Updating the Computer Fraud and Abuse Act

*By Jonathan S. Keim **

Introduction

In recent years, American institutions have suffered from a seemingly endless series of high-profile computer intrusions: Ashley Madison, the Office of Personnel Management, Sony Pictures, and health insurer Anthem.[1] Computer hackers connected with international organized crime groups apparently violate American law with impunity. Defensive technology designed to detect and prevent intrusions has been deployed widely, but attackers always seem to be one step ahead. In response, Congress has been considering a broad range of measures intended to address cybercrime's growing economic impact.

This paper provides some background principles to guide one aspect of that reform: revising the federal criminal statute that governs computer intrusions known as the Computer Fraud and Abuse Act (CFAA).[2] As Part I will show, the need for a strong CFAA has never been greater than it is today. But Part II will explain some of the problems with the current CFAA, which has become too broad. Its sweeping jurisdictional claims and wholesale incorporation of state criminal and tort laws put it into an uncomfortable position in the Constitution's allocation of federal and state powers. Meanwhile, the courts have interpreted the CFAA so broadly that Congress must step in to clarify its limits. The reforms proposed below are designed to fix these problems while ensuring that the CFAA is able to address contemporary threats adequately.

I. How We Got Here: A Brief Overview of Information Security

A. Computer Security from Mainframes to "The Cloud"

In the early days of computers, information security required little more than sturdy doors. Early room- or closet-sized mainframe computers usually required users to physically access the computers or their terminals, which meant that potential intruders necessarily exposed themselves to apprehension. In addition, attacks on centralized computing targeted the entities that could afford to invest vast resources in computing technology such as defense, research, and banking institutions, not consumers.

The expanding popularity of the personal computer in the 1980s decentralized computing power by putting devices into homes and small businesses and, in the process, opened new doors for electronic threats to consumers. This new computing paradigm eventually gave rise to a new type of threat: viruses. Few computers were connected by networks, so malicious software moved slowly from computer to computer through shared floppy disks. Virus writers rarely hoped for pecuniary gain, so viruses tended to be either harmless pranks or malicious data destroyers. Computers attached to networks were still vulnerable to outside attack, but the number of networked computers was so small that attackers could often be identified.

Electronic security threats to consumers and businesses accelerated in the mid-1990s as personal computers began connecting to the internet in large numbers. As more computers connected to the internet, the rise of cheap and fast network connectivity in the first decade of the 21st century began the rapid re-centralization of both data and computing resources in data centers.

On the one hand, technology re-centralization has enabled the growth of new business models based on reliable, fast, inexpensive network connectivity, a model sometimes called "cloud computing."[3] Consumers and businesses entrust "cloud" providers with vast amounts of information that they can access over the internet, but they often have no idea where in the world (literally) their data is being stored.[4]

Such connectivity comes with security risks. A company that handles customer data may be unwilling or unable to repel attacks from outsiders, or it may be populated by untrustworthy employees. In addition, computers attached to home and business networks can be vulnerable to infection by malicious software, known as "malware," which can use the computers to carry out sophisticated fraud transactions and other nefarious activity without the owner's knowledge.

At the same time, a cottage industry in defensive technology has risen to meet these challenges. Antivirus and other technology companies regularly hire ex-military cyber-operations personnel to ensure that their customers have products designed with the most up-to-date knowledge and skills. Penetration testers study computer software and hardware to find flaws. Several companies (and probably many more independent researchers) sell software that exploits these flaws to governments, defense contractors, and others who use them both offensively and defensively.[5]

B. Contemporary Threats

Computer intrusions and attacks generally fall into two general categories: insider and outsider.[6] An insider is typically an employee or other trusted person who has (or had) some level of authorization to access the victim's computer systems, but abuses that knowledge for an illegal purpose. The insider might be a disgruntled ex-employee, a friend, an employee engaging in corporate espionage, or perhaps a systems administrator who likes the thrill of damaging systems.[7]

