The Florida Bar
www.floridabar.org

Search: Go

The Florida Bar Journal
Advertising Rates • Submission Guidelines • Archives • Subscribe • *News*

January, 2013 Volume 87, No. 1 Journal HOME

Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, But Illegal in Miami, Dallas, Chicago, and Boston

by Robert C. Kain

Page 36

The Federal Computer Fraud and Abuse Act, 18 U.S.C. §1030 (CFAA), criminalizes certain computer-related behavior and, if the damage exceeds $5,000 over a single year, provides a civil remedy for its victims. The Ninth Circuit in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), recently held that the CFAA does not cover an employee-hacker or an insider that takes data and uses it in an anticompetitive manner after leaving the company. Three months later, the Fourth Circuit agreed in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012)(after resigning, the ex-employee used the data in an anti-competitive manner)[1] and held that the CFAA is not violated unless an employee lacks *any* authorization to obtain or alter the data when he or she was employed.

In contrast, the First, Fifth, Seventh, and 11th circuits take the opposite view and support the concept that an employee-hacker violates the CFAA whether he or she uses the data with or without financial gain.[2] The Ninth Circuit's analysis in *Nosal* is compelling and the Fourth Circuit followed suit. *Nosal* held that the CFAA covers "hackers" but not corporate insiders, employees, or consultants, called herein "employee-hackers," who improperly use computer data. *WEC*, citing the canon of strict construction of criminal statutes (the rule of lenity), held the CFAA "simply criminalize[s] obtaining or altering information that an individual lacked authorization to obtain or alter."[3] The court also rejected a cessation-of-agency theory, effectively holding that any employee's authorized access continues throughout the employment.[4] This article discusses the divisions between the courts.[5]

The split in the circuits involves the question: What does "exceed[] authorized access" mean? The points raised by the *Nosal* and *WEC* courts are persuasive and the split in authority is not easily rectified.

Florida-based businesses rely upon the CFAA for relief because Florida's Computer Crimes Act, §815.01, *et seq.*, provides a relatively hollow civil action. An injured party "may bring a civil action against any person convicted"[6] under the act. Therefore, a criminal conviction must precede the civil action. Civil actions following a criminal conviction are not an effective enforcement mechanism. When concurrent criminal and civil actions are pending, defendants stymie civil action discovery and hence delay trial by asserting their Fifth Amendment privilege against self-incrimination. Also, the employee-hacker may exhaust his or her monetary resources in the criminal action. Therefore, Florida-based businesses often rely upon the federal act for relief.

Nosal — Ninth Circuit

The Ninth Circuit in *Nosal*, narrowly construed the CFAA finding that the criminal prosecution of an ex-employee, who convinced current employees to access and transfer employer's customer data to him, did not violate the CFAA because "exceeds authorized access" does not cover unauthorized disclosure or use of information, contrary to company policy. The *Nosal* majority stated that the purpose of the statute "is to punish hacking — the circumvention of technological access barriers — not misappropriation of trade secrets."[7] The government argued that the CFAA covers hacking and also prohibits employees and former employees from accessing and using data from an employer's computer without authorization. The court disagreed, finding that the government's position would turn the CFAA into a sweeping Internet-policing mandate, thereby criminalizing employees who G-chat with friends, play games, shop, watch sports highlights, or post false information on Facebook or eHarmony. "Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law."[8] Interestingly, the *Nosal* court cited an earlier decision from the Middle District of Florida, *Lee v. PMSI, Inc.*, No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011),[9] wherein the district court dismissed an employer's CFAA counterclaim in an employment discrimination action.

The *Nosal* court indicated that if criminal liability turns on the vagaries of an employee-employer contract, or a company-consumer contract, then a "notice" issue arises as to 1) the meaning of ambiguous terms; 2) the changeable nature of the contracts; and 3) the scope of "lengthy, opaque, [contracts which are] subject to change and [are] seldom read."[10] Per the court, when an employee can use his or her cell phone to do the same thing, it is unjust to criminally punish the same activity when done on the employer's computer.

