

Computer Fraud And Abuse Act: Finding the Line In the Sand

By **Elkan Abramowitz**
and **Barry A. Bohrer**

Recently described as the “ever expanding statute that has swallowed the Internet,” (see, Orin S. Kerr, “Congress Considers Increasing Penalties, Adding Minimum Sentences to the Computer Fraud and Abuse Act,” *The Volokh Conspiracy Blog* (May 24, 2011)), the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030, was promulgated in 1984 in order to strengthen the government’s ability to prosecute computer crimes involving national security secrets, computers belonging to the federal government, and personal financial information. Since its enactment, the CFAA has been amended numerous times, however, significantly broadening its reach. In its current incarnation — which is the subject of yet another possible amendment — the CFAA “potentially regulates every use of every computer in the United States and even many millions of computers abroad.” Orin S. Kerr, “Vagueness Challenges to the Computer Fraud and Abuse

Act,” 94 *Minn. L. Rev.* 1561 (May 2010) (detailing the legislative expansion of the CFAA).

The scope of the CFAA is the subject of an emerging split among federal courts of appeals as highlighted by a recent opinion by the U.S. Court of Appeals for the Ninth Circuit, which rejected the claim that its decision would make criminals out of millions of employees who might utilize their work computers for personal use.

ACTIVITY COVERED BY CFAA

Most of the crimes set forth in the CFAA prohibit knowingly accessing a “protected computer” — broadly defined as any computer used by a financial institution or the federal government or “which is used in or affecting interstate or foreign commerce or communication — without authorization or in excess of authorized access and then taking specified forbidden actions, such as obtaining information or damaging the computer or its data. The statute also contains a private right of action for “[a]ny person who suffers damage or loss by reason of a violation” of the statute. (See, 18 U.S.C. §§1030(a)(1)-(7), (e)(2), (g).)

Although the statute originally was designed to target computer hackers and others with the ability to “access and control high technology processes vital to our everyday lives” (H.R. Rep. 98-894 (July 24, 1984)), over the past few years, CFAA prosecutions typically have arisen in the employment context where employees are accused of stealing informa-

tion from their employers in violation of a non-compete agreement. Charges for such violations usually are brought under subsections (a)(2) or (a)(4) of the CFAA. Subsection (a)(2) prohibits intentionally accessing a computer without authorization or in excess of authorized access and thereby obtaining “information from any protected computer.” 18 U.S.C. §1030(a)(2)(C).

UNITED STATES V. NOSAL

The Ninth Circuit’s decision in *United States v. Nosal*, —F.3d—, 2011 WL 1585600 (9th Cir. April 28, 2011), illustrates the breadth of the behavior that is criminalized under the CFAA, as well as the burgeoning disagreement among federal courts as to how the statute’s provisions should be interpreted to determine when an individual acts without, or exceeds, authorization. In *Nosal*, the defendant was indicted for conspiring to violate the CFAA by obtaining trade secrets and other highly confidential proprietary information from his former employer’s computer system to start a new business. Three of David Nosal’s former co-workers, who remained employed by Korn/Ferry International, Nosal’s former employer, assisted Nosal by using their company-designated usernames and passwords to access Korn/Ferry’s servers to generate “source lists” of the company’s clients. The indictment alleged that Nosal’s co-conspirators “exceeded their authorized access” in violation of subsection (a)(4) to obtain information from the system to defraud their employer and assist Nosal.

Elkan Abramowitz is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer. He is a former chief of the criminal division in the U.S. Attorney’s Office for the Southern District of New York. **Barry A. Bohrer** is a member of Morvillo Abramowitz and was formerly chief appellate attorney and chief of the major crimes unit in the Southern District U.S. Attorney’s Office. **Gretchan R. Ohlig**, an associate of the firm, assisted in the preparation of this article.

Nosal sought dismissal of the indictment, arguing that the CFAA intended to penalize computer hacking and does not extend to employees who misappropriate information or violate contractual agreements regarding company-owned information. The district court recognized disagreement among courts on this issue, ultimately relying on an earlier Ninth Circuit decision to dismiss the counts brought under subsection (a)(4), based on a determination that “an employee does not exceed authorized access to a computer by accessing information unless the employee has no authority to access the information under *any* circumstances.” *Id.* at 1 (emphasis in original). A three-judge panel of the Ninth Circuit reversed in a 2-1 decision.