An outsider, by contrast, has no authorization to use the targeted system. Because outsider attacks do not begin from a privileged position within a targeted organization, outsiders are likely to use hacking tools or techniques. Outsiders can be organized or disorganized, and their motives can include things like curiosity, anger, ideology, financial gain, nation-state intelligence-gathering, or even obtaining an advantage in competitive video games.[8] Once an attacker has obtained

** Jonathan Keim is Counsel for the Judicial Crisis Network. He is a former information technology professional and a former Special Assistant United States Attorney in the Cybercrime Unit of the U.S. Attorney's Office for the Eastern District of Virginia. All opinions belong to the author.*

control over an attacked system, he can use the computer to eavesdrop, copy, modify or delete data, impersonate computer users, collect passwords and other identity information, or generally wreak havoc.[9]

Early cybercriminals tended to be computer science experts who knew the intricacies of the systems they compromised. Now, however, intrusion expertise has become decentralized and democratized along with computing technology. The last decade has seen the rise of international organized crime syndicates that use sophisticated attack mechanisms in connection with fraud schemes to steal hundreds of millions of dollars from banks, businesses, and individuals.[10] Anonymity technologies designed to help dissidents evade totalitarian regimes have enabled pedophiles to exchange child pornography using what is sometimes called the "Dark Web."[11] In addition, foreign nation-states and others have reportedly sought to obtain access to critical infrastructure and financial institutions.[12]

Just as the legitimate software industry has now created technology enabling kindergarteners to use smartphones, the cybercrime underworld has created consumer-grade tools that enable anyone with a little money and motivation to become a cybercriminal. Underworld merchants have borrowed lessons from business, creating products that make it possible for relatively unsophisticated criminals to perform basic hacking tasks. Sites on the Dark Web sell "off-the-shelf" hacking tools designed with easy-to-use controls, as well as access to prehacked computers and accounts for impatient criminals who can't be bothered to hack their own.[13] These computers can then be used to commit other crimes, send mass unsolicited email (or spam), or hide the source of other attacks.

C. How the CFAA Protects Legal Interests in Property

Computer intrusions affect legal interests in property that will be familiar to any student of tort law.[14] Criminal laws that forbid intrusions, such as the CFAA, generally protect a computer owner's legal interests in exclusive possession and control by prohibiting unauthorized access to the computer;[15] these legal interests are also protected by the common law tort of trespass to chattels.[16] Criminal laws forbidding unauthorized interference with the operation of computers[17] likewise protect the same interests as the torts of conversion and private nuisance because such activities interfere with the rightful control, use, or value of property.[18]

An intrusion that only nominally infringes on the rights of possession, control, or use is not sufficient to constitute a crime under the CFAA, however. It must result in some alteration in the use of the computer,[19] furtherance of a fraud,[20] damage or loss,[21] or a breach of confidentiality (defined as "obtain[ing] information").[22]

The legal interests protected by the statute can have fuzzy boundaries.[23] For instance: The CFAA forbids unauthorized "access" that "affects" a computer that is sometimes used by the government.[24] What degree of interaction is required before an "access" "affects" the operation of a computer? Also, a feared and very common attack called a distributed denial of service (or "DDoS") involves sending a flood of junk network traffic to a target website to crowd out other users' access, but it fits only uncomfortably within the CFAA's prohibitions of a "transmission of a program, information, code, or command" that intentionally causes damage.[25] Does crowding out other users' traffic count as "damage" to a target?

The CFAA's standard for whether a computer user actually trespasses is particularly malleable. Violations of the CFAA can occur if access is either "without authorization" or "exceeding authorization," but the latter has a circular statutory definition. Access that "exceeds [the owner's] authorization" is defined as access "with authorization" that the actor then uses "to obtain or alter information that the individual is not entitled to obtain or alter."[26] Although the drafters of the statute were trying to distinguish between permission to access the computer itself and the level of permission to obtain or alter information on the computer, courts have understandably been confused by the distinction.[27] Among other problems (such as those discussed in Part II.B), the fuzzy statutory boundaries protecting these legal interests ultimately raise questions about whether the CFAA provides adequate clarity to potential defendants about what conduct is prohibited.

