The Law on Computer Fraud in Ireland - Development of the Law on Dishonesty

PEARSE RYAN & ANDY HARBISON

INTRODUCTION

Computer fraud, which along with offences such as theft and forgery is a subdivision of those criminal offences involving dishonesty, has long been an area requiring legislative update, in order to provide Irish law enforcement authorities with the tools to tackle what is a complex and growing problem. This article examines the state of the current law, compares the position in Ireland with the UK, considers developments at international level and, finally, discusses possible legislative developments. This article concentrates primarily on computer fraud, a sub-division of computer based or aided crime generally. It does however, of necessity, discuss other related computer crime areas.

It is difficult to distinguish between computer based and computer aided crimes, just as it is difficult to distinguish between computer fraud and other forms of computer crimes. Typically, all but the most straightforward of frauds are computer based or aided, which renders them computer crimes. Typically, also, a number of offences under the relevant legislation tend to be committed based upon a single incident or set of facts, reflecting, at least in part, a legislative evolution from viewing computer crime as damage to viewing it as a loss creating/gain making activity. There are few pure hackers left nowadays, but there is no shortage of computer criminals.

There are few pure hackers left nowadays, but there is no shortage of computer criminals.

INITIAL LEGISLATION – THE 1991 ACT

THE 1991 ACT

The initial legislation attempting to deal with the area, the *Criminal Damage Act 1991* (the "1991 Act"), set the scene in the Section 1 interpretations by including data within the definition of 'property'. It then went on to define data as "*information in a form in which it can be accessed by means of a computer and includes a program*". Finally, it included reference to data within the definition of "*to damage*" and expressly, firstly, the addition, alteration, corruption, erasing and movement of data and secondly, the doing of acts contributing to the foregoing. The scene was then set for the relevant offences introduced by the 1991 Act:

- Section 2 sets out the offences relating to damaging property. These are not computer specific offences. However, based on the statutory definitions the reference to property can include offences relating to data; and

- Section 5 sets out the offence of unauthorised accessing of data. This is a computer specific offence.

SECTION 2 OFFENCE

Section 2 of the 1991 Act dealt with damage to property and intent to damage property. As mentioned above, the statutory definitions had extended the definition of "*damage*" to data. Section 2 then provided that *"to add to, alter, corrupt, erase or move to a another storage medium"* or to perform any act that might lead to this, will be considered criminal damage, as will making any omission to the data. It is noteworthy that this definition could easily be seen as including developing or intentionally distributing a virus. The definition does not, however, include copying data. In computer science terms to move data is to copy it to a new location, deleting the original version, while *copying* the data means leaving the original version intact.

SECTION 5 OFFENCE

To its credit, Section 5 of the 1991 Act defined for the first time in Irish Law the offence of "*unauthorised accessing of data*", making it an offence for

"a person who without lawful excuse operates a computer

(a) within the State with intent to access any data kept either within or outside the State, or (b) outside the State with intent to access any data kept in the State".

The actus reus of the offence is to operate the computer and the mens rea is to intend to access data. It is immaterial whether the offender actually succeeded in accessing data and "an intention idly to browse through a database seems to be sufficient criminal intent[1]". The offence is thus extremely wide in its application.

The drafting of the section makes it unclear to what part of the section the qualification "*lawful excuse*" applies, i.e. whether it applies to the operation of the computer or the accessing of the data. Section 6, which is a definition section, defines lawful excuse in terms of authority to access data, and not authority to operate a computer. A leading commentator[2] suggests that it is arguable this imports a requirement of unauthorised access into Section 5 and notes that in the US, the comparable offence is phrased in terms of "exceeding authorised access". It is unknown why the Irish legislature did not draft section 5 by expressly referring to unauthorised access if this is what was intended. Therefore, if an accused person had authority to operate the computer in question, the prosecutorial burden is then to show that the accused intended to access data which he was not authorised to access. This would likely arise in an employment context. It is submitted that the success of an unauthorised access provision depends on the presence of extensive, for example, internal workplace policies or website terms and conditions on the scope of authority to access particular data. The Minister of State in a 1991 Seanad debate[3] on the proposed legislation noted that a section 5 offence would not be committed by someone who has not been properly informed about the limits of his authority. It was suggested by the Minister that an employee taking home a disc containing data he was not authorised to access would commit an offence once he had accessed the data using his personal computer. Assuming the courts construed Section 5 in this manner, this could create an anomaly in criminalising the accessing of data in electronic form, as an employee taking home a hard copy file containing confidential information would not commit an offence. In the Seanad Debates, the Minister for Justice stated that the section was justified as "hacking is matter of major and legitimate concern"[4]. It was also intended to provide a useful alternative where damage was not proven in a Section 2 offence (below).

---

[1] Jackson, Clare. (1991) *Irish Current Law Statutes Annotated* Sweet and Maxwell at p. 31-08

[2] McIntyre, T.J. (2005) *Computer Crime in Ireland: A Critical Assessment of the substantive law* 15(1) ICLJ 13 at p. 6

[3] 130 Seanad Debates col. 1991. The Dáil is the lower house of the Irish parliament and the Seanad is the upper house.

[4] 403 Dáil Debates col. 1990.

