002), available as of Dec. 8, 2002 at http://news.com.com/2102-1023-976296.html.

[2860] Nautical Solutions Marketing, Inc. v. Boats.com, No. 8:02-cv-760-T-23TGW (M.D. Fla. Apr. 2, 2004), slip op. at 1-2.

[2861] Id. at 3-4.

[2862] Id. at 4.

[2863] Id. at 5.

[2864] Id. at 6.

The court held that, because the format used by NSM to display on Yachtbroker.com the content copied from Yachtworld.com differed from the format used by Yachtworld.com to display the same information, the compilation of yacht listings on Yachtbroker.com was not virtually identical and was therefore not infringing.[2865]

IV. CONCLUSION

Copyright law provides one of the most important forms of intellectual property protection on the Internet. Considerable challenges are presented, however, in adapting traditional copyright law, which was designed to deal with the creation, distribution and sale of protected works in tangible copies, to the electronic transmissions of the online world in which copies are not tangible in the traditional sense, and it is often difficult to know precisely where a copy resides at any given time within the network.

The most difficult aspect of adapting copyright law to the online world stems from the fact that virtually every activity on the Internet – such as browsing, caching, linking, downloading, accessing information, and operation of an online service – involves the making of copies, at least to the extent the law treats electronic images of data stored in RAM as "copies" for purposes of copyright law. In short, "copying" is both ubiquitous and inherent in the very nature of the medium. If the law were to treat all forms of "copying" as infringements of the copyright holder's rights, then the copyright holder would have very strong control over Internet use of the copyrighted work. Which forms of copying the law should deem to be within the control of the copyright owner and which should not presents a very difficult challenge.

The cumulative effect of the copyright holder's rights being implicated by every use of a work on the Internet may be to give the copyright owner the equivalent of exclusive rights of "transmission and access" of information. Indeed, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty each make such rights express. However, the DMCA does not set up separate rights of transmission and access, although the draft European Copyright Directive would recognize such rights explicitly. Thus, the implementing legislative regimes adopted by various signatory countries to the WIPO treaties may result in varying scopes and/or denominations of rights, which runs contrary to the goal of the WIPO treaties to harmonize copyright law in the digital environment throughout the world.

The ubiquitous nature of "copying" on the Internet raises other difficult issues. For example, the practice of dividing copyright rights (such as the reproduction right, the public performance right, and the distribution right) among separate rights holders, as is common in the movie and music industries, will raise difficult issues of overlapping rights when a work is exploited through the Internet, because the exercise of all such rights will involve the making of "copies." Licensees may therefore need to seek permission from multiple rights holders that may not have been necessary in traditional media.[2866]

[2865] Id. at 7.

[2866] See Lemley, supra note 6, at 568-72.

Moreover, the traditional divisions of the bundle of copyright rights may no longer make sense on the Internet. For example, it is common for different entities to hold the right to reproduce copies of a movie, to distribute copies of the movie, and to grant licenses for public performance of the movie. Under that division of rights, who has the right to make the movie available on the Internet for on-demand viewing by users, since on-demand viewings will involve the making of copies of the movie, the distribution of copies, and the public performance of the movie? Or should it be the holder of the new right of transmission and access under the WIPO treaties?[2867] Because of the overlapping nature of copyright rights when applied to the Internet, new definitions and divisions of those rights will probably be necessary for online usage of copyrighted works. Corresponding new economic and royalty models and industry practices will also have to evolve. In the meantime, many existing licenses will be unclear as to which entity has rights to control online usage of a work, and one can expect to see much litigation over the interpretation of existing licenses.[2868]

The global nature of the Internet may give rise to multiple territorial liability. If every intermediate "copy" made during a transmission is considered infringing, there is the possibility that a single transmission could give rise to potential liability in several countries, even countries in which the sender did not intend or contemplate that its actions would result in the creation of a copy.[2869] Moreover, differing standards could apply – the same intermediate copy created in the course of transmission through the Internet could be considered infringing when passing through one country, and not when passing through another. In addition, the violation of the rights of transmission and access under the WIPO treaties might occur in yet another country. Although the WIPO treaties may afford a vehicle for greater transnational uniformity of copyright law, there is no guarantee that implementing legislation in the various signatory countries will be consistently adopted, consistently interpreted, or consistently applied.

In sum, copyright owners may have potentially unprecedented rights over use of their copyrighted material on the Internet. One can expect that the fair use and implied license doctrines (and their international equivalents) will take center stage in resolving the balance between copyright owners' and users' rights on the Internet. How broadly these doctrines will be applied, and whether they will be consistently applied in various countries, remains to be seen. Copyright lawyers will continue to be busy.

[2867] Because the new right of transmission and access in the WIPO treaties will be in addition to the other rights that may be implicated by Internet uses of copyrighted works, these new rights can be expected to increase the problem of overlapping rights. For example, existing licenses will be silent on these new rights, and there will therefore be great uncertainty as to whether the licensor retains such rights, or whether the licensee has a license under such rights and, if so, of what scope.

[2868] See Lemley, supra note 6, at 572-74. One commentator has considered several possible ways of dealing with the overlap of exclusive copyright rights that occurs on the Internet (placing the burden of overlap on the user; placing the burden of overlap on the copyright owner; and establishing a new right of transmission over a computer network that would *replace* the other rights to the extent they are applicable to network transmissions). See id. at 578-84.

[2869] In addition, at least one court held that where predicate acts occurred in the U.S. leading to infringements that occurred abroad, damages flowing worldwide from a U.S. infringement could be considered. Update Art, Inc. v. Modiin Publishing, Ltd., 843 F.2d 67 (2d Cir. 1988).