Despite these problems, the CFAA remains the primary federal authority protecting computing technology from intrusions. With consumers and businesses facing security threats from every direction, the need for robust computer crime laws and enforcement has never been greater. At the same time, the CFAA must not create more problems through overbreadth than it solves. The next Part will explore several ways that Congress can ensure that the CFAA continues to serve its intended purpose without abandoning other values central to the rule of law.

II. Improving the Computer Fraud and Abuse Act: Problems and Solutions

As the preceding Part shows, protecting property threatened by computer intrusions requires enforcement of computer crime laws. Yet despite the relatively simple nature of the legal interests protected by the CFAA, several new circumstances complicate enforcement. In addition, the CFAA's scope—it claims to protect nearly every computer in the world—raises concerns about whether it occupies the appropriate constitutional role for a federal statute. A definitive answer for how to resolve the tension between effective enforcement of computer crime laws and a limited federal role is outside the scope of this paper, but this Part will identify several ways that would move the CFAA in the right direction.

To begin with, an internationalized and democratized computer security world means that much computer crime takes place across domestic and international boundaries. Congress can make better use of the powers entrusted to it by focusing federal law enforcement resources on inter-jurisdictional and international threats. In addition, fiscal restraint generally makes expensive and risky international investigations hard to justify. Congress should pursue policy federalism, allowing state law enforcement agencies to take increasing responsibility for purely domestic computer crimes that do not implicate a significant federal interest. This would make federal resources available for more ambitious international investigations that clearly implicate the powers of the federal government.

The CFAA also presents an overcriminalization problem. The courts have (until recently) progressively expanded

the scope of potential CFAA liability to include malfeasance that is not obviously trespass or hacking. Congress can fix this problem by scaling back the scope of the CFAA's criminal liability and leaving such matters for civil liability. Along the same lines, the CFAA can have unwanted chilling effects on innovative and socially-useful security research. Clarifying portions of the CFAA could eliminate these chilling effects, thus removing unnecessary legal impediments to development of advanced defensive security technologies. And at the same time, Congress should weigh in on the debate about whether victims of intrusions should be allowed to engage in "hacking back," a controversial practice that directly implicates the CFAA's core protections of property.

A. Prioritize Federal Resources Toward National and International Threats

With the most serious cybercrime threats now coming from international organized crime, Congress should encourage federal law enforcement agencies to prioritize investigative efforts against those threats. Although enforcement prioritization is typically an executive function, Congress has some tools to ensure that law enforcement resources are directed towards the most serious threats.

One drastic step in this direction would be to reduce the number of privately-owned computers that are subject to federal jurisdiction. The CFAA currently protects federal-interest computers (those used by financial institutions or the federal government) and all private computers "used in or affecting interstate or foreign commerce or communication."[28] By its terms, the CFAA effectively covers every computer in the world.[29] Congress could scale back the extent to which the CFAA reaches beyond federal-interest computers to include only private computers that have a *substantial* effect on interstate or international commerce, are used primarily for such commerce, or for which there is reason to suspect a connection to a conspiracy. This would ensure that government agents focus their investigative efforts on solving serious crimes instead of relatively minor computer intrusions for which the relationship with interstate commerce or other federal interests is only incidental.

More cautious steps would include directing federal investigators to prioritize the most significant threats to American consumers and businesses, such as fraud, malicious damage, and international organized crime. And since so much computer crime is committed by criminals located in other countries, this would practically mean reallocating enforcement resources toward international investigations and directing the executive branch to improve mutual legal assistance relationships with foreign governments.

Congress could also use federalism principles to divide responsibility for computer intrusions more evenly between the states and the federal government. Of course, federal law enforcement agencies have a central role investigating computer intrusions because the internet is an interstate telecommunications medium. The centralized federal role works for several simple reasons: federal agencies can easily operate across state lines, agents are unhampered by the daily emergency law enforcement responsibilities that typically apply to state law enforcement agencies, and federal agencies have greater resources and expertise than many state and local agencies. But the rapid development of new and sophisticated online threats is now putting significant pressure on those resources, which are increasingly scarce. As before, Congress could take drastic steps relinquishing federal responsibility to states.[30]

Similarly, Congress should consider reducing the extent to which the CFAA appropriates state law. The CFAA currently incorporates by reference state criminal and tort law—all of it—by turning any intrusion that furthers a state criminal or tortious act into a 5-year felony.[31] But this discourages states from investigating or prosecuting intrusions. After all, why should a state bother to investigate or prosecute a computer intrusion if the federal government will do it instead?