THE TARIFFS

In terms of sanction, the general Section 2 criminal damage to property offence is, as one would expect, a serious offence, punishable on summary conviction or on indictment, ultimately (in relation to non life-threatening offences) by way of fine of up to IR£10,000 or up to ten years imprisonment. Section 5, being a computer specific offence, includes lighter penalties on summary conviction of a fine up to IR£500 or up to three months imprisonment.[5]

THE 1991 ACT AND EVOLUTION OF COMPUTER CRIME

Unfortunately, the 1991 Act reflected a perception of hacking that was never entirely accurate, as well as being outdated by the turn of the century. The 1991 Act essentially saw hacking as a form of vandalism, which to some extent it is, but does not appear to consider that the ultimate objective of hacking a computer could be anything else than wanton destruction. Hence the light penalties imposed for hacking under Section 5.

In reality, only the most trivial of computer crimes are purely destructive in primary intent. The most damaging hacking attacks tend to have an ulterior motive. Even in the strict terms of Section 2, data is rarely accessed for its own sake, but is stolen for the purposes of reuse, resale or extortion. Where data is copied but not moved, it is by no means clear that the Section 2 offence fully applies, with the relatively trivial exception of Section 5.

The 1991 Act essentially saw hacking as a form of vandalism, which to some extent it is, but does not appear to consider that the ultimate objective of hacking a computer could be anything else than wanton destruction.

Furthermore, the 1991 Act does not seem to cover denial-of-service type attacks on computers, where access to a computer is blocked or interdicted by an attacker. Such attacks are usually performed preliminary to an extortion attempt. However, they often do not alter any data on the affected computer. They act by preventing data reaching the target, not by altering the data already stored. The absence of any measure for dealing with such attacks is to some degree understandable, given that at the time the 1991 Act was drafted, deliberate denial of service type attacks were relatively uncommon.

The 1991 Act appears to have been drafted on the basis of a limited understanding of how computer crime is committed. It seems to presume that defeating the security of a computer is a purely technical exercise, entirely based on the operation of a computer. In such a classical hacking attack, the computer criminal will reconnoitre the target computer remotely using software tools, gaining access either by means of a misconfiguration of the target computer, or by means of some vulnerability or fault in its programs or operating system[6]. The 1991 Act deals with the classical approach by making it an offence to possess anything with intent to damage property. This broad definition could easily include many viruses, hacking applications and other malicious software.

In reality however, deception and confidence trickery ('social engineering' in hacking jargon) have always been key weapons in the computer criminal's arsenal[7]. In many of the most successful computer frauds there has been relatively little computer 'operation' in the sense of the 1991 Act.

---

[5] As per Council Regulation (EC) 2666/98 the euro equivalent of IR£10,000 is approximately €12,697.38 and of IR£500 is approximately €635.

[6] McClure, S; Scambray, J.; and Kurtz, G. (2009) "Hacking Exposed" McGraw Hill, 6th ed.. Perhaps the best description of this kind of attack is found in Stoll, C (1989) "The Cuckoo's Egg", Doubleday.

[7] Mitnick, K and Simon, W.L. (2002) "The Art of Deception: Controlling the Human Element of Security",Wiley, 2002.

Indeed, it has been long understood by hackers that the most effective way of gaining access to someone else's computer is to ask them for their password.

The consensus which evolved during the latter stages of the 1990's, as IT became an ever more prevalent feature of our business and personal lives and computer crime demonstrated a parallel if not exponentially faster evolutionary trend, was that this initial legislation in the area of computer fraud and computer crime generally was not sufficiently robust to tackle the complexity and prevalence of computer and computer-aided fraud. This was reflected in the fact that few if any successful prosecutions were obtained under the 1991 Act, despite the exponential increase in computer crime that occurred during the 1990's[8].

The new legislation, discussed below, was enacted to attempt to remedy some of the more glaring deficiencies in the 1991 Act, as well as attempting to adapt to a number of new trends and technologies that had emerged in the intervening years. It was hoped that the new legislation would bring Ireland more into line with international norms and would facilitate the effective prosecution of perpetrators of computer or computer aided fraud. The Minister for Justice, Equality and Law Reform, in introducing the legislation, noted that the Act was "designed to deal with present day realities[9]" and Section 9 was "innovative[10]" in addressing computer based crime. How well it has succeeding in meeting this aspiration is the subject of the remaining discussion.

THE 2001 ACT – A DISCUSSION

Section 9 of the *Criminal Justice (Theft and Fraud Offences) Act, 2001* (the "2001 Act") came into effect on 1st August 2002 and created a new offence where a person *"dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another"*. It can be seen that this is a broad statement with the potential for far-reaching implications, given the all-pervasive nature of the computer in our personal and business lives.

There are a number of components to this new offence, which are worth noting:

LOCATION OF PERPETRATOR

The first point of interest is that the offender need not be in the State at the time the offence is committed. The computer, which is an instrument of the offence, must be situated in the State. However, given network technology, a computer can be remotely operated from any corner of the globe, given the appropriate expertise and equipment. Thus, the computer into which the offender inputs commands is not necessarily the computer that is *"operated"* for the purposes of the 2001 Act. Computer crime can and is commonly committed in one State by a perpetrator located in another - effectively the equivalent of shooting someone from across an international border. The reference to *"causes to be operated"* is a broad statement and does not require physical control of a computer. For example, to direct from outside the State a person within the State to operate a computer within the State would seem to satisfy the requirements of Section 9. Thus, the criminal mastermind pulling the strings while lounging poolside in some exotic location could fall within the ambit of Section 9, although the Gardaí will bear the burden of providing the required link between cause and effect.[11]

---

[8] CSI FBI Computer Crime surveys

[9] 527 Dáil Debates 2000. Mr. C Lenihan welcomed the legislation and noted during the same debate that the rate of computer based crimes reported to the Garda was increasing by 100% each year and that "hackers and code crackers have the potential to wreak havoc unless caught and punished severely".

