The Heritage Foundation
LEADERSHIP FOR AMERICA

# LEGAL MEMORANDUM

No. 95 | JUNE 19, 2013

## Reasonably Construing the Computer Fraud and Abuse Act to Avoid Overcriminalization

*Paul J. Larkin, Jr.*

**Abstract**

*The federal government has a legitimate interest in protecting classified information and financial data. This interest, however, does not extend to using the criminal law to prohibit employees' occasional use of work computers for personal purposes (for instance, checking the baseball standings at ESPN or looking for sales at L.L. Bean). Nor does the government have an interest in using the federal criminal law to protect the secrecy of grandma's recipe for apple pie. Yet some broad interpretations of the Computer Fraud and Abuse Act (CFAA) could lead to such an overreach—a classic example of overcriminalization. Consequently, Congress should take the appropriate steps to narrow the reach of the CFAA and define some of the act's ambiguous terms.*

The Computer Fraud and Abuse Act (CFAA) is the federal government's principal legal weapon in the battle to protect computer systems and electronically stored information from thieves and vandals.[1] A criminal statute that can be enforced by the U.S. Department of Justice, the CFAA also authorizes private parties to bring a civil damages action against anyone who violates its terms.[2]

Two circuits have reasonably construed the CFAA in order to avoid an overbroad interpretation of its terms. Congress, however, may not be interested in clarifying the CFAA and instead may create new and needless ambiguity as to the meaning of its terms.

### The Purpose of the CFAA

Congress enacted the original version of the CFAA in 1984 to keep hackers from obtaining confidential information maintained by the

This paper, in its entirety, can be found at **http://report.heritage.org/lm95**

Produced by the Edwin Meese III Center for Legal and Judicial Studies

**The Heritage Foundation**
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org



### Key Points

- The Computer Fraud and Abuse Act (CFAA) is the federal government's principal legal weapon in the battle to protect computer systems and electronically stored information.
- The CFAA forbids someone from accessing information in a protected computer if he or she acts "without authorization" or "exceeds [his or her] authorized access."
- Congress did not define those terms, however, and the lower federal courts have disagreed over their meaning.
- Some courts have construed those terms quite broadly, a reading that would make it a crime for an employee to use his work computer, for example, to access the Internet in order to check his standing in a fantasy football league.
- Congress should narrow the reach of the CFAA while clarifying any ambiguous terms.

federal government in computer files or from infecting the government's network of computer systems with a virus.[3] Since then, Congress has amended the CFAA on several occasions, each time enlarging the reach of the statute.[4] Today, the CFAA reaches any computer that is connected to the Internet or that a person or company uses that is "in" or "affects" interstate commerce,[5] terms that enable the government to regulate a broad range of conduct.[6]

The CFAA forbids someone from accessing information in a protected computer if he or she acts "without authorization" or "exceeds [his or her] authorized access."[7] Congress did not define those terms, however, and the lower federal courts have disagreed over their meaning.[8]

Some courts have construed those terms quite broadly. For example, some courts have decided that a person violates the CFAA if he or she uses a computer to obtain information or for any other purpose not expressly permitted by the computer's owner. An employee would violate the act if he uses his employer's proprietary information for his own profit, even though he was entitled to access and use that information for his employer's benefit; if his use of a computer violates a state-law duty of honesty; or if he violates any provision of an Internet service provider's terms-of-service contract.

Other courts have read the CFAA far more narrowly. They have concluded that the statute is concerned with accessing information by means of a computer, not with the subsequent use to which the information is put. Those courts have held that a person does not violate the CFAA if he has permission to access information for any purpose, even if he later misuses whatever information he obtains. Under that interpretation of the CFAA, an employee would not act unlawfully by using his employer's proprietary information for his own benefit as long as the employee was entitled to access that material in his job.[9]

Each interpretation of the CFAA has obvious benefits but also creates equally obvious problems. The broad interpretation protects against the misuse of lawfully obtained information, but it also would make it a crime for an employee to use his work computer to access the Internet in order to check his standing in a fantasy football league or for any of the myriad other harmless reasons why a person would surf the net. The second, narrower interpretation avoids criminalizing harmless online Internet access but would not bar an employee from accessing his employer's business plan for the purpose of selling it to a rival or from snooping around his coworkers' electronic medical files.