Encouraging states to pursue their own enforcement priorities would have some potential drawbacks such as reduced efficiency, cross-jurisdictional investigative cooperation problems, non-uniform policy, and so forth. In addition, few states currently have resources or expertise comparable to those of the federal agencies that currently investigate most cybercrimes.

On the other hand, there is little reason to impose a single, uniform national approach to computer intrusions for crimes that have no substantial federal interest or cross-jurisdictional connection. De-federalization of enforcement responsibilities would encourage states to experiment with policies uniquely addressed to particular state needs. California, whose economy depends heavily on its electronic infrastructure, could impose more significant penalties on intrusions than New Hampshire. Rebalancing responsibility among the actors in the federal system would reduce the burdens on federal law enforcement while also empowering states to pursue more locally-desirable solutions.

B. Decriminalize Activity That Can Be Adequately Addressed Through Civil Liability

Decriminalizing conduct that can be adequately addressed through non-criminal forms of legal liability would allow law enforcement to focus on investigating and prosecuting the most serious crimes. This proposal would principally affect the CFAA provisions prohibiting access that "exceeds authorization" and thereby obtains or alters information that the individual "is not entitled" to.[32] This form of liability is designed to enable prosecution of (for example) employees who are given access to a computer, then abuse that access and obtain information that they are not supposed to access. But it has also turned into a tool for punishing employees who violate use restrictions on data they are otherwise entitled to access.

The current language creates two particularly important problems. First, as law professor Orin Kerr has observed, its breadth approaches constitutional limits regarding notice to potential defendants about what conduct violates the statute. [33] The CFAA does not explain how a defendant can know which information she might be "entitled" to. Recent government proposals to amend the CFAA do nothing to address the notice problem, and actually would specifically authorize prosecutions for "exceeds authorization" violations that involve the misuse of data (defined as use for a purpose that the computer owner opposes).[34] By refocusing the CFAA's authorization language on the defendant's wrongful intent, i.e., her intention to violate the

owner's right to exclude her from the property, Congress could eliminate the notice problems and avoid the worst overbreadth.

Second, the CFAA's "exceeds authorization" liability criminalizes disputes that more properly fit within civil processes. Many of the cases concluding that a defendant "exceeds authorization," for instance, seek criminal sanctions for company employees who are entitled to access data but misuse it or misappropriate it in violation of an employment agreement or fiduciary duty.[35] In these cases there is usually been little question about the identity of the responsible defendants and no physical damage or violence (even if there is fraud). In such cases, the intrusive methods and punitive goals of the criminal law seem disproportionate to the wrong. Civil damages or equitable relief, by contrast, could provide victims with a complete remedy without requiring incarceration. Congress should not de-criminalize all forms of "exceeds authorization" liability, however. Deliberate attempts to inflict damage or pecuniary loss would be appropriate bases for criminal liability. But mere breaches of trust or contract should only be subject to civil remedies.[36]

If decriminalization of all "exceeds authorization" cases seems excessive, Congress could take a more modest step of elevating the mens rea to require at least an intentional violation of the owner's property interests. Because intrusion liability has generally been predicated on a trespass of some sort, Congress could refine "exceeds authorization" liability to include only willful violations of express limitations on access. Elevating proof requirements in this way would ensure that the CFAA, much like criminal trespass statutes, punishes the willful violation of an owner's right to exclude others from property, not the mere misuse of information.[37]

C. Clarify the Legal Boundaries for Computer Security Research

In recent years, the CFAA has begun to cast a shadow over the development of technology that is the first line of defense against intrusions for most businesses and consumers. Such technologies are often the result of intense study and experimentation, but research can easily drift into activities of dubious legality, particularly if the activities strongly resemble the activities of a potential intruder. In some cases, researchers have faced criminal prosecution because they pursued their research several steps too far.[38] For the purposes of this Section, though, the main concern is the potential chilling effect on research from excessively broad or ambiguous provisions of the CFAA. Researchers who must choose between potential jail time and not performing important research are likely to avoid innovative forms of research. Here as elsewhere, good fences make good neighbors, and the CFAA is badly in need of some fence-mending in four areas.