[10] 168 Seanad Debates 2001

[11] An Garda Síochana – the police force in Ireland. The office tasked with computer crime is the Bureau of Fraud Investigation

As a general comment on international criminal law, possibly in practise the most important point to note in relation to any significant computer crime incident, given the evolved nature of such organised crimes, the law enforcement authorities will be faced with the challenge of prosecuting possibly numerous offences against possibly numerous accused involving possibly numerous jurisdictions. Section 9 of the 2001 Act, which targets a person, *"whether within or outside the State"*, recognises the possibility of jurisdictional issues arising and has allowed the courts to try an offender regardless of whether he was within the State at the relevant time. This extra-territoriality of jurisdiction, which is an unusual feature in Irish legislation, is essential to the effectiveness of this provision, which underpins the entire of Section 9. However, the development of computer fraud and computer crime generally is so fast that it challenges the traditional enforcement activities of the State. This point is discussed further below.

In its favour, the 2001 Act is based on a realisation that much Internet crime is trans-national. However, it does not take into account the sheer complexity of many modern computer crimes. For example, in a case recently investigated by one of the authors, customers of a major bank were sent deceptive e-mails claiming to be from the bank and requiring customers to follow a link embedded in the false e-mail to a web-site mimicking the banks own e-banking application[12]. Unsuspecting customers entered their e-banking details on the fake web site. The criminals running the web-site then used these details to transfer funds from the customers' bank accounts to so-called 'mule' accounts in the same bank. Petty criminals ('mules') were then employed to extract the funds from the mule accounts at the bank counter or at ATMs.

Were all the computers involved in this scheme based in Ireland or a single other country, then, investigating the crime would have been straightforward, but they were not. The computers used to send the original fraudulent e-mail were based in a number of different countries worldwide. However, all had been hacked by means of virus software originating at a location unknown, and were running e-mail software without the knowledge of their owners. The web-server containing the fake e-banking web-site was based in the Ukraine, but it is possible that this too had been hacked and the users of the site were unaware that the fake e-banking application was running on it. The fraudulent transactions that made use of the stolen customer credentials were made on computers located in Israel. The reason why the embezzled funds had to be transferred to an account in the same bank branch was that the affected banks own anti-fraud procedures prevented it being transferred abroad, but in other banks this could easily have occurred. Police were able to intercept some of the 'mules', but these were minor cogs in a complex mechanism.

The question that arises here is where did the crime or crimes actually occur? While the money was actually stolen out of Irish accounts, it is arguable that offences occurred in three or four different states (despite the fact that Gardaí are sure that the controller of the fraud was based in Ireland). Perhaps a more fundamental problem is how to investigate cases of such labyrinthine complexity. In the absence of binding international agreement it is essentially impossible. In the meantime, the 2001 Act is essentially a dead letter in terms of dealing with this kind of complex international fraud. It is worth noting that we are discussing here fraud in the upper echelons of endeavour by today's standards and we believe outside the contemplation of the authors of the 2001 Act. However, the point as to the effectiveness of the 2001 Act to deal with this growing area of computer fraud is important to the effectiveness of the Irish law enforcement authorities and ultimately the security of the State.

A recent English case of note in relation to the issue of location and jurisdiction is *R. v Sheppard and Whittle*[13] Here, the defendants were charged with publishing material which was threatening, abusive or insulting intending thereby to stir up racial hatred contrary to s.19 of the Public Order Act 1986. The second defendant allegedly emailed the material to the first defendant who then edited it on his computer and uploaded to a website which was hosted by a server in California.

[12] This kind of fraud is known as a 'phishing attack' in hacking parlance

[13] [2010] EWCA Crim 65

The defendants argued that the English court did not have jurisdiction to deal with the matter, since the server was based in California. The court held, referring to the test established in *R. v Smith (Wallace Duncan) (no. 4)*[14], that the Crown Court had jurisdiction to try a defendant if a "substantial measure" of the activities constituting the crime took place in England. It was decided that almost all of the activities had occurred in England. It would be interesting to see whether the Irish courts would adopt such an approach in a situation where a defendant had caused a loss or made a gain under the 2001 Act. It could be argued that in the aforementioned case of bank fraud occurring in numerous jurisdictions, were the Gardaí to provide evidence that the controller of the fraud was based in Ireland, the court would have been able to hold that "substantial measures" had taken place in Ireland, and that it therefore had jurisdiction to decide that case. Nevertheless, it is clear that the rapid development of technology available to commit crime over the internet necessitates international co-operation beyond mere domestic legislative reform.

