DRAFT V6

Circuits Split Over Federal Computer Fraud and Abuse Act - Employee Hacking: Legal in California and Virginia But Not In Chicago, Boston, Dallas or Miami

By Robert Kain, at rkain@complexip.com

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 9th Circuit Court of Appeals recently held that the CFAA does not cover an employee-hacker or an insider that takes or destroys data. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)(en banc). Two months later, the 4th Circuit Court of Appeals agreed and held that the CFAA is not violated unless an employee lacks any authorization to obtain or alter the data. WEC Carolina Energy Solutions LLC v. Miller, Case No. 11-1201 (4th Cir. July 26, 2012). In contrast, the 1st, 5th, 7th and 11th Circuits take the opposite view and support the concept that an employee hacker does violate the CFAA. See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578-79 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); and United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

The 9th Circuit's decisional analysis in Nosal is compelling and the 4th Circuit has followed suit. The regional split cannot be ignored. Nosal held that the CFAA covers "hackers" but not corporate insiders, employees or consultants, called herein "employee hackers," who disabuse computer data. WEC, citing the canon of strict construction of criminal statutes, the so-called "rule lenity," held the CFAA "simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter." Slip opn. p. 11. Further, WEC rejected a cessation-of-agency theory, effectively holding that any employee's authorized access continues throughout the employment. Id. p. 12. This article seeks to spark a discussion over the issue of what to do with the employee hacker.

Call to Action for the I.P. and Computer Law Committee

The split in the circuits will surely result in an appeal to the Supreme Court on the issue of: 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. To fix the civil action side of the CFAA, the Committee may consider the following amendments. Comments are welcome.

Proposal A - use based, civil litigation solution

> Amend: § 1030(g) Any person ~~who~~ may maintain a civil action against a violator of this section to obtain compensatory damages and injunctive relief or other equitable relief if that person: (1) suffers damage or loss by reason of a violation of this section or (2) suffers a competitive injury, damage or loss due to unauthorized use of data, a program, a system or information 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 ...

Proposal B: Criminalize all "unauthorized use" of data:

Amend: 18 U.S.C. § 1030(e)(6): (6) 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 or to use such information in an unauthorized manner.

Florida's Computer Crimes Act, Fla.Stat. §. 815.01 et seq. provides for a relatively hollow civil action. The Act states that the injured party "may bring a civil action against any person convicted under ..." the Act. Fla.Stat. § 815.06(4)(a). Civil actions following a criminal conviction are not an effective enforcement mechanism. Therefore, Florida-based businesses must rely upon the federal act for relief.

Key CFAA Violations

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." 18 U.S.C. § 1030(e)(6). The secondary issue of what is "authorized" was the subject of a law review article in 1995 but this concept is not addressed in the present article. R. Kain, "Independent Contractors and Computer Crimes - The Impossible Prosecution?," 1 Boston U. Jour. Science and Tech. Law 13, 1995.[1]

The CFAA[2] (reproduced in the end note) is a moderately complex statute. The following excerpts are typically cited against an employee hacker.

Broad Scope Access Violations:

§ (a)(2)(C) Violation: "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... (C) information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C).

§ (a)(5)(B) Violation: "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage." 18 U.S.C. § 1030(a)(5)(B).

§ (a)(5)(C) Violation: "intentionally accesses a protected computer without authorization, and as a result of such conduct, intentionally causes damage." 18 U.S.C. § 1030(a)(5)(C).

Fraud Violations:

§ (a)(4) Violation: "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, 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." 18 U.S.C. § 1030(a)(4).

§ (a)(6) Violation: "knowingly and with intent to defraud traffics ... in any password." 18 U.S.C. § 1030(a)(6)

Violations: Accessing, Transferring Data Violations from Government or Financial Computers
18 U.S.C. § 1030(a)(1): national defense or foreign relations data
18 U.S.C. § 1030(a)(2)(A): financial records, credit reporting agency records
18 U.S.C. § 1030(a)(2)(B): U.S. department or agency data
18 U.S.C. § 1030(a)(2)(C): see above.
18 U.S.C. § 1030(a)(3): any non-public computer of any U.S. department or agency
18 U.S.C. § 1030(a)(4): see above
18 U.S.C. § 1030(a)(5)(A): transmission of a program, data or code which causes damage
18 U.S.C. § 1030(a)(5)(B): see above
18 U.S.C. § 1030(a)(5)(C): see above
18 U.S.C. § 1030(a)(6): see above
18 U.S.C. § 1030(a)(7): extort money or other value by threat to cause damage to computer

Civil Liability - Defendant Must Engage In One of the Following (see 18 U.S.C. § 1030(g)):

"(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;
(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(III) physical injury to any person;
(IV) a threat to public health or safety; or
(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(c)(4)(A)(i).