Nosal Dissent

The dissent in *Nosal* points out that the 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. 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.[11]

Defendant Nosal was charged with a CFAA §(a)(4) violation of "knowingly and with intent to defraud, accesses a protected computer without authorization ... and by means of such conduct furthers the intended fraud."[12] Therefore, the statute requires mens rea and specific intent to defraud. According to the dissent, the majority conjures up a "parade of horribles that might occur under different subsections of the CFAA, such as subsection (a)(2)(C), which does not have the scienter or specific intent to defraud requirements that subsection (a)(4) has."[13] More importantly, the dissent recognizes that portions of the CFAA may be unconstitutionally vague. [14]

WEC — Fourth Circuit

The Fourth Circuit Court of Appeals in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), held that the act was not violated by an employee, who took computer data while employed by WEC in violation of corporate policy, resigned from the company, went to work for WEC's competitor, and then allegedly used WEC's data to pitch a project to a customer. The *WEC* court acknowledged that the "conclusion here[in] likely will disappoint employers hoping for a means to rein in rogue employees,"[15] indicated "that the distinction between these terms [in the CFAA] is arguably minute,"[16] stated, "we adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access,' and hold 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."[17] Further, the court "reject[ed] any interpretation that [] CFAA liability [can be predicated] on a cessation-of-agency theory."[18]

Employee Hacking Illegal in the First, Fifth, Seventh, and 11th Circuits

The 11th Circuit in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), held that access alone, without any financial gain to anyone (not to the violator or any other person), is a CFAA violation. The court rejected defendant's arguments that 1) he did not exceed his authorized access to the government's Social Security database; 2) he did not use the information to further another crime; and 3) he did not gain financially. The court said that the CFAA makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any department or agency of the United States,"[19] even if the accused party does not defraud anyone or gains financially.[20]

The Fifth Circuit in *United States v. John*, 597 F.3d 263 (5th Cir. 2010), held that an employee-hacker, an account manager at a Citigroup bank, violated the CFAA by releasing credit card data to her cohorts who incurred fraudulent charges. The court rejected the employee's argument that she was authorized to use Citigroup's computers at that time. The court analyzed the scope of the user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user and applied this "intended-use analysis" to conclude that the defendant exceeded authorized access.[21]

The First Circuit held that an employment agreement can establish the parameters of "authorized" access in *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 578-79 (1st Cir. 2001). Defendants hired a programmer to scrape EF's website for brochure material and tour codes that contained pricing information for specific tourist travel tours by sending more than 30,000 inquiries to the EF website, and downloading over 60,000 lines of data.[22]

The Seventh Circuit in *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), found that the CFAA was violated when an employee-hacker took his employer's target marketing data for corporate mergers, resigned, and then used the data in an anti-competitive manner. The company provided the defendant with a laptop that he used to compile data on corporate acquisition targets. He then quit the company, went into business by himself, breached his employment contract, deleted all the data from the laptop, loaded a secure-erasure program onto the laptop, and then gave the laptop back to the company. The company had no copies of the erased files.

Key CFAA Violations

The CFAA is a moderately complex statute establishing criminal and civil violations for a wide variety of acts. Unauthorized "access" to data is a violation, at least in some jurisdictions, without regard to the subsequent "misuse" of data. With respect to employee-hackers, one key inquiry is whether the employee properly accessed the computer data or program.[23] The CFAA defines "exceeds authorized access" as "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."[24] Various violations of the CFAA are described below.