COMPUTER

Section 9 refers to a *"computer"*. In line with what seems to be standard practice in Irish legislative drafting, the 2001 Act does not define a *"computer"*, thereby allowing for technological development. Also, Irish interpretation legislation in enabling is providing that "…*in construing a provision of any Act or statutory instrument, a court may make allowances for any changes in the law, social conditions, technology, the meaning of words used in that Act or statutory instrument and other relevant matters, which have secured since the date of the passing of that Act or the making of that statutory instrument, but only insofar as its text, purpose and context permit*".[15]

One can envisage defendants' lawyers raising arguments in relation to certain forms of devices not falling within the scope of the term, but, unless the devices are quite far removed from the common understanding of the term, such arguments are unlikely to persuade the criminal courts. For example, at first glance the use of a manufactured swipe-card to activate a door-access control device, or ATM, would not seem to constitute use of a computer. However, the use of a computer was required in order to manufacture the device and the device in turn causes the operation of a computer controlling the door access, or ATM. Both actions would seem to satisfy the requirements of Section 9. In technical terms there exists a very precise and long-standing definition of what constitutes a computer, devised by Alan Turing, someone with a legitimate claim to be one of the inventors of modern computers[16]. A precise, formal definition of what constitutes a computer is given in Turing's 1936 paper "*On computable numbers, with an application to the Entscheidungsproblem*"[17], a rather dense document which, nevertheless, can claim to be one of the most important written in human history. In summary, the paper demonstrates mathematically that

Any numerical calculation can be performed by a machine with an input device, an output device, a memory and a simple numerical processor. Any such machine can be considered a computer.

Of course this definition is rather broad, but this is no disadvantage. Certain recent technological developments in nanomechanical[18] and quantum computing[19] have produced computers very

[14] [2004] EWCA Crim 631

[15] Section 6, Interpretation Act 2005 (No. 23 of 2005)

[16] Leavitt, D.(2006) "The Man Who Knew Too Much: Alan Turing and the Invention of the Computer", W.W.Norton

[17] Turing, A.M. (1936) "On computable numbers, with an application to the Entscheidungsproblem", Proceedings of the London Mathematical Society, Series 2, 42), pp 230 - 265

[18] Blick, R.H. et al (2007) "A nanomechanical computer—exploring new avenues of computing" New J. Phys. 9 (2007) 241

unlike the modern silicon based devices that sit on all our desks, but still falling within the Turing definition. While at present these devices exist only in laboratories, it is a distinct possibility that they will become more generally available in the medium term and most likely in the next few decades.

OPERATION OF COMPUTER

Crucially the term "*operate*" is not defined in the 2001 Act. However, if the Act is to have teeth "*operate*" must include any manipulation or control of a computer, however basic or trivial. Hence, mere data access may constitute an offence under the 2001 Act, as one cannot, either directly or remotely, access data without the performance of a task by one or more computers. The UK Computer Misuse Act 1990 refers to "*causing a computer to perform any function*", which in effect, could be an action as simple as switching it on. The term "*operate*" in the Irish provision could be construed as having an equally broad meaning.

One benefit of this broad definition is that it allows a certain amount of latitude in dealing with new forms of computer crime. In particular, the definition of unlawful use clearly covers the denial of service type attacks so clearly missed in the 1991 Act.

In technical terms, to "*operate*" a computer could be considered to be carrying out an action which caused the contents of the computer's memory to alter (falling back on the Turing definition). This would have the additional advantage of defining operating in terms that could be investigated and detected using existing computer forensics techniques and technologies. [20]

DISHONESTY

A key element of the 2001 Act, and Section 9 in particular, is the introduction into Irish law of the concept of "*dishonesty*". This follows a recommendation of the Law Reform Commission[21]. "*Dishonestly*" is defined in Section 2(1) of the 2001 Act as *"without a claim of right made in good faith"*.

Section 9 refers to the carrying out of the offence by a *"person"*. Statutory interpretation legislation provides that ""*Person shall be read as importing a body corporate… and an unincorporated body of persons, as well as an individual…*".[22] The authors are not aware of any ecrime prosecutions of non-individuals whether in the UK or Ireland, although they are aware of circumstances which would seem to allow for prosecutions, notwithstanding the difficulties inherent in any form of corporate criminal law prosecution, and assume the prosecution authorities are even more reluctant to prosecute non-individuals than individuals.

The person, to be guilty of an offence under Section 9, must have operated a computer or caused the operation of a computer when they could not in good faith claim to be rightfully entitled to do so. As noted above, physical location of the perpetrator within the state is not necessary for the commission of an offence under Section 9. The term *"dishonesty"* falls within the part of the Section dealing with operation of a computer, rather than making of gain or causing loss to another. The question arises as to the effect of this reference. It would seem that where a gain is made or loss caused to another, with intention, by way of direct use of a computer or causing of operation of a computer, which is authorised use or authorised causing of operation, then, no offence has been committed. The question then arises as to when such circumstances might

---

[19] Kaye, P, Laflamme, R. and Mosca, M. (2006) "An Introduction to Quantum Computing" Oxford. Available as an e-book at http://www.free-ebook-download.net/science-book/581-introduction-quantum-computing.html

[20] For example, as described in Jones, K.J., Bejtlich, R. and Rose, C.W. (2005) "Real Digital Forensics: Computer Security and Incident Response", Addison Wesley

[21] Recommendation contained in the Report on *The Law Relating to Dishonesty* (1992)

[22] Section 18 (c) Interpretation Act 2005 (No. 23 of 2005)

arise. For example, where a CFO has unrestricted access to the company financial management software and transfers monies from a corporate account to a personal account, then, this would fall outside the scope of authorised use of company computer resources, meaning the act is done without a *"claim of right made in good faith"*.

