New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 248—NO. 45
TUESDAY, SEPTEMBER 4, 2012

WHITE-COLLAR CRIME

Expert Analysis

Different Strokes: Interpreting Computer Fraud and Abuse Act

By **Elkan Abramowitz**

And **Barry A. Bohrer**

Originally enacted in 1984 to address the growing problem of computer hacking, the Computer Fraud and Abuse Act has been used to prosecute a wide variety of behavior, such as the violation of a non-compete agreement by a former employee, the leak of classified government materials, and cyber-bullying. The perceived breadth of activities prohibited by the CFAA is staggering and, as previously suggested by the authors, may not be constitutional.[1] The courts have had a lot to say about this topic, and recent congressional action indicates a belief that the reach of the statute is overbroad. The Justice Department does not agree.

The CFAA proscribes the knowing access of a computer used in or affecting interstate or foreign commerce or communication without authorization or in excess of authorized access.[2] The statute provides that the term "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."[3] The exact meaning of this definition has arisen in recent CFAA prosecutions targeting individuals alleged to have violated an employer's computer use policy or website or Internet service provider policies in the use of a computer.

Employment Cases

The existence of an inter-circuit split in CFAA employment cases brought against employees alleged to have misappropriated information from an employer's computer has been widely publicized. The Fifth, Seventh, and Eleventh circuits have adopted a broad interpretation of the statute, finding that an individual accesses a computer "without authorization" or in excess of his authority when the employee acquires an interest adverse to his employer or breaches a duty of loyalty owed to an employer.[4] The Ninth and Fourth circuits and numerous district courts, including district courts within the Second Circuit, have adopted a narrower reading, finding that the CFAA addresses only improper access, not an employee's misuse or misappropriation of information.[5] The issue seemingly was primed for the Supreme Court to resolve this term, but earlier this month the Justice Department opted not to seek certiorari.[6]

'United States v. Nosal'

The Justice Department declined to seek review of an en banc opinion of the U.S. Court of Appeals for the Ninth Circuit. The court rejected the government's argument that the CFAA should be read to incorporate corporate policies governing use of information. The court opined that such a reading would transform the anti-hacking statute into "an expansive misappropriation statute."[7] The defendant, David Nosal, was indicted for conspiring with three former coworkers to obtain information from his former employer's computer system to start a new business. The indictment alleged that Nosal's coconspirators "exceeded their authorized access" in violation of the CFAA to obtain information from the system and defraud their employer.

The court declined to read the statute to encompass the employees' violation of their employer's computer use policy, noting that contrary decisions from sister circuits examined only the culpable behavior of the individual before them and "failed to consider the effect on millions of ordinary citizens."[8] Instead, the Ninth Circuit opined that because the CFAA's broadest provision makes it a crime to exceed authorized access of a computer connected to the Internet without any culpable intent, the government's construction "would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."

For instance, the court observed that using a work computer to surf the Internet or chat with friends—activities routinely prohibited by corporate computer use policies—would be a federal crime. The court distinguished between employees who call family members from work versus those who send an email and employees who read the sports section of a newspaper at work versus those who look up sports scores online, opining that otherwise innocuous behavior would be converted into a federal crime simply because it involved a computer. Although the court found it unlikely that employees would be prosecuted for "such minor dalliances," it noted that employers could use the possibility of prosecution to rid themselves of troublesome employees without following established procedures. "Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement."[9]

The court further noted that employee-employer and company-consumer relationships typically are governed by tort and contract law and that private parties should not be permitted to use the CFAA to turn these relationships into ones policed by the criminal law. The government's assurances that it would not prosecute minor violations did little to persuade the court, which observed that "we shouldn't have to live at the mercy of our local prosecutor."

Fourth Circuit Decision

The U.S. Court of Appeals for the Fourth Circuit is the most recent circuit court to consider the issue, addressing the application of the CFAA in a civil case,[10] in which an employer sued a former employee for downloading and using the employer's proprietary information for use in soliciting business on behalf of a competitor company. The company alleged nine state law claims against its former employee but brought its case in federal court based on the single CFAA claim. The district court held that plaintiff failed to state a claim under the CFAA and declined to exercise jurisdiction over the remaining state law claims.

On review, the Fourth Circuit adopted the narrow reading of the terms "without

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 currently a litigation partner at Schulte Roth & Zabel 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 attorney, assisted in the preparation of this article.*

authorization" and "exceeds authorized access" to find that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.[11] The court found that the plain meaning of the statute, the rule of lenity (which dictates that ambiguities in criminal statutes be read in favor of the defendant), legislative history, and congressional intent all supported such a finding.

"Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy. Providing such recourse not only is unnecessary, given that other legal remedies exist for these grievances, but also is violative of the Supreme Court's counsel to construe criminal statutes strictly."[12] This decision, issued on the heels of *Nosal*, may confirm some momentum in the courts toward the narrow reading of the statute. Given that the decision was handed down before the Justice Department's petition for a writ of certiorari was due in *Nosal*, one can reasonably infer that it may have played a part in the government's decision not to seek Supreme Court review.

