The Coverage Inkwell

Emerging Coverage Issues in Intellectual Property, Privacy, and Cyber Liability

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

April 13, 2012

The Computer Fraud and Abuse Act Prohibits Unauthorized Access, Not Use (or the Ninth Circuit Really Likes ESPN.Com and Online Sudoku at Work)

The other day, I stumbled upon a new touchstone of getting old. In a moment of cheek with my tween son, I said "I want my MTV." All I got in return was a blank stare. Well, for those who want their ESPN.com and online Sudoku in the workplace (please, no more blank stares), the Ninth Circuit understood (well, sort of), and used such online activities to buttress a decision it issued this week on the scope of the Computer Fraud and Abuse Act (CFAA), 28 U.S.C. § 1030.

In 1984, Congress enacted the CFAA to address the then-growing problem of computer hacking. It is the central piece used by civil litigants and federal prosecutors in the statutory framework prohibiting computer hacking, the use of viruses and malware, and the unauthorized access of material in private databases, including trade secrets and personal identifiable information, such as mailing addresses and social security numbers.

In its essence, the CFAA creates civil and criminal liability for anyone who accesses a protected computer without authorization which—for civil liability—results in certain harm. A divide, however, has developed over the statute's meaning of access without authorization. Does the statute only prohibit a user from accessing a computer (or computer file) to which he or she is not authorized to access? Or does it also prohibit a user, who otherwise is authorized to access a computer, to use the computer or information contained therein in a manner that is not authorized and is improper? The difference between the two meanings can be stark.

This week, the issue was addressed in *United States v. Nosal*, --- F.3d ---, 2012 WL 1176119 (9th Cir. Apr. 10, 2012) (en banc). There, the Ninth Circuit held that the phrase "exceeds authorized access," as defined in the CFAA, is limited to "violations of restrictions on access to information, and not restrictions on its use." *Id.* at *8 (emphasis in original). Notably, the *Nosal* court rejected the reasoning of other U.S. Courts of Appeals when it rendered its decision and relied upon a parade of horribles to justify it. Although *Nosal* is a criminal case, the case will have a direct effect on civil liability for computer hacking, use of spyware, and other digital trespass claims. The decision can play an important role for evaluating coverage under a CFAA claim, as well as exposure to potential liability.

Defendant David Nosal worked for Korn/Ferry, an executive search firm. Shortly after Nosal left Korn/Ferry, Nosal convinced some of his former colleagues at Korn/Ferry to help him start a competing business. The employees used their company log-in credentials to download source lists, names, and contact information from a confidential database on Korn/Ferry's computer. They then transferred the confidential information to Nosal. *Id.* at *1. The employees were authorized to access the database, but Korn/Ferry policy forbade the disclosure of the confidential information, especially to a competitor. *Id.*

The U.S. government indicted Nosal on 20 counts, including theft of trade secret, mail fraud, conspiracy, as well as violation of the CFAA under 18 U.S.C. § 1030(a)(4) for aiding and abetting the Korn/Ferry employees in "exceed[ing their] authorized access" with intent to defraud. Nosal moved to dismiss the CFAA counts, arguing that the statute targets only hackers, not individuals who access a computer with authorization but then misuse the information they obtain. *Id.* The district court ultimately granted Nosal's motion and dismissed the counts. The government appealed, and the Ninth Circuit affirmed. *Id.*

18 U.S.C. § 1030(a)(4) provides:

> (a) Whoever—
>
> (4) 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 ...
>
> shall be punished.... [Emphasis added.]

"Exceeds authorized access" means:

> to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

18 U.S.C. § 1030(e)(6) (emphasis added).

The Court acknowledged that the definition for "exceeds authorized access" could be read in two ways: either to prohibit only the access of unauthorized computer files, or also to prohibit the unauthorized use of information to which the defendant had access to:

> First, as Nosal suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data; he would "exceed[ ] authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a

> computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor.

Id. at *1.

The government argued that the word "entitled" in the definition for "exceeds authorized access" meant that because Korn/Ferry's computer-use policy gave employees only certain rights, when the employees violated the policy, they "exceed[ed] authorized access" under the CFAA. *Id.* at *2. The Court disagreed, reasoning that the word "entitled" in the statute's text referred to "how an accesser 'obtain[s] or alter[s]' the information, whereas the computer-use policy uses 'entitled' to limit how the information is used after it is obtained." *Id.* (emphasis added). The Court also concluded that an "equally or more sensible reading of 'entitled' is as a synonym for 'authorized.' So read, 'exceeds authorized access' would refer to data or files on a computer that one is not authorized to access." *Id.*

The government also argued that the word "so" meant "in that manner," which it claimed must refer to use restrictions. "In the government's view, reading the definition narrowly would render 'so' superfluous." *Id.* at *2. The Court rejected this argument as well, stating that the government's interpretation placed undue weight "on a two-letter word that is essentially a conjunction" and would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* The Court concluded that if Congress intended to expand the scope of criminal liability "to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose." *Id.* Thereafter, the Court emphasized its point with a parade of horrible, including use of ESPN.com and online Sudoku.

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you could be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. [Emphasis added.]
>
> * * *
>
> Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And Sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work

> computers might give them more than enough time to hone their Sudoku skills behind bars.

Id. at *4-5.

Notably, the Court's holding rejects the reasoning of other Circuits that have interpreted the CFAA to prohibit violations of corporate consumer-use restrictions. *See United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Rodriquez*, 628 F.3d 1258 (11th Cir. 2010); *see also EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577 (1st Cir. 2001) (holding that an employee likely exceeded his authorized access when he used that access to disclose information in violation of a confidentiality agreement); *United States v. Teague*, 646 F.3d 1119, 1121 (8th Cir. 2011) (upholding conviction under §1030(a)(2) and (c)(2)(A) where government employee used his privileged access to government database to obtain President Obama's private student loan records). Thus, a split is developing among the Circuits.

Finally, a strongly-worded dissent did not buy into the majority's logic or its use of a parade of horribles to justify the opinion's reasoning. Justice Silverman, joined by Justice Tallman, stated that the majority wrongly had parsed a "a plainly written statute" into a "a hyper-complicated" reading "that distorts the obvious intent of Congress."

> This case has nothing to do with playing Sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts. The indictment here charged that Nosal and his co-conspirators knowingly exceeded the access to a protected company computer they were given by an executive search firm that employed them; that they did so with the intent to defraud; and further, that they stole the victim's valuable proprietary information by means of that fraudulent conduct in order to profit from using it. In ridiculing scenarios not remotely presented by *this* case, the majority does a good job of knocking down straw men—far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy.
>
> The majority also takes a plainly written statute and parses it in a hyper-complicated way that distorts the obvious intent of Congress. No other circuit that has considered this statute finds the problems that the majority does.

Id. at *8.

It will be interesting to see how the *Nosal* decision affects civil and criminal prosecution under the CFAA, as well as the reaction of the other Circuits to the opinion's reasoning and whether the Supreme Court will review this case, or another addressing the same issues.

The Coverage Inkwell

Joshua A. Mooney | Counsel
1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103-7395
Direct 215.864.6345 | Fax 215.399.9613
mooneyj@whiteandwilliams.com | whiteandwilliams.com
Assistant: Dana Genovese | 215.864-6331