Another area where this problem commonly arises is where dishonest actions are committed by computer administrators. Such individuals have, as part of their jobs, extremely wide ranging and powerful privileges on computer systems. Given the extent of administration privileges, it is often very difficult to conclusively state if such an individual has culpably exceeded the limits of their role.

It is difficult to produce an example of authorised use or controlling of a computer which gives rise to loss to another in the corporate sphere, as terms of employment typically restrict employee authorised use of company IT resources. In the personal sphere there are no such controlling terms and an individual is free to dictate his own scope of use. Clearly, where the computer used or caused to be operated is either stolen or hacked into, then, no claim of right of use exists. Where the computer is legitimately owned or leased, then, the use is with a claim of right and this essential part of the definition is not satisfied. For example, internet based share dealing via an authorised intermediary would seem to satisfy all the requirements of Section 9, save for the presence of dishonesty. If carried out by an authorised subscriber to a share dealing service in accordance with the service terms of use there would seem to be no dishonesty. However, to hack into an internet based share dealing service, set up a false account and conduct trades, does involve dishonesty and would seem to satisfy the requirements of Section 9. The foregoing facts are of the type often seen in the all too common financial scandals involving in-house traders causing their employers extraordinary trading financial losses.

INTENTION

The required mental element of an offence under Section 9 is intent. Apart from strict liability, which is generally confined to regulatory offences, intent is the highest level of culpability in criminal law. The person who dishonestly operates a computer within the State, and who causes a loss to another or a gain for himself or another, must have intended to achieve this outcome through his actions. An individual who performs the same actions and causes loss to another, without intending to do so, but with mere indifference as to whether his activities occasion such losses, is not guilty of an offence under Section 9. Clearly Section 9 is aimed at malicious or professional wrongdoers and not at those whose ill-judged misadventures inadvertently cause loss to others.

McIntrye highlights the point that the legislation only seems to cover a situation where a perpetrator utilises the computer to cause a loss or make a gain in monetary terms[23]. Unlike the UK legislation – *the Computer Misuse Act 1990*, Section 2 – the 2001 Act does not anticipate a scenario where an offender dishonestly gains access to a computer in order to collect information which will then be used to commit a crime which is not related to making a gain or causing a loss in monetary terms. If, for example, someone accesses information about a person with the ultimate objective of murdering them, it does not appear that their activity will be encompassed by the legislation.

GARDAÍ POWERS

The Gardaí are equipped with new powers to aid the investigation of offences under the 2001 Act. In carrying out the terms of a search warrant granted under Section 48 of the 2001 Act, the Gardaí are empowered to:

[23] McIntyre, TJ (2008) 'Cybercrime in Ireland' In: Reich, P (eds). *Cybercrime and Security*. Oxford: Oxford University Press at p. 23

(i) seize or operate any computer at a place being searched;

(ii) require persons at a place being searched to disclose passwords and enable Gardaí to access information stored on any computer; and

(iii) access any computer, which is lawfully accessible, by means of a computer being operated at a place being searched.

While these new powers clarify and expand the investigative options available to the Gardaí, unfortunately, the penalties for failing to disclose passwords are so minor that a serious question arises as to their effectiveness. The authors believe this to be one of the main areas of Gardaí concern with the legislation. Section 49(1)(c) provides that the tariff is a maximum fine of IR£500[24] or six months imprisonment. As is discussed below, increasing the penalties in this section has repercussions on the right to silence of an accused.

Computer criminals increasingly use encryption of files, or entire computer disks, to cover their actions. Where encryption has been implemented correctly (and it is not very difficult to do) it is effectively impossible for Gardaí to gain access to a computer without being provided with the encryption keys, or at least the security password to the file on the computer in which they are recorded (the 'key store'). If a computer contains evidence of serious malfeasance, it is well worth a criminal's while putting up with the relatively minor inconvenience of a small fine or brief imprisonment so as not to make this information available to police.

For comparison, in the UK the equivalent penalty for failing to disclose passwords is two years imprisonment, (or five years under the Terrorism Act 2006 in a 'national security' case), and even this is considered by some commentators to be insufficient in the light of increasingly serious crimes being committed by means of, or with the support of, computers.[25] However, this obligation to disclose the password raises issues around the safeguards of criminal procedure, such as the right to silence and not to self-incriminate. Walden notes that whilst refusal to comply in order to avail of a lesser penalty than would be the case under a more serious charge once the police obtained the necessary evidence "may be unfortunate, it would seem to be a necessary compromise where the rights of the individual are balanced against the need to protect society".[26] In Ireland, an increase in the penalties under Section 49 of the 2001 Act may not therefore be a viable option, given the possible threat of a constitutional based challenge[27].

PENALTIES

The 2001 Act introduced severe penalties for Section 9 offences, available on indictment, of a fine of unspecified amount, or maximum of ten years imprisonment, or both. The penalties are not generally seen as the area of difficulty under the 2001 Act, with the exception of those applicable to non-disclosure of passwords.

[24] Approximately €635 and see Footnote 5

[25] Section 53 of the Regulation of Investigatory Powers Act 2000

[26] Walden, Ian. (2007) *Computer Crimes and Digital Investigations*, Oxford University Press at para. 4.331

[27] e.g. in *Heaney v. Ireland* [1994] 3. I.R 593 Costello J noted that the right to silence was not absolute and could be restricted by legislation, as long as those restrictions withstood a "proportionality test".