The first relates to the definition of "access" under the CFAA. Private security researchers often find it useful to access computers attached to the internet to collect data through automated scanning.[39] But some courts have concluded that the Terms of Service posted on a website can be legally binding and that visitors can be held liable for violations of those terms under the CFAA.[40] This puts researchers who use automated tools to a Hobson's choice: How would a potential defendant ever know what potentially liability-creating restrictions an owner has placed on access to the computer without first accessing the computer? Defining "access" would help clarify the scope of such prohibitions.

The second relates to aggressive techniques used by some security researchers. Teams of volunteers perform research on malware and help shut down networks of infected computers (called "botnets") under the control of a criminal (the "botmaster") that can be used for a variety of nefarious purposes, such as banking fraud or DDoS attacks. But under existing law, these public-spirited researchers could someday find themselves the targets of prosecution, since shutting down a computer without the owner's express permission seems to fit within the CFAA's prohibited conduct.[41] Some researchers forge ahead with research despite the possibility of prosecution.[42] Congress should find a way to encourage such socially beneficial activities without authorizing outright vigilantism.

Third, the Department of Justice and private sector actors have performed a valuable service in recent years to shut down botnets down by cobbling together civil and criminal legal remedies.[43] But the ad hoc approach and lack of congressionally-authorized standards for such operations raises concerns about accountability for mistakes, disruptions, and potential misconduct. This is particularly concerning because of the significant possibility of collateral damage from such operations.[44] Whatever the best policy in this area, minimizing the legal gray areas around research and mitigation efforts, as well as articulating standards for judicial review, would protect computer owners from unwarranted interference while also permitting remediation efforts to continue.

The fourth area concerns the disclosure of security vulnerabilities. "White hat" researchers sometimes infiltrate "black hat" circles or make purchases on the black market to publicize cutting-edge techniques and vulnerabilities of commercial products. Security experts who discover vulnerabilities in software or other technologies publish vulnerability information to the public as a way of shaming manufacturers who are slow to rectify the problems with their products.[45] Although the ethical boundaries around such practices are still being debated,[46] Congress should clarify the legal boundaries.

As in other areas of law, clarification of the actors' legal rights promotes Coasian bargaining about the scope of permissible access. Clarity encourages companies and researchers to contract around potential disputes, as Google and many other others have done, by establishing "bug bounty" programs that reward researchers for finding security problems before criminals find and exploit them.[47] Researchers who obtain consent from consumers before engaging in more aggressive forms of research or testing would facilitate research while also eliminating the risk of CFAA liability. This approach allows the parties to work out a desirable outcome without tying the hands of the industry that creates advanced technologies far more nimbly than Congress or any administrative agency could act.

D. Clarify the Legal Boundaries for Self-Help

For more than a decade, academic and policy experts have debated the desirability of permitting self-help as a countermeasure to computer intrusions.[48] With defensive technology lagging a step or two behind offensive technologies, some have

proposed that the CFAA should allow intrusion victims to "hack back."[49] The Department of Justice has steadfastly maintained that the CFAA prohibits hacking back, but some commentators claim that it is justified as a form of limited self-defense.[50] Either way, Congress should weigh in to provide certainty about legal consequences for victims of computer intrusions who are tempted to return fire.

III. Conclusion

New threats from international and organized crime are changing the way that Americans use the internet. Legislation alone will not solve the problem of computer intrusions. Improved computer security will require efforts by law enforcement, yes, but also by the private sector, the computer security industry, and consumers. To that end, Congress should ensure that the CFAA provides law enforcement agencies the clearest possible authority for prosecuting serious threats while allowing security researchers to develop the tools that will make possible tomorrow's defense.

