

United States House of Representatives
Subcommittee on Crime, Terrorism,
Homeland Security and Investigations

"Investigating and Prosecuting 21st Century Cyber Threats"
Wednesday, March 13, 2013
2237 Rayburn House Office Building, 11:30 a.m.

WRITTEN STATEMENT OF ORIN S. KERR
FRED C. STEVENSON RESEARCH PROFESSOR
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

The federal computer crime law known as the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030, must strike a vital balance. On one hand, the law must allow the government to criminally prosecute and appropriately punish those who break into vital computer networks and cause significant harms. On the other hand, the law must not allow the government to criminally prosecute and punish innocent computer users who engage in routine harmless activity such as violating Terms of Service or visiting public websites.

In order to achieve both goals at once, the law must be clear. The law must specify what it prohibits and what it does not prohibit, what is a felony and what is a misdemeanor. When the law is clear, courts can easily interpret it to both ensure that the government has the power it needs to prosecute wrongdoers and also that the government does not have the power to prosecute innocent Americans who engage in common and innocuous online activity.

Unfortunately, the CFAA is remarkably vague. Congress has largely given up the task of explaining what the law covers, leaving the courts to grapple with what the statute means. The lower courts are deeply divided on the statute's scope, with some courts concluding that the law is remarkably broad. As a result of this confusion, the meaning of the law presently varies depending on which part of the country you happen to be in. This situation is intolerable. Congress should step in and state clearly what

harmful conduct Congress wants to prohibit with the force of federal criminal law. Clarity will ensure that both of the essential goals of the CFAA can be satisfied at once: The law should both punish what should be punished and ensure that innocent conduct is not criminalized.

In my written testimony, I will begin by briefly addressing my experience with the CFAA. I will then explain the broadest and most important provision of the CFAA, and then will then explain how courts have interpreted the most important aspects of the statute. I will conclude by offering my views on how the CFAA should be amended.

I. My Experience With the CFAA

Before I begin, let me briefly explain my experience with the CFAA. I have worked with the CFAA at various times in the capacity of prosecutor, legal scholar, and defense attorney. I first began studying the Computer Fraud and Abuse Act in 1998, when I joined the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. From 1998 to 2001, I assisted in the investigation and prosecution of many CFAA cases as a Justice Department Trial Attorney and as a Special Assistant U.S. Attorney in the Eastern District of Virginia.

In 2001, I joined the faculty at George Washington University Law School. Since that time, I have authored a chapter of a law school casebook on the CFAA, and I have taught the law of the CFAA in a course on computer crime law. *See* Orin S. Kerr, *Computer Crime Law* (Thomson-West 3rd ed. 2013). I have also written two law review articles about the Act. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 *Minn. L. Rev.* 1561 (2010); *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 *NYU L. Rev.* 1596 (2003).

Finally, I have worked and continue to work as a defense attorney in CFAA cases on a *pro bono* basis to try to block the expansive readings of the Act that are the subject of my testimony. My written testimony draws from all of these experiences, although of course it is made entirely in my personal capacity.

II. The Broadest Section of the CFAA, 18 U.S.C. § 1030(a)(2)(C).

The CFAA is essentially a computer trespass statute. It prohibits trespassing on to a computer much like a trespass statute punishes trespassing onto physical land. The CFAA contains a number of different crimes, but the best way to understand the statute is to focus on its broadest section, 18 U.S.C. § 1030(a)(2)(C). This provision punishes whoever “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” We can break this federal crime into its three elements as follows:

- (1) Intentionally accesses a computer without authorization or exceeds authorized access
- (2) Obtains information
- (3) From a protected computer

Critically, elements (2) and (3) will be satisfied in most instances of routine computer usage. Element (2), the requirement that a person “obtains information,” is satisfied by merely observing information. *See, e.g., United States v. Tolliver*, 2009 WL 2342639 (E.D. Pa. 2009) (citing S. Rep. No. 99-432 at 2484 (1986)). The statute does not require that the information be valuable or private. *Any* information of *any* kind is enough. Routine and entirely innocent conduct such as visiting a website, clicking on a hyperlink, or opening an e-mail generally will suffice.

Element (3) is easily satisfied because almost everything with a microchip counts as a protected computer. The device doesn’t need to be what most people think of as a “computer,” and it doesn’t need to be connected to the Internet. Consider the relevant definitions. Under 18 U.S.C. § 1030(e)(1), a “computer” is defined as:

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[.]

This definition “captures any device that makes use of a electronic data processor.” *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011). Indeed, the Justice Department has argued that any “electronic, magnetic, optical, [and] electrochemical” data processing device is included, whether or not it is “high speed.” *Id.* at n.3. Given that many everyday items include electronic data processors, the definition might plausibly include everything from many children’s toys to some of today’s toasters and coffeemakers.