• *Broad Scope Access Violations* — There are three "access violations" in the CFAA. A §(a)(2)(C) violation involving: "intentionally access[ing] a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer if the conduct involved an interstate or foreign communication;"[25] a §(a)(5)(B) violation for "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly causes damage;"[26] and a §(a)(5)(C) violation for "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, intentionally causes damage." [27]

• *Fraud Violations* — Fraud-based violations of the act include a §(a)(4) violation of "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period"[28] and a §(a)(6) violation of "knowingly and with intent to defraud traffic[ing] ... in any password."[29]

• *Computers and Miscellaneous Violations* — When the CFAA was initially enacted, Congress was concerned about the interstate commerce scope of the act. Therefore, the act broadly defines a "protected computer" which includes government computers, financial institutions, and private computers that affect "interstate or foreign commerce or communication of the United States."[30] Other access or data transfer violations involve national defense or foreign relations data;[31] financial records, credit reporting agency records or data;[32] U.S. department or agency data;[33] data from any nonpublic computer of any U.S. department or agency;[34] transmission of a program, data, or code which causes damage to a protected computer;[35] or the extortion of money or other item of value by threat to cause damage to a protected computer.[36]

• *Civil Liability* — Civil liability attaches when a person suffers damage from a violation of the CFAA and satisfies at least one of five statutory conditions.[37] The defendant must engage in one of the following: 1) loss in any one year aggregating at least $5,000 in value; 2) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of another; 3) physical injury to any person; 4) a threat to public health or safety; or 5) damage affecting a computer used by or for an entity of the U.S. government in furtherance of the administration of justice, national defense, or national security.[38] Typically, the basis for a CFAA civil action is the first statutory condition, a loss exceeding $5,000.

• *Criminal Versus Civil Statutes* — One problem associated with civil enforcement of the CFAA is that criminal statutes are construed narrowly and all terms are construed consistently in both criminal and civil actions. The *Nosal* court used this distinction to distance itself from the above-cited decisions by stating that the other circuits "failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid 'making criminal law in Congress's stead.'"[39] Statutes criminalizing the access, theft, and misuse of intellectual property have been narrowed under the rule of lenity because, given a choice between two constructs, the courts choose the more lenient version.[40]

The *WEC* court, similar to *Nosal*, narrowly construed the CFAA due to the criminal nature of the statute. "Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the more obliging route."[41] Further, both *Nosal* and *WEC* indicated that the CFAA does not criminalize misuse of data. The *Nosal* court stated that the CFAA does not cover the misappropriation of computer data.[42] The WEC court acknowledged that the defendant employee Miller may have misappropriated information, but stated that he "did not access a computer without authorization or exceed their authorized access."[43]

Conclusion

The stage is set for an appeal to the Supreme Court on the scope of the CFAA as it relates to employee-hackers and what is the meaning of "authorized access" in the phrase "exceeds authorized access." Is the authorization a matter of timing (a temporal condition) or "intended-use" or keyed to a cessation-of-agency theory? Does "exceed authorized access" incorporate the concept that a subsequent misuse of data causes one to "exceed authorized access?" For Florida-based businesses, the Florida Computer Crimes Act provides a hollow remedy and, therefore, Florida employers now rely upon the CFAA. That reliance may be short lived since the Ninth and the Fourth circuits believe that the CFAA, as it applies to employee-hackers, is unconstitutionally vague.

[1] *See also Lee v. PMSI, Inc.*, No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011).

[2] *See United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (employee-hacker violated statute even though he never used the data for financial gain); *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (after resigning, the ex-employee used the data in an anticompetitive manner and violated the act); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 578-79 (1st Cir. 2001) (an employment agreement establishes the parameters of unauthorized access); and *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (employee-hacker violated statute even though she rightfully had access to the computer data, but then gave the data to cohorts who incurred fraudulent credit card charges).

[3] *Nosal,* 676 F.3d at 206.

[4] *Id.*

[5] The Florida Bar's Computer Law Committee and Intellectual Property Committee has established a task force to study the employee-hacker problem and, if appropriate, suggest legislative action through the Bar's Business Law Section. The author is chairperson of the task force.