## The Decisions in *Nosal* and *WEC*

The United States Courts of Appeals for the Ninth and Fourth Circuits addressed this issue in similar contexts last year and reached the same conclusion.[10] Each case involved a person who, acting by

1. 18 U.S.C. § 1030 (2012). For a description of the history of the CFAA, *see* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010); Orin S. Kerr, *Cybercrime's Scope: Access and Authorization in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1605–07 (2003) (hereafter Kerr, *Cybercrime's Scope*); Paul J. Larkin, Jr., United States v. Nosal: *Rebooting the Computer Fraud and Abuse Act*, 8 Seton Hall Cir. Rev. 257 (2012).
2. *See* 18 U.S.C. § 1030(c) (2012) (authorizing imprisonment for no more than 20 years); *id*. § 1030(g) (authorizing civil damages and injunctive relief); *id*. § 1030(c)(4)(A)(i)(I)–(V) (factors necessary to maintain a civil action).
3. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (1984) (codified at 18 U.S.C. § 1030 (2012)); Larkin, *supra* note 1, at 262.
4. *See* Kerr, *Cybercrime's Scope*, *supra* note 1, at 1569–71; Larkin, *supra* note 1, at 262–63 & nn.22–23.
5. *See id*.
6. *See*, *e.g.*, Gonzales v. Raich, 545 U.S. 1 (2005); Wickard v. Filburn, 317 U.S. 111 (1942). It is unclear just how far Congress can extend its reach under the Commerce Clause, U.S. Const. Art. I, § 8, Cl. 3. *See* United States v. Lopez, 514 U.S. 549 (1995); United States v. Morrison, 529 U.S. 598 (2000); Sebelius v. NFIB, 132 S. Ct. 2566, 2584–93 (2012) (opinion of Roberts, C.J.); *id*. at 2642–50 (opinion of Scalia, Kennedy, Thomas & Alito, JJ., dissenting); *cf*., *e.g.*, Jones v. United States, 529 U.S. 848 (2000) (the arson of an owner-occupied dwelling not used for commercial purposes is not property used in interstate commerce or in an activity affecting interstate commerce and therefore cannot be prosecuted under 18 U.S.C. § 844(i) (2006)).
7. *See*, *e.g.*, 18 U.S.C. § 1030(a)(2), (a)(4), (a)(5) & (e)(6) (2012).
8. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive.").
9. *See* Larkin, *supra* note 1, at 265 (discussing the competing interpretations).

himself or with confederate insiders at a company, obtained a firm's proprietary business information and used it for his own benefit. In each case, the circuit court rejected an expansive construction of the CFAA because of the fear that a broad interpretation would criminalize conduct that no one would characterize as blameworthy. Both courts ruled that the relevant inquiry is whether someone is permitted to access information by means of a computer. If the answer is "Yes," the inquiry is over, regardless of the use that person later makes of the information.

The Ninth Circuit case involved David Nosal, a former senior official at Korn/Ferry International, an executive search firm. Nosal enticed company employees to supply him with valuable information that he used at his own rival firm. The federal government charged him with violating the CFAA, but the en banc Ninth Circuit rejected the government's reading of the statute. In *United States v. Nosal*, the court held that Nosal did not violate the CFAA because his confederates had permission to access Korn/Ferry's data base, even though they did not have permission to give that information to him.[11]

*WEC Carolina Energy Solutions v. Miller*, a civil lawsuit, involved a comparable set of facts, the principal difference being that Mike Miller downloaded WEC's proprietary information before he left the company and later used it to win a welding contract for one of WEC's rivals. Relying heavily on the Ninth Circuit's decision in *Nosal*, the Fourth Circuit affirmed the dismissal of WEC's lawsuit against Miller.