Because Nosal's former co-workers clearly were authorized to access the Korn/Ferry computers, the question was whether they exceeded their authorized access by accessing information they were entitled to hold in only limited circumstances. Korn/Ferry had communicated the confidential nature of the information by requiring all employees to execute agreements acknowledging the restricted use and disclosure of such information and marking the information “Korn/Ferry Proprietary and Confidential.” In addition, every time an employee logged onto the company's computer system, he or she was met with the notification that “[t]his computer system and information it stores and processes are the property of Korn/Ferry” and access without authority “can lead to disciplinary action or criminal prosecution.”

Nevertheless, Nosal argued that his co-conspirators could not have exceeded their authorized access because they had permission to access the computer and the information at issue. The Ninth Circuit looked first to the plain language of the CFAA, which defines “exceeds authorized access” as “access[ing] a computer without authorization and [] us[ing] such ac-

cess to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” 18 U.S.C. §1030(e) (6). The court agreed with the government's assertion that Nosal's interpretation “render[ed] superfluous the word ‘so’ in the statutory definition.” Instead, the court found that an employee exceeds authorized access when he or she uses that access to obtain or alter information in a manner other than that intended by the employer. *See, Nosal* at 4.

EMPLOYER DETERMINES ‘AUTHORIZED ACCESS’

In further support of the notion that the limits established by an employer dictate whether an employee has acted without or beyond authorized access, the court relied on its decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In *Brekka*, the defendant was sued under the CFAA's private right of action by his former employer after he e-mailed several business documents to himself before leaving his job due to a dispute regarding the defendant's purchase of an ownership interest in the business. The district court granted the defendant's motion for summary judgment, finding that the plaintiff had failed to establish that Christopher Brekka had acted “without authorization” in violation of either subsection (a)(2) or (a)(4).

On appeal, the Ninth Circuit rejected plaintiff's argument that the court should adopt the U.S. Court of Appeals for the Seventh Circuit's position that pursuant to common law agency principles, an employee loses authorization to use a computer once he acts adverse to his duty of loyalty, believing the approach created ambiguity concerning the scope of the criminal provisions of the CFAA. *See, International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Instead, in *Brekka*, the Ninth Circuit found that the employer's actions determine whether an employee is authorized to use a com-

puter, and where an employer has not rescinded the employee's access, “the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA.” *Brekka* at 1135. Because Brekka was authorized to access the computer and had not been notified by his employer of any restrictions, he would have had no way of knowing whether or when his access was unauthorized. Accordingly, the Ninth Circuit held that Brekka was authorized to use the computers and did not violate the CFAA.

In *Nosal*, the Ninth Circuit noted that unlike Brekka, the Korn/Ferry employees who assisted Nosal were on clear notice of the restrictions surrounding their access of the Korn/Ferry database. Applying the rationale underlying *Brekka*, the court concluded that Nosal's former co-workers had “exceeded authorized access” when they knowingly violated the limits set by Korn/Ferry on their computer use. Despite this conclusion, the court insisted it did not “dismiss lightly Nosal's argument that our decision will make criminals out of millions of employees who might use their work computers for personal use,” asserting that a violation of subsection (a)(4) requires more than the violation of an employer's use restrictions, but also requires the specific intent to defraud and specified causation. *See, Nosal* at 7.

As pointed out by the dissenting opinion in *Nosal*, however, the majority's opinion impacts more than just cases brought under subsection (a)(4) because the term “exceeds authorized access” appears in other provisions of the CFAA. Specifically, the dissent pointed to subsection (a)(2), which has no intent requirement and frequently is prosecuted as a misdemeanor, in opining that the majority's broad definition could mean that “any person who obtains information from any computer

connected to the [I]nternet, in violation of her employer's computer use restrictions, is guilty of a federal crime." *Nosal* at 9 (Campbell, J. dissenting).

The dissent asserted that the majority's definition would "lend itself to arbitrary enforcement" of the CFAA and render it unconstitutionally vague. Instead, the dissent believed that the phrase "exceeds authorized access" should be interpreted in the context of legislative history indicating that Congress enacted the CFAA to curb computer hacking. "[U]nder the majority's interpretation of 'exceeds authorized access,' the CFAA would proscribe fraud (a standalone crime) that happens to be effectuated through the use of a computer and in violation of a computer use policy. This was not Congress's intent." *Id.* at 10.

