http://www.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf

Summary

On Tuesday, April 10, 2012, the Ninth Circuit, in an *en banc* decision penned by Judge Kozinski, held that an employee could not be criminally liable under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") for "exceeding authorized access" to an employer's computer by accessing proprietary information in violation of the employer's written policies. In so holding, the Ninth Circuit reversed course from the initial panel decision, and entrenched its split from other circuits that have interpreted the CFAA's "exceeds authorized access" prong to cover violations of an employer's clearly disclosed computer use policy. The *Nosal* decision clarifies the Ninth Circuit's view that the CFAA targets true "hacking," and not violations of company computer use policies or website terms of service.

Background of the Case

David Nosal had worked for the executive search firm Korn/Ferry International, which he left to start a competing firm. Soon after leaving Korn/Ferry, Nosal allegedly induced three of its employees to download proprietary information about executive candidates from Korn/Ferry's password-protected database and to provide that information to Nosal. The Korn/Ferry employees in question had access to the database for work purposes, but had signed employment agreements prohibiting disclosure of the information at issue. That such disclosure violated Korn/Ferry's computer use policy was not in dispute.

Nosal was charged with an aiding and abetting violation of section 1030(a)(4) of the CFAA, which imposes criminal liability for anyone who: "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." The government alleged that, while the employees in question had permission to access the database in question for legitimate work purposes, their use of the database for a prohibited purpose exceeded their authorized access and hence put the conduct within the ambit of the CFAA. Nosal moved to dismiss the CFAA claims on the ground that the "exceeds authorized access" prong does not apply where the computer access itself was authorized, regardless of whether the ultimate use of the obtained information is authorized. The district court granted his motion, following the Ninth Circuit's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) which had held that the actions of individuals who had misused their otherwise authorized access did not constitute "access . . . without authorization."

In April of 2011, the panel reversed the district court, holding that because the computer use policy prohibited disclosure to outside parties and use other than for legitimate business purposes, the employees exceeded their authorization by violating those restrictions. The Ninth Circuit voted to hear the case *en banc,* and oral argument was held on December 15, 2011. Yesterday, the *en banc* court reached the opposite conclusion from the three-judge panel and affirmed the district court's decision dismissing the five CFAA criminal counts.

The Ninth Circuit's Decision

In affirming the district court, the *en banc* Ninth Circuit held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." This is an issue with a long history, by internet standards, that has split the circuits: the Ninth Circuit's interpretation stands in contrast to the broader view taken by the Fifth, Seventh and Eleventh Circuits.

For more than a decade, courts have wrestled with the scope of the terms "authorization" and "access." The issue boils down to whether a violation of conditions on computer access can negate the authorization that was otherwise in

effect, and render the access unauthorized or in excess of authorization. This issue often arises in circumstances similar to *Nosal* (for example, where an employee has clearance to use the employer's computers information for legitimate company business, but instead does so for an unauthorized purpose), but occassionally arises in other situations as well. Notably, courts have addressed similar questions in cases where a website user obtained authorized access to a site, but then uses the site in violation of the site's terms of use. Recognizing the distinction between authorized *access* and authorized *use*, the Ninth Circuit has now clarified that the CFAA is not triggered where there is merely unauthorized *use* of information from a computer—the access itself must have been without or in excess of authorization. Thus, under *Nosal*, if a business wants to protect its sensitive information, it must either limit *access* to that information, or, rely on legal remedies other than the CFAA.

The *Nosal* opinion expresses grave concern that the broad reading of the statutory phrase "exceeds authorized access" advocated by the government could criminalize violations of private use policies generally. In particular, the Court notes that the phrase "exceeds authorized access" appears in another section of the CFAA, § 1030(a)(2)(C), which does not contain any requirement of fraudulent purpose, and requires only that the person who "exceeds authorized access" has "obtain[ed] . . . information from any protected computer." As this provision encompasses any computer involved in interstate commerce (i.e. that can connect to the Internet), a reading that finds a violation of company policy exceeds authorized access could "make every violation of a private computer use policy a federal crime."

Judge Kozinski notes the ubiquity of transgressions of computer use policies, wryly observing that the universe of those who use a computer in violation of computer use restrictions "may well include everyone who uses a computer." The Court reasoned that the narrow interpretation advanced by Nosal, requiring that the access itself must be unauthorized, comports with Congress's legislative intent to criminalize computer hacking and was inherently more plausible than the broad interpretation proposed by the government. The latter reading, that allows unauthorized use to satisfy the CFAA's unauthorized access prong, would "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." Judge Kozinski colorfully cautioned, "Under the government's proposed interpretation of the CFAA . . . describing yourself [on a dating website] as 'tall, dark, and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."

The opinion concludes by recognizing that the Ninth Circuit is at odds with the Fifth, Seventh, and Eleventh Circuits, each of which adopted broader interpretations of the CFAA's authorization requirement. Judge Kozinski appears to be quite deliberate in laying the groundwork for the Supreme Court to review the Ninth Circuit's decision and resolve this circuit split.