The Ninth and Fourth Circuits were troubled by the breadth of the government's interpretation of the CFAA. As Ninth Circuit Chief Judge Alex Kozinski feared, under the government's reading of the CFAA, "millions of unsuspecting individuals would find that they are engaging in criminal conduct" simply because they have violated one of the "terms of service" adopted by their Internet service provider.[12] As Judge Kozinski explained:

> 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....
>
> 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. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a "nonbusiness purpose"? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?
>
> Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can

10. *See* WEC Carolina Energy Solutions v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).
11. For a detailed discussion of the *Nosal* decision, see Larkin, *supra* note 1.
12. *Nosal*, 676 F.3d at 860 (footnotes omitted).

> sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.[13]

In each case, the circuit court denied the complaining party relief under the CFAA but noted that state tort law—and possibly even state criminal law—might offer a remedy for unsavory conduct.[14]

Were this problem a simple matter of selecting the appropriate tort remedy, the federal courts could weigh the competing interests and over time, using the incremental, case-by-case adjudication process characteristic of common-law decision-making, craft an answer that best accommodates competing societal and individual interests. The CFAA, however, is a criminal statute, which changes the nature of the resolution process. Courts must interpret its text rather than use it as a launching pad to create federal common law, since federal courts lack authority to define crimes.[15] Courts also must construe the CFAA's terms strictly, because whatever reading the courts adopt will be applied in Justice Department–initiated criminal prosecutions, not just in damages actions filed by injured private parties.[16]

The Fourth and Ninth Circuits both correctly followed that approach. The CFAA uses the term "authorization" but does not define it. The ordinary dictionary meaning of "authorize" is to grant permission, to warrant, or to sanction.[17] That interpretation focuses on the front end of the process at issue in cases like *WEC* and *Nosal*—that is, a party's use of a computer to *reach or retrieve* information acquired for later use.

The private plaintiff and the government in *WEC* and *Nosal*, respectively, sought to expand the meaning of those terms to include a later, impermissible *use* of information that was permissibly obtained. The fundamental problem with that reading of the CFAA, as both circuits recognized, is that it would make criminals out of millions of people who use a government or private work computer to visit the Internet for purposes that no one would deem inappropriate, such as briefly reading the news at Fox, checking the baseball standings at ESPN, playing Sudoku, or looking for sales at L.L. Bean. Diversions like those have replaced coffee room chatter for many people today, and no one would consider sojourns to those websites inherently unlawful, immoral, or dangerous. Both courts correctly rejected an argument that would criminalize vast amounts of innocuous behavior. Indeed, that is one of the archetypical instances in which the criminal law rule of lenity should be applied.

The result in each case might seem harsh. The government cannot prosecute Nosal under the CFAA, and Miller's former employer cannot sue him under that law. Injured parties—Korn/Ferry, WEC, and the public—are denied a remedy under a law that sought to protect the integrity of computer storage systems against misappropriation. But a federal criminal prosecution or a federal damages action is not the only available response. State law may make it a crime to engage in the same conduct involved in *WEC* and *Nosal* or may provide a tort remedy for an injured party. In any event, the federal courts ought not to construe ambiguous criminal law broadly for fear that an offender will escape.

13. *Id.*

14. Historically, the criminal law governing theft protected tangible, personal property (the common law term was "chattels") against permanent misappropriation. *See* Jerome Hall, Theft, Law, and Society (1935). How the contemporary law of theft should treat intangible property like trade secrets, other forms of intellectual property, and confidential business information generally is an interesting and important subject, raising issues beyond the scope of this Legal Memorandum. For a discussion of those issues, *see* Stuart P. Green, 13 Ways to Steal a Bicycle (2012).

15. Only Congress can create a criminal law. *See* United States v. Hudson, 11 U.S. (7 Cranch) 32 (1812). Ambiguous criminal statutes must be narrowly construed so that the federal courts avoid "making criminal law in Congress's stead." United States v. Santos, 553 U.S. 507, 514 (2008).