THE UK POSITION – A COMPARISON

COMPUTER MISUSE ACT 1990

The equivalent legislation in the UK to the 2001 Act is the Computer Misuse Act 1990 ("the CMA"). There were three main offences under the CMA when first enacted:

- Section 1 - unauthorised access to computer material (e.g. hacking);
- Section 2 - unauthorised access to computer material with intent to commit or facilitate further offences (e.g. fraud); and
- Section 3 - unauthorised modification of computer material (e.g. the spreading of viruses).

For the purposes of this article, the Section 2 offence is the most relevant, as it involves the commission of a Section 1 unauthorised access offence, together with the intention to commit or the commission of a further offence, for example fraud. An example of the successful application of Section 2 of the CMA in the English courts is the case of *R v Borg*, where an investment company analyst was convicted for making fraudulent transfers from fake accounts he had established within a fund management system.[28]

In many respects the CMA and 2001 Act are similar. Certain terms such as 'computer' or 'data' remain undefined so as to ensure technological developments do not render the legislation obsolete. Also, the CMA has broad application, in that it contains a provision similar to Section 9 of the 2001 Act, whereby an unauthorised access offence can be committed by a perpetrator located outside the UK, where there is *"a significant link with the domestic jurisdiction*".[29] By virtue of this section, if the accused were located outside the UK when he or she caused the computer to perform the criminal function and the computer containing the program or data to which access was illegally obtained was in the UK, then, an offence is committed for the purpose of the CMA. The penalties under Section 2 of the CMA are twelve months' imprisonment[30] and/or a fine "not exceeding the statutory maximum" on summary conviction, and five years' imprisonment and/or a fine for a conviction on indictment. The statutory maximum is £2,000.[31]

STATUTORY DEVELOPMENTS - APIG

It appears that few prosecutions have been brought under the CMA. Possible reasons for this include a low level of appreciation of the scope of the CMA, the complex technical nature of the crimes which makes evidence gathering difficult, and a feeling that the police, prosecution service and courts do not take computer crime as seriously as other criminal activities.[32] Often prosecuting parties appeared to prefer more general legislation, such as for example the Theft Act 1968, when dealing with issues of fraud involving computers, as such legislation is regarded as having "inherent flexibility and freedom from the technicalities of the Computer Misuse Act".[33] For this reason a House of Commons All Party Internet Group ("APIG") was

---

[28] Unreported March 1993; Chris Reed and John Angel; Computer Law; 4th edition [2000] Ch. 9 Computer Crime by Ian Walden p.284

[29] Sections 4 and 5 of the Computer Misuse Act 1990

[30] Six months on summary conviction in Scotland – section 2(5)(b)

[31] http://www.lancs.ac.uk/iss/governance/rules/cmisuse.htm

[32] SJ Berwin: "Is the Computer Misuse Act 1990 doing its job?"

[33] David I Bainbridge (2000) *Introduction to Computer Law*; 4th edition Ch 24 Computer Fraud at p 300

established in March 2004 to consider the effectiveness of the legislation in its original form. The APIG inquiry focused on whether the CMA was broad enough to cover modern criminal practices, whether there were loopholes in the legislation that needed to be addressed and whether the level of penalties were sufficient to deter modern criminal computer activity.

Interestingly, the APIG report did not call for widespread amendments to the CMA. The report suggested two main amendments to the CMA:

- The addition of a denial-of-service (DoS) offence to the CMA; and
- An increase in the tariff for CMA hacking offences from six months to two years.

The Police and Justice Act 2006 (the "PJA") made a number of amendments to the CMA in order to implement certain recommendations made in the APIG report:

- Section 35 of the PJA amended Section 1 of the CMA, in order to convert the summary offence of "*unauthorised access to computer material*" into an offence triable either summarily or on indictment. This amendment renders this offence extraditable and therefore more easily enforced extra-territorially;
- Section 36 of the PJA amended Section 3 of the CMA, by changing it from an offence of "*unauthorised modification of computer material*" to "*unauthorised acts with intent to impair*" computer material. In addition this section also creates a new offence of "*unauthorised acts with recklessness as to impairing*" computer material. There is a maximum penalty of 12 months imprisonment on summary conviction and 10 years imprisonment on indictment. This amended Section 3 of the CMA therefore criminalises the commission of a DoS type act, which was recommended by the APIG report; and
- Section 37 of the PJA inserted into the CMA a new Section 3A offence relating to "*making, supplying or obtaining articles for use in computer misuse offences*". This criminalised the creation, use and supply of so-called hacker tools. The offence is broad in potential application, referring to "…*intending it is to be used to commit, or to assist in the commissioning of an offence under Section 1 or* 3" as well as the far more broad brush offence of "… *believing that it is likely to be used to commit*…" an offence under such sections.[34] Both offences and in particular the latter offence have given rise to much comment, especially within the computer science community.[35] A subsequent CPS guidance paper on the CMA has also attracted much comment.[36] Such an offence does not exist in the Irish legislation. The UK Fraud Act 2006 (considered below) also addressed the issue of hacker tools.

