2011

Cyber Security: Protecting America's New Frontier: Hearing Before the H. Subcomm. on the Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong., November 15, 2011 (Statement of Orin S. Kerr, Prof. of Law, GW Law School)

Orin S. Kerr
George Washington University Law School, okerr@law.gwu.edu

Testimony of Orin S. Kerr
Professor, George Washington University Law School

United States House of Representatives
Committee on the Judiciary
Subcommittee on the Crime, Terrorism,
and Homeland Security

"Cyber Security: Protecting America's New Frontier"
Tuesday, November 15, 2011
2141 Rayburn House Office Building, 10 a.m.

_____

WRITTEN STATEMENT OF ORIN S. KERR

The current version of the Computer Fraud and Abuse Act (CFAA) poses a threat to the civil liberties of the millions of Americans who use computers and the Internet. As interpreted by the Justice Department, many if not most computer users violate the CFAA on a regular basis. Any of them could face arrest and criminal prosecution.

In the Justice Department's view, the CFAA criminalizes conduct as innocuous as using a fake name on Facebook or lying about your weight in an online dating profile. That situation is intolerable. Routine computer use should not be a crime. Any cybersecurity legislation that this Congress passes should reject the extraordinarily broad interpretations endorsed by the United States Department of Justice.

In my testimony, I want to explain why the CFAA presents a significant threat to civil liberties. I want to then offer two narrow and simple ways to amend the CFAA to respond to these problems. I will conclude by responding to arguments I anticipate the Justice Department officials might make in defense of the current statute.

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 26-109 (West 2nd ed. 2009). 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 also worked as a defense attorney and consulted with defense lawyers 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. In particular, I briefed and argued the successful motion to dismiss in the so-called "MySpace Suicide" case. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). My written testimony draws from all of these experiences, although of course it is made entirely in my personal capacity.

II. The Extraordinary Scope of 18 U.S.C. §1030, the Computer Fraud and Abuse Act.

When the Computer Fraud and Abuse Act was first enacted in the 1980s, it was a narrow statute that targeted computer hacking and other harmful computer misuse. Over the last 25 years, however, Congress has broadened the statute dramatically four different times: in 1986, 1996, 2001, and 2008. Each of these amendments significantly expanded the reach of the statute. Today's statute is breathtakingly broad, and its key terms are subject to a wide range of interpretation that can make it so broad as to render the statute unconstitutionally vague. *See generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010).

A quick look at the broadest crime in the statute reveals the problem. The broadest provision of the broadest crime, 18 U.S.C. § 1030(a)(2)(C), punishes whoever "intentionally . . . 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 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 conduct "exceeds authorized access"? 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.

This provides little guidance, unfortunately, as the definition is largely circular. Under the definition, conduct exceeds authorization if it exceeds entitlement. But what determines entitlement? The statute doesn't say, and that failure to provide guidance has allowed the Justice Department to adopt extremely broad readings of what might exceed authorized access.

As a practical matter, the key question has become whether conduct "exceeds authorized access" merely because it violates a written restriction on computer access such as the Terms of Use of a website. The Justice Department has taken the position that it does. 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 – triggers a remarkable set of consequences. A few examples emphasize the point:

(a) The Terms of Service of the popular Internet search engine Google.com says that "[y]ou may not use" Google if "you are not of legal age to form a binding contract with Google." http://www.google.com/accounts/TOS (last visited November 14, 2011). The legal age of contract formation in most states is 18. As a result, a 17-year-old who conducts a Google search in the course of researching a term paper has likely violated Google's Terms of Service. According to the Justice Department's interpretation of the statute, he or she is a criminal.