16. A statute that defines a crime and creates a civil remedy must be construed as if it would be applied only in a criminal prosecution and cannot be applied broadly in order to ensure that compensation will be available for an injured party. *See, e.g.*, Clark v. Martinez, 543 U.S. 371, 380–81 (2005); Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004).

17. *See WEC*, 687 F.3d at 204 (quoting Oxford English Dictionary (3d ed. 2011; online version 2012)); Larkin, *supra* note 1, at 265.

The rule of lenity has been an important part of the Anglo–American law since the 18th century, and it is as valuable a feature of the penal law as are the statutes defining offenses. The rule of lenity has survived for more than two centuries for an eminently sensible and important reason: It protects morally blameless parties from the risk of being erroneously charged with a crime, the burden of defending themselves against a criminal accusation, the fear of being convicted of an offense, the public obloquy that always follows that event, and the pain of suffering a criminal punishment.

Those parties always will be offstage whenever a case like *WEC* or *Nosal* is litigated, so it can be easy to overlook them. But they always are present, and they, too, are entitled to the protection of the law. The decisions by the Ninth and Fourth Circuits correctly recognize that a properly limited criminal statute is as valuable to the innocent members of the public as is a vigorously prosecuted law.

## Congress Does Not Get the Message

The circuit court decisions in *Nosal* and *WEC* gave rise to the hope that the courts would reject the government's attempt to give an unduly broad interpretation to the CFAA's terms. The tragic death of Aaron Swartz—a computer prodigy who committed suicide rather than stand trial for violating the CFAA by allegedly using MIT's computers to download millions of scholarly articles from JSTOR, a website normally accessible by paying a fee[18]—also led some people to believe that Congress might trim the reach of the CFAA. Unfortunately, it often takes such an event to generate the critical mass in Congress necessary to change the law.[19]

It is not clear, however, that Congress will limit the reach of the CFAA. A draft bill circulating among the members and staff of the House Judiciary Committee could expand the potential for criminal liability under the CFAA.[20] Yet, while some of the terms in the draft bill that are used to define a crime are quite broad, a critical term is left undefined.

Specifically, the draft bill would make it a crime for anyone "intentionally" to access "any protected computer" in a manner that "exceeds authorized access" and that enables that party to obtain "non-public information of an entity or another individual." The first three elements of that proposal are quite broad. The term "intentionally" takes in everyone who uses a computer to access the Internet. A "protected computer" includes every Internet-connected computer. A manner that "exceeds authorized access" embraces a violation of any of the terms or conditions of a party's Internet service provider's contract.[21]

The $64,000 question, therefore, is what does the draft bill mean by the term "non-public information of an entity or another individual"? The draft bill does not define that term. It could mean any information not published in the print edition of *The New York Times*. If so, that term is quite broad. Or it could mean only information that is not accessible via the Internet and that can be obtained only by "hacking" into someone else's computer. If that latter interpretation were true, the draft bill would be far more limited. Indeed, it might limit the bill to conduct that is akin to breaking into a locked file cabinet or vault in order to obtain information that its owner certainly wanted to be unavailable to anyone not given a key. Regrettably, it is unclear whether the term "non-public information of an entity or another individual" should be given a broad, a narrow, or an intermediate-range construction because the draft bill does not define that term.

18. *See, e.g.*, Michael Martinez, *Internet Prodigy, Activist Aaron Swartz Commits Suicide*, CNN (Mar. 7, 2013), http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide (last visited Apr. 8, 2013); Larissa MacFarquhar, *Requiem for a Dream*, The New Yorker (Mar. 11, 2013), *available at* http://www.newyorker.com/reporting/2013/03/11/130311fa_fact_macfarquhar (last visited Apr. 8, 2013); Quinn Norton, *Life Inside the Aaron Swartz Investigation*, The Atlantic (Mar. 3, 2013), *available at* http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/?single_page=true (last visited Apr. 8, 2013); James D. Zirin, *Aaron Swartz' Suicide Forces Hard Questions About the Criminal Justice System*, Forbes (Mar. 29, 2013), *available at* http://www.forbes.com/sites/jameszirin/2013/03/29/aaron-swartz-suicide-forces-hard-questions-about-the-criminal-justice-system/ (last visited Apr. 8, 2013).