Violation of Terms of Use

In *United States v. Drew,* the U.S. District Court for the Central District of California addressed the question of whether a computer user's intentional violation of one or more provisions in a website's terms of service satisfies the "without authorization" or "exceeds authorized access" element of claims brought under the CFAA.[13] Lori Drew was charged with conspiracy to commit the tortious act of intentional infliction of emotional distress and three counts of violating the felony provision of the CFAA when she set up a fictitious profile of a 16-year-old boy on MySpace for the purpose of bullying her daughter's 13-year-old classmate. Through the MySpace account, Drew—as the fictitious teenage boy—posted a message to the girl saying that he did not like her and that "the world would be a better place without her in it." The girl subsequently committed suicide, after which Drew had the account deleted.

Although Drew was acquitted of the felony CFAA charges, she was found guilty of three CFAA misdemeanor crimes for violating the MySpace terms of service and privacy policy.[14] On the defendant's motion, the court acquitted her on this charge as well. The court noted that although a website's terms of service could define what is or is not authorized access, the use of those terms as a basis for a CFAA violation would essentially allow website owners to define criminal conduct. "[I]f any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that [the CFAA] becomes a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].'"[15]

Congressional Action

Senator Patrick Leahy (D-Vt) has introduced an amendment to the CFAA that includes what has been referred to as a "statutory fix" to the division among courts about the meaning of authorized access. This amendment adopts the narrow view endorsed by the Ninth and Fourth circuits, providing that a CFAA action may not be brought where the sole basis for determining unauthorized access to a computer is an alleged violation of an "acceptable use policy or terms of service agreement with an Internet service provider, Internet website, or non-government employer."

> The Fourth Circuit adopted the narrow reading of the terms "without authorization" and "exceeds authorized access" to find that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.

Congressional effort in this regard is not altogether surprising. Originally, the CFAA defined "exceeds authorized access" as occurring when an individual, "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." In 1986, that language was removed and replaced with the current definition. According to legislative history, that original broader language was replaced to "remove[] from the sweep of the statute one of the murkier grounds of liability, under which a[n]…employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances."[16] The recent proposed amendment would cement congressional intent in this regard.

In September 2011, this proposed change was supported unanimously by the Senate Judiciary Committee and also has been endorsed "across the philosophical spectrum."[17] The Justice Department opposes this portion of the proposed amendment, however, while endorsing those sections of the amendment that increase the penalty provisions of the CFAA. Indeed, such an amendment to the CFAA would impact current prosecutions, including the current court-martial case brought against U.S. Army Private First Class Bradley Manning, who is accused of providing large amounts of classified materials and diplomatic cables to the whistleblower website Wikileaks without breaking into any computer to obtain the information.[18]

Conclusion

One is left to wonder why the Justice Department so vehemently objects to the "statutory fix." As noted by both the Fourth and Ninth circuits, prosecutors and private individuals can pursue a number of alternative charges or causes of action in seeking remedies for the type of activity currently alleged under the CFAA. Indeed, in most cases, these charges are brought alongside the CFAA claim. Nosal's trial on conspiracy, trade secret theft, and mail fraud is set to begin this fall. If the amendment is not adopted, attorneys on both sides will have to weigh the risk of seeking Supreme Court review.

1. Elkan Abramowitz and Barry A. Bohrer, "Computer Fraud and Abuse Act: Finding the Line in the Sand," NYLJ (July 5, 2011).
2. 18 U.S.C. §1030 et seq.
3. Id. §1030(e)(6).
4. *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), cert. denied, 131 S.Ct. 2166; *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).
5. *WEC Carolina Energy Solutions v. Miller*, __F.3d__, 2012 WL 3039213 (4th Cir. July 26, 2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *Orbit One Communications v. Numerex*, 692 F.Supp.2d 373 (S.D.N.Y. 2010); *Condux International v. Haugum*, 2008 WL 5244818 (D.Minn. Dec. 15, 2008).
6. Motion for Issuance of the Mandate, *United States v. Nosal*, No. 10-10038 (9th Cir. Aug. 2, 2012).
7. 676 F.3d at 857.
8. Id. at 862.
9. Id. at 860.
10. Because the CFAA provides for a private right of action, cases brought in the civil context also have an impact in the criminal context. 18 U.S.C. §1030(g).
11. 2012 WL 3039213 at *6.
12. Id. at *7.
13. 259 F.R.D. 449 (C.D.Cal. 2009).
14. The conspiracy count was dismissed without prejudice at the government's request.
15. Id. at 467.
16. S. Rep. No. 99-432 at 21.
17. Greg Nojeim and Jake Laperruque, "Why Fibbing About Your Age is Relevant to the Cybersecurity Bill," Center for Democracy and Technology Website (July 30, 2012).
18. David Kravets, "DOJ Won't Ask Supreme Court to Review Hacking Case," Wired.com (Aug. 10, 2012).