The statutory requirement that the computer must be a “protected” computer does not provide an additional limit. In 2008, Congress amended the definition of “protected” computer to include any computer “used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). In federal law, regulation that “affects interstate or foreign commerce” is a term of art: It means that the regulation shall extend as far as the Commerce Clause allows. *See Russell v. United States*, 471 U.S. 858, 849 (1985). Under the aggregation principle of *Gonzales v. Raich*, 545 U.S. 1 (2005), this appears to include all computers, period. As a result, every computer is a “protected” computer.

Because elements (2) and (3) are so extraordinarily broad, liability for federal crimes under 18 U.S.C. § 1030(a)(2)(C) hinges largely on the first element: What does it mean to access a computer without authorization or to exceed authorized access? Unfortunately, courts have not settled on clear answers to these questions. The terms “access” and “without authorization” are not defined by the CFAA. The phrase “exceeds authorized access” is a defined term, but the definition is largely circular. That phrase is defined in 18 U.S.C. § 1030(e)(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.

Under this definition, conduct exceeds authorization if it exceeds entitlement. But this merely restates the problem: What determines entitlement? Unfortunately, the statute doesn’t say. Because these key phrases are either undefined or defined poorly, judicial

interpretations of “access without authorization” and “exceeds authorization” are surprisingly murky. The next two sections will focus on how courts have interpreted these two terms.

II. The Meaning of “Access Without Authorization”

The two most important precedents on the meaning of “access without authorization” are *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), and *Pulte Homes, Inc. v. Laborers' International Union Of North America*, 648 F.3d 295 (6th Cir. 2011). These two cases indicate that a person accesses a computer without authorization when that person bypasses some kind of password gate or code-based restriction to gain access to a computer.

In *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), the Second Circuit held that sending out an Internet “worm” had accessed victim computers without authorization by gaining access to them in unauthorized ways. The Second Circuit identified two specific ways that accessing the victim computers was without authorization. The first way was gaining access to a computer by guessing a password that controlled access to that computer. This makes sense: Guessing a password is something like picking a physical lock, and using a stolen password is something like making a copy of the key and using it without the owner’s permission. The second way identified by the *Morris* court to access a computer without authorization is by exploiting a security flaw in a program to gain access in a way contrary to the program’s “intended function.” The basic idea is that if a program has a security flaw that enables an outsider to gain access to the computer based on an unintended effect of that program, then the access is not authorized. For a physical analogy, imagine a burglar breaks in to a home by finding a window that has accidentally been left open. The entrance would be without authorization because the homeowner did not intend to allow individuals to enter his home through the window.

The second case, *Pulte Homes, Inc. v. Laborers' International Union Of North America*, 648 F.3d 295 (6th Cir. 2011), provides a helpful bookend to *Morris*. *Pulte Homes* was a civil case involving a lawsuit by a company involved in a labor dispute against a union. According to the complaint, the union hired an auto-dialing service to

place thousands of calls to clog access to the phone system of the company. The company claimed that this constituted an “access without authorization” of the company’s computers. The Sixth Circuit disagreed. According to the Sixth Circuit, the difference between access without authorization and exceeds authorized access is that a person who accesses a computer without authorization has no rights at all to access that computer. The company’s communications system could not have been accessed without authorization, the court held, because it was an unprotected public means of communications. The company “allows all members of the public to contact its offices and executives,” and does not require “a password or code to call or e-mail its business.” “[L]ike an unprotected website,” the Sixth Circuit explained, the company’s “phone and e-mail systems were open to the public, so [everyone] was authorized to use them.” *Id.* at 303-04.

Morris and *Pulte Homes* thus offer a relatively clear answer to the meaning of “access without authorization,” at least in the networked setting when a user accesses a computer over a remote network. Under those two cases, a person accesses a computer without authorization when that person bypasses some kind of password gate or code-based restriction to gain access to the computer.

Importantly, however, even this relatively clear standard does not answer how the concept of “access without authorization” applies outside the network setting. For example, imagine a person has a laptop computer in a locked room, and someone breaks the lock and enters the room to use the computer. Alternatively, imagine *A* borrows *B*’s laptop with *B*’s permission; later on *B* changes his mind and tells *A* that *A* can no longer use it; and *A* uses it anyway. Are these acts “access without authorization” prohibited by the CFAA? At this point, the answer is unclear. *Cf. Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (concluding that an employee who accesses his employer’s laptop computer while breaching the employee’s duty of loyalty accesses the computer “without authorization.”)