Legal In the 9th and the 4th Circuits

Earlier this year, the Ninth Circuit Court of Appeals 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 (a contractually imposed terms of use or terms of service, "TOU" or "TOS"). United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

Nosal was charged with violating § (a)(4) CFAA which prohibits: "knowingly accessing computer without authorization, or exceed[ing] authorized access to obtain anything of value in excess of $5,000.00. 18 U.S.C. § 1030(a)(4). 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." 18 U.S.C. § 1030(e)(6).

The Nosal court raised on two examples. (A) An employee, who is permitted to access only product information on the company's computer but accesses customer data, potentially "exceeds authorized access" if he looks at the customer list. (B) An employee who may be authorized to access the customer list in order to do his job but is not contractually permitted to use the entire list, would also potentially exceed authorized access by misuse of the information.

Per the Nosal court, the purpose of the statute "is to punish hacking — the circumvention of technological access barriers — not misappropriation of trade secrets".[3] Nosal, 676 F.3d at 863. The court found that the CFAA is an anti-hacking statute and not a misappropriation statute. "The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word ['so' in the CFAA] that is essentially a conjunction. If Congress meant 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." Nosal, 676 F.3d at 857.

Inside Versus Outside Hackers - the CFAA Is Not An Internet Policing Policy

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.

Per the Court, "But it is possible to read both prohibitions as applying to hackers: '[W]ithout authorization' would apply to outside hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate. The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer." Nosal, 676 F.3d at 857.

"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. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement." Nosal, 676 F.3d at 860. "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." Nosal, 676 F.3d at 860.

As further support to limit the CFAA to outside hackers, the court cited Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011), wherein 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.

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 (a) the meaning of ambiguous terms; (b) the changeable nature of the contracts; and (c) the scope of "lengthy, opaque [contracts which are], subject to change and seldom read." Nosal, 676 F.3d at 860. Also, when an employee can use his or her cell phone to get the same information from the Internet, it is unjust to criminally punish the same activity when done on the employer's computer. Nosal, 676 F.3d at 860. The court then analyzes Google's and Facebook's terms of service or terms of use and notes that the Government's statutory construction would criminalize "vast numbers of teens and pre-teens." The dating service eHarmony's TOS prohibits inaccurate or misleading information and since many adults misrepresent their attributes and faults, the proposed construction would criminalize this behavior. In the past, the Supreme Court has refused to adopt the government's broad interpretation of a statute because it would "criminalize a broad range of day-to-day activity." Nosal, 676 F.3d at 861, quoting United States v. Kozminski, 487 U.S. 931, 949 (1988).

The Court discounted other appellate court decisions contrary to its statutory construction. "We remain unpersuaded by the decisions of our sister circuits." See United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); 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). "These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access.' They therefore 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.' United States v. Santos, 553 U.S. 507, 514 (2008)." Nosal, 676 F.3d at 862-63.

The Court followed its earlier decision in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), which narrowly construed the phrases "without authorization" and "exceeds authorized access" in the CFAA. A "growing number of courts that have reached the same conclusion. These courts recognize that the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.' Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted); see also Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ('The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation.'); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) ('[A] violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted.'); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005) ('[T]he CFAA, however, do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access.')." Nosal, 676 F.3d at 863.

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." Id. at 864.

Defendant Nosal was charged with an (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." 18 U.S.C. § 1030(a)(4). The statute "is perfectly clear that a person with both the requisite mens rea and the specific intent to defraud - but only such persons - can violate this subsection in one of two ways: first, by accessing a computer without authorization, or second, by exceeding authorized access." Nosal, 676 F.3d at 864. 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 ... 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." Id.

4th Circuit - WEC Carolina Energy Solutions LLC v. Miller

The 4th Circuit Court of Appeals recently agreed with the 9th Circuit and held that the CFAA is not violated unless an employee lacks any authorization to obtain or alter the data. WEC Carolina Energy Solutions LLC v. Miller, Case No. 11-1201 (4th Cir. July 26, 2012). The 4th Circuit held

that the Act was not violated by an employee, who took computer data while employed by WEC, 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. Impressed, the customer hired WEC's competitor, thereby precipitating the federal CFAA suit with 9 other state law actions. The employee Miller moved to dismiss the CFAA count and the trial court agreed, dismissing the sole federal count and refusing to hear the ancillary state court claims. The decision in the WEC case is more compelling since it was issued two (2) months after the 9th Circuit decision in Nosal.