OTHER CIRCUITS

The points raised in the dissent have been echoed by the defendant in *Nosal*, who has filed a petition for rehearing *en banc* to resolve the intra-circuit conflict on whether an employee can be held liable under the CFAA where he is permitted to use the computers, but does so in a manner that violates company policy. See, *Petition for Rehearing En Banc, United States v. Nosal*, No. 10-10038 (9th Cir. June 13, 2011).

The conflict is not limited to the Ninth Circuit, however. As noted in *Brekka*, in *International Airport Centers*, the Seventh Circuit has taken the unique position of looking to the law of agency to find that an employee is "without authorization" under the CFAA once he breaches his duty of loyalty to his employer.

There also is an intra-circuit split within the U.S. Court of Appeals for the Second Circuit on the issue, though it has arisen in the civil context. In *Orbit One Communications Inc. v. Numerex Corp.*, 692 F.Supp.2d 373 (S.D.N.Y. 2010), Southern District of New York Judge Lewis A. Kaplan considered CFAA claims brought by

a corporation against former employees alleging that the employees intentionally accessed the company's computer system and downloaded and removed confidential and proprietary information. The employees moved for summary judgment, maintaining that an action cannot be brought under the CFAA where employees access their employer's information "in the ordinary course of their duties."

Judge Kaplan noted that district courts within the Second Circuit had interpreted the authorization provisions of the CFAA two different ways. While one court adopted the view that an employee is liable under the CFAA once he acts contrary to his employer's interests (see, *Calyon v. Mizuho Sec. USA Inc.*, 2007 WL 2618658 at 1 (S.D.N.Y. July 24, 2007) (employee acting without or in excess of authorization where accesses documents on a computer system that employee "had to know was in contravention of the wishes and interests of his employer"), another held that the CFAA's prohibition against improper "access" does not include an employee's misuse or misappropriation of lawfully obtained information belonging to the employer. See, *Jet One Group v. Halcyon Jet Holdings Inc.*, 2009 WL 2524864 at 6 (E.D.N.Y. Aug. 14, 2009) ("It is simply not appropriate to 'expand' the CFAA in a manner not consistent with the statute's plain meaning, and, in so doing, transform what has always been a common law civil tort (*i.e.*, misappropriation of confidential information) into a federal criminal offense"). Judge Kaplan held that the more narrow interpretation should be adopted, finding that the text and legislative history of the CFAA supported the position that while "[t]he CFAA expressly prohibits improper 'access' of computer information ... [i]t does not prohibit misuse or misappropriation."

Further, the court observed that the CFAA's definitions of "damages" as "any impairment to the integrity or availability of data, a program, a system, or in-

formation" and "losses" as the cost of responding to an offense, restoring the computer equipment and programs, and any revenue lost as a result of service interruption, were consistent with the view that the CFAA was meant to prohibit computer hacking rather than employee misappropriation of information. Judge Kaplan implied that the Second Circuit would take a similar position, noting that it previously had upheld a district court decision that a plaintiff could not recover under the CFAA revenue lost "as a result of defendants' ability to unfairly compete for business' where the defendants misappropriated the plaintiff's proprietary information." *Orbit One* at 386 (citing *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F.Supp.2d 468, 477 (S.D.N.Y. 2004), *aff'd*, 166 Fed. Appx. 559 (2d Cir. 2006)).

CONCLUSION

In May 2011, the White House released a legislative proposal calling for an increase in the penalties associated with the crimes set forth in the CFAA and for the inclusion of CFAA offenses in the definition of "racketeering activity" under the RICO statute. See, White House, "Cybersecurity Legislative Proposal" (May 12, 2011) (available at www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf).

Clearly, the federal government perceives the CFAA as a means of addressing much more than the types of "computer hacking" originally contemplated in 1984, a pattern evidenced by the breadth of the behavior prosecutors have targeted under the statute. The Ninth Circuit's decision in *Nosal* may highlight for the Supreme Court the issue of whether the CFAA has been expanded beyond its original purpose — or even constitutional recognition.