III. The Meaning of “Exceeds Authorized Access”

If the meaning of “access without authorization” is relatively clear, the same cannot be said for the meaning of “exceeds authorized access.” Courts have struggled to

understand the meaning of “exceeds authorized access” under the CFAA. The issue is presently the subject of massive confusion in the lower courts, with the federal courts of appeals sharply divided. Much of the problem is the circular definition of “exceeds authorized access,” which is defined in 18 U.S.C. § 1030(e)(6) to mean “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.” Courts have divided on what conduct “exceeds authorized access” means because they disagree on what controls “entitlement.”

Some courts have held that a written statement as to what the owner of the computer allows controls entitlement. Under this view, if a computer owner announces a written rule that governs how users must access the computer, then using the computer in a way inconsistent with that written rule “exceeds authorized access.” For example, in *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010), the Eleventh Circuit held that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he used a SSA database for personal reasons. SSA policy limited access to the database for official business: By breaching that policy and accessing the database for non-business reasons, the defendant had exceeded authorized access. *See id.* at 1263-64.

Other courts have taken a narrower view. For example, in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the en banc Ninth Circuit held that written restrictions do not govern access. According to the Ninth Circuit, a person “exceeds authorized access” when they have some rights to access a computer but nonetheless circumvent technological access barriers to access other information on the computer that they are not entitled to access. *See id.* at 858, 863. Put another way, under the Ninth Circuit view the CFAA only punishes hackers. Hackers who have no rights to access a network “access without authorization,” while hackers have some rights to access a network “exceed[] authorized access. *See id.* at 858. Accord Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 NYU L. Rev. 1596, 1662-63 (2003).

Courts have also divided on whether conduct “exceeds authorized access” absent explicit written conditions from the computer owner. For example, some courts contend

that an employee acts without authorization by accessing his employer's computer with an intent to further acts contrary to the employer's interests. Under this agency theory, a employee violates criminal law by using the employer's computer outside of the scope of agency. *See Citrin*, 440 F.3d at 420–21. On the other hand, other courts have rejected the agency approach and held that an employee does not exceed authorized access by accessing the employer's computer with an intent to act contrary to the employer's interests. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (“Such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems.”)

To add to the confusion, the Justice Department has taken the view that “exceeds authorized access” includes violating a written restriction on computer access such as the Terms of Use of a website. *See United States v. Drew*, 259 F.R.D. 449 (C.D.Cal.2009). This interpretation has the effect of prohibiting an extraordinary amount of routine computer usage. It is common for computers and computer services to be governed by Terms of Use or Terms of Service that are written extraordinarily broadly. Companies write those conditions broadly in part to avoid civil liability if a user of the computer engages in wrongdoing. If Terms of Use are written to cover everything slightly bad about using a computer, the thinking goes, then the company can't be sued for wrongful conduct by an individual user. Those terms are not designed to carry the weight of criminal liability. As a result, the Justice Department's view that such written Terms should define criminal liability – thus delegating the scope of criminal law online to the drafting of Terms by computer owners – would make criminals out of most computer users.

IV. What Should Be Prohibited By the CFAA?

The underlying question raised by the difficulties courts have in interpreting the CFAA is what kind of conduct Congress intended to prohibit. And since this Congress has the power to amend the statute, the more important question is prospective: What kind of conduct should be prohibited under the CFAA?

I urge Congress to expressly adopt the *Nosal* rule. The CFAA should only apply to those who circumvent technological access barriers. The law should apply only to those who break in to computers – to use the common term, it should apply only to “hackers.” In my view, this is the best reading of existing law. Further, Congress should expressly codify it to make clear the appropriate scope of the CFAA.

To be sure, there are some situations in which people do very bad things that happen to involve a violation of a written access restriction. If an individual commits a crime and happens to violate Terms of Service along the way, then the individual should be prosecuted for the crime committed. But the CFAA should not be a catch-all statute that always gives the federal government another ground on which to charge a wrongdoer who violated some other crime that happened to involve a computer.

The problem with a broader approach is that it inevitably ends up covering a great deal of innocent activity. Consider a few examples:

- A. A political blog announces a new rule that readers only are allowed to visit the blog if they plan to vote Republican in the next Presidential election. A reader who plans to vote for the Democratic nominee visits the blog in violation of the rule.
- B. A law student who is forbidden by law school policy to access the law school network during class intentionally violates the rule by checking his e-mail during a particularly boring lecture.
- C. You receive an e-mail from a friend that a new website, www.dontvisitme.com, has some incredible pictures posted that you must see. But there’s a catch: The Terms of Service of the website clearly and unambiguously say that no one is allowed to visit the website. You want to see the pictures anyway and visit the website from your home Internet connection.

If violating an express condition on computer usage is a crime, then all three of the individuals in these scenarios above have committed a federal offense.