The WEC Court acknowledged that the "conclusion here[in] likely will disappoint employers hoping for a means to rein in rogue employees" (slip opn. P. 13), indicated that "that the distinction between these terms [in the CFAA] is arguably minute" (P. 9), stated that "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." P. 12. Further, the Court "reject[ed] any interpretation that [] CFAA liability [can be predicated] on a cessation-of-agency theory." P. 12.

The WEC Court agreed that the defendant employee Miller may have misappropriated information, but stated that "they did not access a computer without authorization or exceed their authorized access." P. 13 (citing 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), (a)(5)(B)-(C)). The decision in WEC follows-on the Nosal's Court opinion that the CFAA is an anti-hacking statute and not a misappropriation statute. The WEC Court "adopt[ed] a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and [held] 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." P. 12.

In WEC, Defendant Miller was a project manager WEC who allegedly took WEC data prior to his resignation. Shortly thereafter, Miller pitched a project to a WEC competitor, who then hired Miller's new employer. WEC's complaint alleged that Miller had access to numerous confidential and trade secret documents stored on computer servers (pricing, technical specs and pending projects) and WEC had a corporate policy that prohibited employees from using corporate information without authorization or downloading it to a personal computer. WEC alleged that Miller emailed the confidential data to his personal computer, thereby accessing the information without authorization per the corporate policy. Therefore, WEC alleged that employee Miller violated corporate policy regarding access and use of the WEC computer data.

The WEC Court, in a similar manner as the Nosal Court, was compelled to narrowly consture the CFAA due to the criminal nature of the statute. "Thus, faced with the option of two interpretations [of the term 'so'], we yield to the rule of lenity and choose the more obliging route." P. 11 (citing United States v. Universal C. I. T. Credit Corp., 344 U.S. 218, 221-22 (1952) and Nosal, 676 F.3d at 863).

Illegal in the 1st, 5th, 7th and 11th Circuits

In United States v. John, 597 F.3d 263 (5th Cir. 2010), the 5th Circuit held that an employee hacker violated the CFAA by releasing credit card data. Defendant Ms. Levon John was an account manager at a Citigroup bank. John provided her half-brother with Citibank customer account information which enabled him and other confederates to incur fraudulent charges. John accessed and printed information pertaining to at least 76 corporate customer accounts and her cohorts incurred fraudulent charges on four different accounts. John argued on appeal that she was authorized to use Citigroup's computers and that the CFAA did not prohibit unlawful use of material that she was authorized to access. The appeals court rejected that argument and held that CFAA is violated when a person uses data without authorization. "In Phillips, we recognized that '[c]ourts have . . . typically analyzed the scope of a 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.' We applied this 'intended-use analysis' to conclude that a student who used his privilege of access to a university's computer was not authorized to access parts of the system to which he had not been given a password." United States v. John, 597 F.3d 263, 271 (5th Cir. 2010)(citing United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).

The First Circuit has held that an employment agreement can establish the parameters of "authorized" access. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 578-79 (1st Cir. 2001); cited as authority in John, 597 F.3d at 272.

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. Rodriguez, a former employee of the Social Security Administration ("SSA"), appealed his conviction and argued that he did not exceed his authorized access to the SSA's database and that he did not use the information to further another crime or to gain financially. Rodriquez obtained personal identifying information, such as birth dates and home addresses, of 17 persons (his girl friend, her father and his ex-wife's sister, among others). He never used the information or otherwise disclosed it to other third parties. Per the Rodriguez court, 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." 18 U.S.C. § 1030(a)(2)(B). Therefore, even if the accused party does not defraud anyone or gains financially, the CFAA is violated.

In the 7th Circuit case of Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006), the employee-hacker took his employer's target marketing data and was found to be civilly liable under the CFAA. The defendant, Citrin, was employed by the plaintiffs IAC. IAC lent Citrin a laptop to use to record data that he collected in the course of his work identifying potential corporate acquisition targets. Citrin decided to quit IAC and go into business for himself, in breach of his employment contract. He deleted all the data from the laptop and loaded a secure-erasure program onto the computer. IAC had no copies of the files that Citrin erased.

IAC argued that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without

authorization, to a protected computer" violates the CFAA. 18 U.S.C. § 1030(a)(5)(A)(i). Citrin argued that merely erasing a file from a computer is not a "transmission." The court noted that the transmission by Citrin of the secure-erasure program to the computer caused "damage"as in defined in the CFAA as an "impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. § 1030(e)(8).