Also noteworthy were several other recommendations contained in the APIG report.[37] The APIG report suggested:

- the Director of Public Prosecutions (DPP) should set out a permissive policy for private prosecutions under the CMA. This would allow private companies to tackle cases that the police/prosecuting service did not consider as priority matters;

---

[34] Section 37 (1) and 37 (2) respectively of the Police and Justice Act 2006

[35] For example, see Light Blue Touchpaper – Security Research, Computer Laboratory, University of Cambridge, posting (including interesting comments) dated December 31st by Richard Clayton, entitled "*Hacking Tool guidance finally appears*" – http://www.lightbluetouchpaper.org/2007/12/31/hacking-tool-guidance-finally-appears/

[36] For CPG guidelines see http://www.cps.gov.uk/legal/a-to-c/computer_misuse_act_1990/index.html . For an example of commentary on CPS Guidelines and Section 3A see Footnote 35 and see ZDNet discussion at http://www.zdnet.co.uk/news/security-threats/2008/01/03/expert-cps-hack-tool-guidance-confused-39291862/.

[37] Press Release Wednesday 30th June 2004**:** All Party Internet Group report on Computer Misuse Act 1990 and page 18 of the APIG Report

- the introduction of a new Fraud Bill to address issues such as 'phishing'. The UK government enacted the Fraud Act 2006, which contains provisions criminalising the possession, making or supplying of any articles, which includes programme or data held in electronic form, with the intention to commit fraud. There is a maximum penalty of 12 months imprisonment and/or a fine not exceeding the statutory maximum on summary conviction and on indictment to 10 years imprisonment and/or a fine; and

- improving information in this area. Evidence to the inquiry showed a noteworthy lack of understanding of the CMA. The report suggested more educational material be used to combat this lack of understanding. This is an interesting comment on what must be a worldwide reluctance of state law enforcement authorities to prosecute what are technical and complex matters, generally of a commercial nature. The exception would be in matters of state security, where the law enforcement focus seems strong and ever developing.

The APIG report suggested the problems with prosecuting computer crime in the UK did not lie with the law, but rather with practical issues such as evidence gathering and the mind-set of the bodies enforcing the legislation.[38] This appears not to have changed significantly.

SURVEILLANCE AND INTERCEPTION

There are significant powers of surveillance[39] and interception contained in the Regulation of Investigatory Powers Act 2000 ("RIPA") which have application to cybercrime. Walden notes that this would include keystroke loggers or other types of 'spyware' placed on a suspect's machine to record and disclose information[40].

Section 17 of RIPA provides that any evidence obtained through interception cannot be used as evidence in court and is only for the purpose of an investigation, although there is no corresponding provision for evidence obtained through surveillance. It is difficult to defend evidence obtained by remote searching in court, due to difficulties in proving that the evidence has not been tampered with. The authors are not aware of such evidence having been used in court. It appears the use of 'remote searching' by the police has been in use in the UK for some time although it appears not to have been widely used[41].

On 27 November 2008, the EU Council of Ministers invited Member States and the Commission "*to introduce measures based on case studies, particularly taking into account technological developments, so as to prepare tools for operational use, in the short and medium term, such as….. facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country*"[42]. These non binding "conclusions" followed on from the Commission's communication of 22 May 2007 to the European Parliament, the Council and the Committee of

[38] SJ Berwin: "Is the Computer Misuse Act 1990 doing its job?"

[39] Surveillance, as defined in Section 48(2) of RIPA , includes "*surveillance by or with the assistance of a surveillance device*". A 'surveillance device' is defined in Section 48(1) as "*any apparatus designed or adapted for use in surveillance*". Similar to the powers of interception of communications contained in section 5 of RIPA, surveillance can only be used if proportionate and necessary "*in the interests of national security, for the purpose of preventing or detecting serious crime, to safeguard the economic well-being of the United Kingdom*". Section 5(3) and Section 28(3) Section 5(3(d) in respect of interceptions also includes the justification of responding to a request under mutual legal assistance procedures

[40] op. cit. n 23 at para 4.63

[41] Sunday Times, 4 January 2009 available at http://www.timesonline.co.uk/tol/news/politics/article5439604.ece

[42] Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime" (2009/C 62/05) at paragraph 2(b)

the Regions *"Towards an Overall Policy Against Cybercrime"* and the Council of Europe Conference on Global Co-operation Against Cybercrime in April 2008[43].

INTERNATIONAL DEVELOPMENTS AND CONCLUSION

THE INTERNATIONAL PROBLEM

The 2001 Act unequivocally contains within Section 9 the twin concepts of dishonesty and intention. The relationship between the two will fall to be teased-out in prosecutions under the 2001 Act. The State will be required to satisfy both tests in order to obtain prosecutions under the Section. This may be a stiff challenge for the prosecution. The requirement for dishonesty will likely operate to exclude from the scope of the Section a number of uses of computers involving the making of a gain or causing a loss to another. There has been a notable reluctance on the part of the Gardaí and prosecution services to prosecute under the 2001 Act and, as mentioned below, the 2001 Act may be on the legislative calendar for substantial reform.

The offence of unlawful use of a computer is defined with the existence of the global village firmly in mind. However, the effectiveness of the Gardaí in investigating computer related offences, and, in particular, in tracing and charging offenders, is subject to the limitations of national law. We might live in a global village, but technology allows the knowledgeable perpetrator the anonymity of a metropolis. The problem is not unique to Ireland, but the global village allows for anonymity of criminals, something of which they are all too aware. National police forces, including the Gardaí, can do little in the absence of, firstly, specific international co-operation in the area of computer crime and, secondly, a concerted international discussion on how best to tackle this ever-growing branch of the criminal family. Any movement in this area in order to be effective needs to be co-ordinated within the international community.