Such a law would be intolerable because Terms of Service are essentially arbitrary. Anyone can set up a website and announce whatever Terms of Use they like.

Perhaps the Terms of Use will declare that only people who have been to Alaska can visit the website; or only people named “Frank” can visit. Under the Justice Department’s interpretation of the statute, all of these Terms of Use can be criminally enforced. It is true that the statute requires that the exceeding of authorized access be “intentional,” but this is a very modest requirement because the element itself is so easily satisfied. Presumably, any user who knows that the Terms of Use exist, and who intends to do the conduct that violated the Term of Use, will have “intentionally” exceeded authorized access.

I do not see any serious argument why such conduct should be criminal. Computer owners and operators are free to place contractual restrictions on the use of their computers. If they believe that users have entered into a binding contract with them, and the users have violated the contract, the owners and operators can sue in state court under a breach of contract theory. But breaching a contract should not be a federal crime. The fact that persons have violated an express term on computer usage simply says nothing about whether their conduct is harmful and culpable enough to justify criminal punishment. There may be cases in which harmful conduct happens to violate Terms of Use, and if so, those individuals should be punished under criminal statutes specifically prohibiting that harmful conduct. But the act of violating Terms of Service alone should not be criminalized.

In my view, the answer is to codify the *Nosal* rule. Instead of prohibiting two different acts, “access without authorization” and “exceed[ing] authorized access,” the law should simply prohibit “access without authorization” defined in the following simple way: “the term ‘access without authorization’ means to circumvent technological access barriers to a computer or data without the express or implied permission of the owner or operator of the computer.” This rule would codify *Nosal* and result in a simple rule that would allow the government to prosecute real intruders in networks but not go after those who simply breach terms of service.

V. Additional Thoughts About the Future of CFAA Reform

My written testimony only scratches the surface of the changes to the CFAA that I think are necessary. In addition to adopting the *Nosal* rule, I think Congress needs to better define and narrow the felony provisions of the statute to ensure that the statute accurately distinguishes minor offenses from major ones. I have posted statutory language that I suggest for CFAA reform here: <http://www.volokh.com/wp-content/uploads/2013/01/Amended10302.pdf> I would be happy to discuss any of the changes I recommend in that draft during your questioning.

I want to conclude with four points about the future of CFAA reform:

1) *Congress can do this.* The CFAA dates back to the 1980s, and the major questions raised as to its scope are decades old. As a result, Congress should not be afraid to step in and better define the coverage of the statute. Although computer technologies can change quickly, the scope of authorization is a timeless issue. Federal criminal statutes are purely a creature of Congress: There are no federal common law crimes. As a result, Congress should feel not only the ability but the responsibility to explain with clarity what kind of conduct the criminal laws prohibit.

2) *A narrow but clear CFAA will serve both government interests and civil liberties interests.* The major ambiguity over the scope of the CFAA is an obvious problem from the standpoint of civil liberties. But it is also a problem for law enforcement. Significant statutory vagueness in a criminal statute invites courts to narrow or even invalidate the statute under the “void for vagueness” doctrine. As long as the CFAA retains its existing text, vagueness challenges will continue. *See generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010). Prosecutors need to rely on the CFAA when prosecuting important cases with real harms. A clear and specific statute will better serve government interests than a vague and opaque one.

3) *Insider threats can be covered under a different statute.* Under the *Nosal* rule, insider threats can still be punished under some sections of the CFAA, such as 18 U.S.C. § 1030(a)(5)(A). But if Congress wishes to punish insiders beyond 18 U.S.C. § 1030(a)(5)(A), the answer is to punish insider threats using a different statute. To some

extent, other criminal laws will apply already. For example, many insider threats can be punished under the federal theft of trade secrets statute, 18 U.S.C. § 1832. But Congress can easily address the insider threat through other statutes such as the Interstate Transportation of Stolen Property Act, 18 U.S.C. § 2314.

4) *The CFAA is only becoming more important.* A final reason to focus attention on CFAA reform is that the statute will only become more important over time. Every year, the American public uses computers for more hours and for more tasks. The recent public uproar over the tragic death of Internet activist Aaron Swartz has brought new attention to the scope of the CFAA. Swartz was facing felony charges under the CFAA, and many believe that those charges show that the CFAA is overly broad and overly punitive. *See, e.g., Lessig on 'Aaron's Laws - Law and Justice in a Digital Age'*, available at <http://www.youtube.com/watch?v=9HAw1i4gOU4>. But whether inspired by recent events or simply by the need to address the scope of a statute that has become ever more important in our Internet age, Congress should take this opportunity to revisit the CFAA to make sure that it both provides appropriate tools for law enforcement but does not end up prohibiting innocent activity.

Thank you for this opportunity to testify. I look forward to your questions.