As for establishing "exceeding access," the court looked to a violation of Citrin's employment contract and a violation of the duty of loyalty that agency law imposes on an employee. The CFAA "distinguishes between 'without authorization' and 'exceeding authorized access,' 18 U.S.C. §§ 1030(a)(1), (2), (4), and, while making both punishable, defines the latter as 'accessing a computer with authorization and . . . using such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.' § 1030(e)(6). ... The difference between 'without authorization' and 'exceeding authorized access' is paper thin." Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d at 420.

Although Citrin argued that the employment contract authorized him to "return or destroy" data in the laptop when he ceased being employed, the court stated that this clause more likely was to remind Citrin that he was not to disseminate confidential data after he left the company's employ.

Criminal Statues Versus Civil Remedies

One problem associated with civil enforcement of the CFAA is that criminal statutes are construed narrowly. The Nosal Court used this distinction to distance itself from the other circuits 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.'" Nosal, 676 F.3d at 863 (quoting United States v. Santos, 553 U.S. 507, 514 (2008)). See also U.S. v. Aleynikov, 676 F.3d 71 (2d Cir. 2012), wherein the 2nd Circuit stated that "'[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.'" (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)). XX check quote.

When courts construe a statute that has both criminal and a civil remedy, the statutory terms are construed consistently in both actions.

Confusion or Conclusion

Although the majority's opinion in Nosal may be criticized for its broad brush stroke analysis and consideration of facts not within the record, the issue raised therein, the meaning and scope of "exceeds authorized access," 18 U.S.C. § 1030 (e)(6), cannot be ignored. Furthermore, the glaring split between the circuits on this issue invites a constitutional challenge to the bulk of the statute.

One solution may be to split the statute in two, one for criminal activity requiring specific mens rea, and another for civil violations based upon negligence.

1. Available online at
http://complexip.com/files/pub-IndependentContractors-computercrime.pdf.

2. 18 U.S.C. § 1030. Fraud and related activity in connection with computers

(a) Whoever--
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y.[(y)] of section 11 of the Atomic Energy Act of 1954 [42 USCS § 2014(y)], with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(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, 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;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[;]

(6) knowingly and with intent to defraud traffics (as defined in section 1029 [18 USCS § 1029]) in any password or similar information through which a computer may be accessed without authorization, if--
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [or]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--
(A) threat to cause damage to a protected computer;
(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--
(1) (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section; or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the

Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $ 5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4)[,] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;
(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--
(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--
(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;
(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(III) physical injury to any person;
(IV) a threat to public health or safety;
(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or
(VI) damage affecting 10 or more protected computers during any 1-year period; or
(ii) an attempt to commit an offense punishable under this subparagraph;
(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--
(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or
(ii) an attempt to commit an offense punishable under this subparagraph;
(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--
(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or
(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--
(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or
(ii) an attempt to commit an offense punishable under this subparagraph;
(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;
(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or
(G) a fine under this title, imprisonment for not more than 1 year, or both, for--
(i) any other offense under subsection (a)(5); or
(ii) an attempt to commit an offense punishable under this subparagraph.
(5) [Deleted]

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title [18 USCS § 3056(a)].
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(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;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934 [15 USCS § 78o];
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978 [12 USCS § 3101(1) and (3)]); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) 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;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive department enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any 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.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection [enacted Sept. 13, 1994], concerning investigations and prosecutions under subsection (a)(5).

(i) (1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--
(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and
(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.
(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:
(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.
(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section[.]

3. The Court pointed out that there is a federal trade secrets statute, 18 U.S.C. § 1832 — where Congress used the common law terms for misappropriation, including "with intent to convert," "steals," "appropriates" and "takes." See 18 U.S.C. § 1832(a), the Economic Espionage Act of 1996, which provides penalties for anyone that knowingly engages in theft of trade secrets or the attempt or conspiracy to steal trade secrets. Nosal, 676 F.3d at 857. However, there is no private cause of action under 18 U.S.C. § 1832. Pisani v. Van Iderstine, Case. No. 07-187S , 2011 U.S. Dist. LEXIS 73985 (D.R.I. June 27, 2011); Gibbs v. SLM Corp., 336 F.Supp.2d 1, 17 (D. Mass. 2004); Ryan v. Ohio Edison Co., 611 F.2d 1170, 1178-1179 (6th Cir.1979). There is also no private cause of action for mail fraud under 18 U.S.C. § 1341 or wire fraud under 18 U.S.C. § 1343. See Pisani, supra, and Vasile v. Dean Witter Reynolds Inc., 20 F.Supp.2d 465, 478 (E.D.N.Y. 1998).