[6] Fla. Stat. §815.06 states: "(4)(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages. (b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party."

[7] *Nosal,* 676 F. 3d at 863.

[8] *Id.* at 860.

[9] In *Lee*, the court dismissed an employer's counterclaim under the CFAA notwithstanding the fact that the plaintiff employee made personal use of the Internet at work by checking Facebook and sending personal email in violation of company policy.

[10] *Nosal*, 676 F.3d at 860.

[11] *Id.* at 864.

[12] 18 U.S.C. §1030(a)(4).

[13] *Nosal*, 676 F.3d at 864.

[14] *Id.* "Other sections of the CFAA may or may not be unconstitutionally vague or pose other problems. We need to wait for an actual case or controversy to frame these issues, rather than posit a laundry list of wacky hypotheticals."

[15] *WEC,* 687 F. 3d at 207.

[16] *Id.* at 204.

[17] *Id.* at 206.

[18] *Id.*

[19] CFAA, 18 U.S.C. §1030(a)(2)(B).

[20] *Rodriguez,* 628 F. 3d at 1264.

[21] *John,* 597 F.3d at 271, *citing United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007).

[22] *EF Cultural Travel,* 274 F. 3d at 579.

[23] For purposes of this article, unauthorized access to “computer data” is synonymous with the access or misuse of a “computer program.”

[24] 18 U.S.C. §1030(e)(6).

[25] 18 U.S.C. §1030(a)(2)(C).

[26] 18 U.S.C. §1030(a)(5)(B).

[27] 18 U.S.C. §1030(a)(5)(C).

[28] 18 U.S.C. §1030(a)(4).

[29] 18 U.S.C. §1030(a)(6).

[30] 18 U.S.C. §1030(e)(2). “The term ‘protected computer’ means a computer (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.”

[31] 18 U.S.C. §1030(a)(1).

[32] 18 U.S.C. §1030(a)(2)(A).

[33] 18 U.S.C. §1030(a)(2)(B).

[34] 18 U.S.C. §1030(a)(3).

[35] 18 U.S.C. §1030(a)(5)(A).

[36] 18 U.S.C. §1030(a)(7).

[37] 18 U.S.C. §1030(g). A civil remedy is provided to “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [subclause] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.”

[38] *See* 18 U.S.C. §1030(c)(4)(A)(i)(I), (II), (III), (IV), and (V), referenced in 18 U.S.C. §1030(g).

[39] *Nosal*, 676 F.3d at 863 (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008)).

[40] *See also U.S. v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), (quoting *Rewis v. United States*, 401 U.S. 808, 812 (1971) and *United States v. Universal C.I.T. Credit Corp.*, 344 U.S. 218, 221-22 (1952). “‘[A]mbiguity

concerning the ambit of criminal statutes should be resolved in favor of lenity' and 'when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.'"

[41] *WEC,* 687 F.3d at 206, (citing *United States v. Universal C. I. T. Credit Corp.*, 344 U.S. 218, 221-22 (1952) and *Nosal*, 676 F.3d at 863).

[42] *Nosal,* 676 F.3d at 863.

[43] *WEC,* 687 F.3d at 207, *citing* 18 U.S.C. §§1030(a)(2)(C), (a)(4), and (a)(5)(B)-(C)).

***Robert C. Kain** has practiced exclusively in the patent, trademark, copyright, and computer law fields for over 30 years and is a board certified intellectual property attorney. His firm, Kain & Associates, located in Ft. Lauderdale, specializes in all phases of intellectual property law: patent, trademark, copyright, computer, Internet and trade secret law, related litigation in state and federal courts, domain disputes (ICANN) and AAA arbitration, and administrative actions before the USPTO.*

This column is submitted on behalf of the Business Law Section, Brian Keith Gart, chair, Lynn Sherman, editor.

[Revised: 12-28-2012]

Journal HOME

| Disclaimer | Top of page | PDF