Judge Silverman dissented, joined by Judge Tallman. The dissent emphasizes the knowing and intentional fraud committed by Nosal and his confederates—a very different situation than the "innocuous violations of office policy" invoked by the majority opinion. Under the dissent's view, the language and logic of the statute apply to a person who is authorized to access a computer for some purposes, but who uses the access for other purposes. The dissent takes issue with the majority's "laundry list of wacky hypotheticals," in part because the conduct at issue in the present case is so clearly wrongful. The dissent sees no need to consider the ramifications of its interpretation of the CFAA on less culpable actors because other elements of the crime—intent to defraud, furthering the fraud, and obtaining something of value—limit the statute's application to innocent workplace conduct. In the unlikely event that reading ESPN.com at work subjected an employee to criminal sanctions, Judge Silverman concludes "well, . . . that is what an as-applied challenge is for."

Implications

The *Nosal* opinion clarifies and preserves the status quo. The Ninth Circuit had already adopted a narrow interpretation of the access prong of the CFAA in *LVRC Holdings LLC v. Brekka*. *Brekka* addressed the term "without authorization," and found that the element could not be satisfied by a violation of a use restriction, but it left open to debate whether the term "exceeds authorized access" could be met by breach

of use restrictions. Since *Brekka,* most district courts in this circuit have not allowed CFAA cases to proceed based only on violations of use restrictions, although the issue was heavily litigated. Now, in the Ninth Circuit, that issue is closed. In other circuits, however, contractual use restrictions remain enforceable through the CFAA.

The specific implications of this decision vary depending on the context of the contractual use restriction:

Employment Agreements—Companies have been recently adopting a variety of technology acceptable use and data security policies, or adding contractual restrictions on the use of confidential data in employment agreements. Under *Nosal*, those policies and agreements are not valid bases for bringing a CFAA claim against an employee. They are, however, still useful for CFAA litigation outside the Ninth Circuit and for raising breach of contract, trade secret misappropriation, and related state law claims. As these alternative causes of action are based on state law, the main effect of today's decision is to foreclose the possibility of suing a former employee in *federal* district court in the Ninth Circuit on CFAA grounds.

Website Terms of Use—Companies have had variable success in enforcing their website terms of service under the CFAA. Under the CFAA, some companies have attempted to enforce their terms of service offensively—to sue a consumer for violating specific provisions. In most instances, the "consumer" was in fact a competitor that was scraping data from the company's website. For example, in *Facebook v. Power.com*, No. 10-cv-02389-JW (N.D. Cal.), Facebook sued Power.com for scraping data about Facebook users' friends in violation of Facebook's terms of service.

The holding in *Nosal* makes it unlikely a lower court will permit a company to bring a CFAA claim against a competitor for violating the company's terms of service alone. The district court in *Power.com* had reached the same conclusion, holding Power.com could only be liable under the CFAA if it had circumvented "technical barriers." *Nosal* comes close to adopting this position, noting the "general purpose" of the CFAA is to "punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets." The Ninth Circuit, however, does not explicitly adopt a "technical barriers" standard.

The range of technical barriers, however, is currently unexplored. In *Power.com*, the district court held IP blocking was a technical barrier and that Power.com circumvented that barrier by accessing Facebook's website from a different IP address. This suggests that technical barriers do not need to be robust or sophisticated to trigger CFAA liability. *Nosal* will undoubtedly put pressure on companies to examine what technical barriers are in place to bar competitors from scraping their public websites or gaining access to restricted customer sites.

Privacy Policies—Plaintiffs' lawyers have recently filed a spate of class action lawsuits pleading the CFAA as a cause of action against technology companies that collect and distribute demographic information in alleged excess of what consumers "authorize" when agreeing to the companies' privacy policies. Under *Nosal*, consumers can no longer plead a CFAA cause of action under the theory that each consumer allowed a company to access their personally identifiable information, but did not authorize the company to disclose that information to third party advertisers. To date, many of these class actions have been filed in the Northern District of California; *Nosal* may push Plaintiffs' lawyers to file future privacy class actions in districts outside the Ninth Circuit.

The Supreme Court has yet to address the CFAA, but *Nosal* substantially increases the likelihood that the high court will intervene to resolve this ongoing circuit split.

For further information, please contact:

Ilana S. Rubel, Partner, Litigation Group
irubel@fenwick.com, 650.335.7208

Sebastian E. Kaplan, Associate, Litigation Group
skaplan@fenwick.com, 415.875.2477

Erin Simon, Associate, Litigation Group
esimon@fenwick.com, 650.335.7140

©2012 Fenwick & West LLP. All Rights Reserved.

THE VIEWS EXPRESSED IN THIS PUBLICATION ARE SOLELY THOSE OF THE AUTHOR, AND DO NOT NECESSARILY REFLECT THE VIEWS OF FENWICK & WEST LLP OR ITS CLIENTS. THE CONTENT OF THE PUBLICATION ("CONTENT") IS NOT OFFERED AS LEGAL SHOULD NOT BE REGARDED AS ADVERTISING, SOLICITATION, LEGAL ADVICE OR ANY OTHER ADVICE ON ANY PARTICULAR MATTER. THE PUBLICATION OF ANY CONTENT IS NOT INTENDED TO CREATE AND DOES NOT CONSTITUTE AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN YOU AND FENWICK & WEST LLP. YOU SHOULD NOT ACT OR REFRAIN FROM ACTING ON THE BASIS OF ANY CONTENT INCLUDED IN THE PUBLICATION WITHOUT SEEKING THE APPROPRIATE LEGAL OR PROFESSIONAL ADVICE ON THE PARTICULAR FACTS AND CIRCUMSTANCES AT ISSUE.