EUROPEAN CONVENTION & IRISH IMPLEMENTATION

Ireland has signed the Council of Europe Convention on Cybercrime (the "Cybercrime Convention") but has yet to ratify the Cybercrime Convention.[44] The Cybercrime Convention was specifically formulated against a background where *"… new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other then where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus, solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society".*[45]

Discussion of the complex provisions of the Cybercrime Convention is outside the scope of this article, however, it was created with the global village firmly in mind. Implementation into local law would:

- fulfil the Irish obligation in terms of harmonising domestic criminal law in the area of computer and computer aided crime across the Cybercrime Convention signatories;
- fulfil the Irish obligation in terms of harmonising enhanced international co-operation, including extradition rules; and
- in terms of domestic law, provide for procedural law powers agreed internationally as necessary for the investigation and prosecution of computer and computer aided crime offences.

---

[43] ibid

[44] Signature dated 28/02/02

[45] Explanatory report to the Convention on Cybercrime – Clause 1

The Cybercrime Convention required ratification by a minimum of five states in order to come into effect, which occurred on 1st July 2005. As mentioned, it has yet to be ratified by Ireland. Interestingly, there has been criticism of the Cybercrime Convention in failing to provide sufficient protection for privacy rights. The Cybercrime Convention provides that a participating country is to award new powers of search and seizure to its law enforcers including a power to monitor a citizen's online activities in real time.[46]

EU INITIATIVES

Tackling cybercrime has been a concern at EU level since a European Council meeting in Tampere in October 1999 affirmed the need to approximate provisions concerning offences and sentencing in the area of cybercrime, which was subsequently recognised and reaffirmed in a 2000 Communication entitled: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime[47]. The Council Framework Decision[48] of 2005 on attacks against information systems complements the work of the Cybercrime Convention and proposes to approximate criminal law systems and enhance co-operation between judicial authorities concerning illegal access to information systems, illegal system interference and illegal data interference, including aiding, abetting and attempting to commit these offences[49]. The Framework Decision provides that each Member State will have jurisdiction over an offence committed on its territory or by one of its nationals. If several Member States have jurisdiction over an offence, they must cooperate to decide which State will prosecute the offence. The deadline for implementation passed on 16th March 2007.

IRELAND WHERE TO NOW?

There has been on the legislative agenda in Ireland for some years now a legislative initiative entitled "*Criminal Justice (Cybercrime and Attacks against Information Systems) Bill*". This will transpose the Framework Decision on attacks against information systems and give effect to the Cybercrime Convention, as referred to above. As of the date of this article[50], the Bill has not yet been drafted, and the Government Legislation Programme states that it is not possible to give an expected publication date. It is included in the list under the heading 'Bills in respect of which heads have yet to be approved by Government'.[51]

By analogy, this is the equivalent of engaging in a boxing match with a technically adept opponent, who knows the rules, with one arm tied behind your back and not being able to leave your corner. The chances of a knockout or even a points victory are not great.

The Irish Reporting and Information Security Service (IRISS) held its first annual cyber crime conference in Dublin in November 2009[52]. IRISS

[46] Article 20

[47] COM/2000/0890 final (not published in the Ofl lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2000&nu_doc=890

[48] Under Title VI of the EU Treaty, Framework Decisions are used to approximate the laws and regulations of the Member States. Proposals are made on the initiative of the Commission or a Member State and they have to be adopted unanimously. They are binding on the Member States as to the result to be achieved but leave the choice of form and methods to the national authorities - http://europa.eu/scadplus/glossary/framework_decisions_en.htm

[49] Council Framework Decision 2005/222/JHA of 24th February 2005

[50] June 2010

[51] http://www.taoiseach.gov.ie/eng/Taoiseach_and_Government/Government_Legislation_Programme/SECTION_C11.html

[52] Irish Times, December 4, 2009

was formed in 2008 as a voluntary organisation to address the Irish government's failure to establish a Computer Emergency Response Team (CERT) to advise organisations on security threats to their IT systems. IRISS issues free advice and warnings on information security threats to 250 member organisations. Detective Inspector Paul Gillen, head of the Garda Computer Crime Investigation Unit, told the conference that computer perpetrated fraud was "highly organised" and the only way to deal with it is to set up a task force of IT security professionals, academics, law enforcement and a CERT "because everyone has information that could be a piece of evidence". Speakers emphasised that Government involvement was crucial in creating a national cyber security strategy and that EU states benefit from CERT's sharing information with each other.[53]

Until implementation of the Cybercrime Convention and transposition of the Council Framework Decision on attacks on information systems into domestic law, national law enforcement agencies across the Cybercrime Convention signatories, including the Irish, will combat the more complex and generally international computer crime with purely domestic tools. By analogy, this is the equivalent of engaging in a boxing match with a technically adept opponent, who knows the rules, with one arm tied behind your back and not being able to leave your corner. The chances of a knockout or even a points victory are not great.

Pearse Ryan is a partner in the Technology & Life Sciences Group at Arthur Cox, Dublin. www.arthurcox.com. **Andrew Harbison** is Director in the Forensic & Investigation Services Group at Grant Thornton, Dublin.

This article was originally published in *Computers and Law* (www.scl.org)

[53] Marco Thorbruegge, expert on CERT's within the European Network and Information Security Agency, Irish Times, December 4, 2009