(b) The Terms of Use of the popular Internet dating site Match.com says that "You will not provide inaccurate, misleading or false information . . . to any other Member." http://www.match.com/registration/membagr.aspx (last visited November 14, 2011). If a user writes in his profile that he goes to the gym every day – but in truth he goes only once a month – he has violated Match.com's Terms of Use. Similarly, a man who claims to be 5 foot 10 inches tall, but is only 5 foot 9 inches tall, has violated the Terms. So has a woman who claims to 32 years old but really is 33 years old. One study has suggested that about 80% of Internet dating profiles contain false or misleading information about height, weight and age alone. *See* John Hancock, et. al., *The Truth about Lying in Online Dating Profiles* (2007), available at https://www.msu.edu/~nellison/hancock_et_al_2007.pdf. If that estimate is correct, most Americans who have an Internet dating profiles are criminals under the Justice Department's interpretation of the CFAA.

(C) Terms of Use can be arbitrary and even nonsensical. Anyone can set up a website and announce whatever Terms of Use they like. Perhaps the Terms of Use will declare that only registered Democrats can visit the website; or only people who have been to Alaska; or only people named "Frank." 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.

III. Two Statutory Solutions to the Overbreadth of the CFAA

Fortunately, there are two simple ways to amend the CFAA to cure its overbreadth. The first solution is to amend the statutory definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6) to clarify that should not be interpreted to prohibit Terms of Service violations. The Senate Judiciary Committee recently approved an amendment to a pending bill, S.1151, that includes such language limiting the scope of the CFAA. As amended, Section 110 of S.1151 states:

> Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''

This is a very helpful amendment, and I endorse it. To be sure, it is not a model of clarity. It defines "exceeds authorized access" by what it *isn't* rather than by what it *is*, which may lead to confusion. It also leaves unclear when a violation should be deemed

the "sole basis for determining that access to a protected computer is unauthorized," as compared to merely one part of that basis. But I read the amendment as indicating that the Justice Department generally cannot bring prosecutions based on violations of Terms of Service and Terms of Use.

Notably, the language carves out one significant exception. The government can pursue prosecutions for violations of computer use policies used by government employees. This will enable prosecutions when government officials misuse sensitive government databases. *See, e.g., United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (allowing a criminal prosecution of a Social Security Administration employee for accessing Social Security Administration databases for nonbusiness reasons in violation of workplace policies). Many government workplace computer use policies protect important government interests, and violations of such policies can trigger significant societal harms. As a result, it is sensible that the Justice Department's broad theory of the CFAA should be retained in that specific setting. Other uses of the Justice Department's broad theory will be prohibited.

(b) An alternative statutory solution would be to limit § 1030(a)(2) directly by creating significant limits on the kind of information that can trigger liability under 18 U.S.C. § 1030(a)(2)(A)-(C). As explained above, the current version of § 1030(a)(2) is triggered when an individual obtains *any* information. It doesn't matter what the information is, or whether it has any value. This means that the prohibition can apply even to violating arbitrary Terms of Use that protect websites that contain no private or valuable information. To correct this, the statute could be rewritten to limit § 1030(a)(2) to obtaining the specific kinds of information that, when obtained in excess of authorization, are associated with significant harms. For example, § 1030(a)(2) could apply only when an individual obtains:

> (a) information with a value of more than $5,000; or
> (b) sensitive or private information involving an identifiable individual (including such information in the possession of a third party), including medical records, wills, diaries, private correspondence, financial records, or photographs of a sensitive or private nature;

Under this proposal, violating Terms of Service could still violate the CFAA in *some* cases. However, liability only would extend to the rare violations of Terms of Service

in which the violation allowed an individual to obtain very valuable or very private information to which they were not entitled. These will tend to be the rare cases in which the violation of an express term on computer use is associated with a harm that might justify criminal prosecution.

IV. Responses to Anticipated Counterarguments

I anticipate that the Justice Department will defend the current state of the law with three related arguments. The first argument I anticipate is that although the current language of the statute is tremendously broad, the Justice Department can be trusted with this power because it has not often abused its authority under the statute. The second argument is that the Justice Department needs maximum discretion in this area to account for the unpredictability of technological change. The third argument I anticipate is that the broad reading of the statute is helpful to the Justice Department because it may make it easier to punish some individuals who have caused harms using computers.