19. For a discussion of why that is the case and how that process occurs, *see* Paul J. Larkin, Jr., *John Kingdon's "Three Streams" Theory and the Antiterrorism and Effective Death Penalty Act of 1996,* 28 J.L. & Pol. 25 (2012).

20. A "discussion draft" of a bill to amend the CFAA can be found at http://www.scribd.com/doc/132249133/House-Judiciary-Committee-discussion-draft (last visited Apr. 8, 2013). The phrases quoted in the text are found in Section 3 of the discussion draft.

21. *See* Larkin, *supra* note 1, at 269–81.

The Ninth Circuit's decision in *Nosal* and the Fourth Circuit's decision in *WEC* indicated that those courts were aware of the serious risk of overcriminalization that would follow from endorsing the government's overly broad interpretation of the CFAA. Now it seems that there is a risk that Congress did not get the message that each decision seemed clearly to transmit.

The problem is twofold: First, it is unclear how far the draft bill would reach. That is unfortunate because a criminal statute ought to identify clearly whatever conduct it outlaws. That is a basic principle of criminal and constitutional law, and it is therefore irresponsible to leave important terms in a federal criminal statute undefined.

Second, there is no question that the Justice Department reads the current version of the CFAA as making it a crime to breach a term or condition of a party's Internet service provider's contract. That interpretation is flawed for the reasons given by the Ninth Circuit in *Nosal* and the Fourth Circuit in *WEC*. The government's interpretation of the CFAA, for example, would make it a crime to lie about one's age, height, weight, and so forth on an Internet dating site if that site, or if the telecommunications company connecting a visitor to that site, required everyone to be completely truthful about every fact, in which case lying to gain access to the site would be "unauthorized" and anyone who did so would be exceeding authorized access.

Further, the government's interpretation of the CFAA also does not require that someone *knowingly* violate a term-of-service agreement, let alone that a person do so *willfully*—that is, *intentionally flout* the law.[22] The Justice Department's reading of the CFAA would hold someone strictly liable for violating a term or condition of an Internet service contract even though Anglo–American law generally treats strict liability offenses as unwanted stepchildren.[23]

## Conclusion

The federal government has a legitimate interest in protecting classified information, financial data, and the like, but it has no interest in using the criminal law to prohibit private parties from checking their March Madness selections on an employer's computer, regardless of that employer's computer use policy. Any statute that would make such conduct a crime is a classic example of overcriminalization and gives the criminal law a bad name. Nor does the government have an interest in using the federal criminal law to protect the secrecy of grandma's recipe for apple pie. Civil law can adequately protect that interest. Moreover, it is unwise as a matter of policy for Congress not to make clear exactly what would be a crime.

The Ninth and Fourth Circuits correctly identified the problems that would follow from the Justice Department's interpretation of the CFAA. The appropriate step for Congress to take is to say that those circuits were right and to narrow the reach of the CFAA, not to expand the reach of the statute or to leave new, ambiguous terms undefined.

***—Paul J. Larkin Jr.,*** *is a Senior Legal Fellow and Manager of the Overcriminalization Project in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation.*

22. A person acts "knowingly" if he or she has knowledge of the facts of his or her actions, regardless of whether that person knows that those facts make out a crime. A person acts "willfully" if he or she intentionally violates a known legal duty. *See, e.g.*, Dixon v. United States, 548 U.S. 1, 5–6 (2006).

23. *See, e.g.*, Lon Fuller, The Morality of Law 77 (1969) ("Strict criminal liability has never achieved respectability in our law."); H.L.A. Hart, *Negligence,* Mens Rea*, and Criminal Responsibility*, in H.L.A. Hart, Punishment and Responsibility 136, 152 (2d ed. 2008) ("strict liability is odious"); Alan C. Michaels, *Constitutional Innocence*, 112 Harv. L. Rev. 828, 831 n.15 (1999) (listing numerous books and articles criticizing strict criminal liability).