I'll start with the first argument, that the Justice Department can be trusted with this power because it has exercised its discretion wisely This argument is problematic for two reasons. First, it appears to misunderstand the proper role of Congress and the Executive branch in the enforcement of criminal law. It is the responsibility of the United States Congress to enact criminal laws that only prohibit conduct that is harmful, culpable, and deserving of criminal punishment. It is the responsibility of the Executive to enforce those violations in appropriate cases. This division of duties does not allow Congress to write DOJ a blank check, and for DOJ to be the ultimate arbiter of what is criminal.

This argument is also weak because the Justice Department's broad interpretation of the CFAA has not been clearly endorsed by the courts, meaning that it is not at all clear that the prosecutors actually enjoy the discretion they might claim to have wisely exercised. In the one and only criminal prosecution for violating Internet terms of service, the district court rejected the Justice Department's interpretation as unconstitutional and dismissed the charges. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). The Justice Department declined to pursue an appeal from that ruling. Just a few weeks ago, the Ninth Circuit granted the defendant's petition for rehearing *en*

banc in the first criminal prosecution based on violations of a private-sector employee computer use policy. *See United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), *reh'g granted*, -- F.3d --, 2011 WL 5109831 (October 27, 2011). In light of the judicial resistance to the Justice Department's efforts to read the CFAA so broadly, it would be premature for Justice Department officials to commend themselves for how prosecutors have exercised the power that prosecutors may or may not have.

I am also unpersuaded by the second argument I anticipate, that the Justice Department needs maximum discretion in this area to account for the unpredictability of technological change. This argument might have been persuasive in the 1980s, when Congress enacted 18 U.S.C. § 1030. It might have made sense in the 1990s, when most Americans first began to use the Internet regularly. But the argument doesn't work in late 2011, more than a quarter-century after the passage of the CFAA. The basic ways that computers might be misused have been well-known for decades. The concepts and principles are the same today as they were twenty years ago. There is little new under the sun, and therefore no apparent need for maximum discretion to account for technological change.

The third and final argument I anticipate is that the broad reading of the statute is helpful to the Justice Department because it may facilitate punishment of some individuals who have caused harms using computers. If Justice Department officials make this argument, I urge the Committee to ask for specific scenarios and to make sure that the conduct described isn't already criminal under other provisions of the criminal code. Making a threat using a computer already violates the federal threat statute, for example. Stealing trade secrets using a computer already violates the federal theft of trade secrets statute. It is hard to see what value there is in making such conduct also a CFAA violation.

Indeed, it is easy to see the harms of doing so. A broad reading of the CFAA that effectively makes it illegal to do anything harmful using a computer would mean that the carefully-crafted statutory scheme of federal criminal law would be trumped whenever a computer is involved. If computer-related conduct is harmful, prosecutors should charge the preexisting crimes that relate to the harm. They should not use the CFAA as a catch-all.

The pending case of *United States v. Nosal* provides a helpful illustration of the problem. The facts of *Nosal* justify a theft of trade secrets prosecution: Nosal allegedly worked with employees of his old company to help steal secrets from that company so he could set up a competing business. The Justice Department charged the defendants with both theft of trade secrets and violating the CFAA. The trade secrets charge was based on stealing trade secrets, and the CFAA charge was based on the employees' violating a workplace computer policy that banned use for reasons other than official company business. If the Ninth Circuit allows the CFAA charges in *Nosal* to proceed, the CFAA charges will be much easier to prove. Establishing a theft of trade secrets requires proving all the elements of the crime, and that can be a difficult task. In contrast, proving that an employee did *something* for reasons other than official company business is vastly easier. To my mind, allowing this theory would set a dangerous precedent. If the government is really bringing the prosecution because of the alleged theft of trade secrets, the government should have to prove a theft of trade secrets.

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

———————