Endnotes

1 Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, Vanity Fair, Mar. 2015, http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg (last accessed Oct. 8, 2015); Dan Goodin, *Ashley Madison hack is not only real, it's worse than we thought*, Ars Technica, Aug. 19, 2015, http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/ (last accessed Oct. 8, 2015); Andrea Peterson, *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*, The Switch, The Washington Post, Oct. 8, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/ (last accessed Sept. 25, 2015); Ellen Nakashima, *Security firm finds link between China and Anthem hack*, The Switch, The Washington Post, Feb. 27, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/ (last accessed Oct. 8, 2015).

2 18 U.S.C. § 1030.

3 Paradoxically, re-centralization has not affected the physical decentralization that the internet enabled. Instead, cheap and fast network connectivity has allowed businesses to integrate computers that are physically located around the world into a single organizational whole.

4 Sanjay Ghemawat, Howard Gobioff, & Shun-Tak Leung, *The Google File System*, 37 Operating Systems Review 29 (Dec. 2003), *available at* http://research.google.com/archive/gfs.html (last accessed Oct. 8, 2015).

5 An Italian company called Hacking Team apparently sold their offensive technologies to American law enforcement agencies in addition to many foreign governments. *See* Andrea Peterson, *A company that sells hacking tools to governments just got hacked*, The Switch, The Washington Post, July 6, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/07/06/a-company-that-sells-hacking-tools-to-governments-just-got-hacked/ (last accessed Oct. 8, 2015).

6 Somewhat confusingly, the academic literature applies the "insider" label to former employees. This is because a former employee has an enormous informational advantage compared to an attacker who is a total stranger. See Chris Strohm & Jordan Robertson, *Companies' Worst Hacking Threat May Be Their Own Workers*, Bloomberg Business, Sept. 26, 2014, http://www.bloomberg.com/news/2014-09-26/companies-worst-hacking-threat-may-be-their-own-workers.html (last accessed Oct. 8, 2015).

7 National Cybersecurity and Communications Integration Center, *Combating the Insider Threat*, May 2, 2014, https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf (last accessed Oct. 8, 2015).

8 Brian Krebs, *The Internet of Dangerous Things*, Krebs on Security, Jan. 15, 2015, http://krebsonsecurity.com/2015/01/the-internet-of-dangerous-things/ (last accessed Oct. 8, 2015); Jai Vijayan, *Long-Running Cyberattacks Become the Norm*, Dark Reading, Jan. 2, 2015, http://www.DarkReading.com/attacks-breaches/long-running-cyberattacks-become-the-norm/d/d-id/1318392 (last accessed Oct. 8, 2015); Kelly Jackson Higgins, *More Than 100 Flavors of Malware Are Stealing Bitcoins*, Dark Reading, Feb. 26, 2014, http://www.DarkReading.com/attacks-breaches/more-than-100-flavors-of-malware-are-stealing-bitcoins/d/d-id/1141396 (last accessed Oct. 8, 2015); Australian Institute of Criminology, *Hacking Motives*, 6 High Tech Crime Brief at 1 (2005), *available at* http://aic.gov.au/media_library/publications/htcb/htcb006.pdf (last accessed Oct. 8, 2015).

9 *Common Types of Network Attacks*, Microsoft TechNet, https://technet.microsoft.com/en-us/library/cc959354.aspx (last accessed Feb. 9, 2015); Brian Krebs, *Anthem Breach May Have Started in April 2014*, Krebs On Security, Oct. 8, 2015, http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/ (last accessed Oct. 8, 2015); Seal, *Sony's Hacking Saga*, http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

10 Andrea Allievi & Earl Carter, *Ransomware on Steroids: Cryptowall 2.0*, Cisco Blog, Jan. 6, 2015, http://blogs.cisco.com/security/talos/cryptowall-2 (last accessed Feb. 9, 2015); 2013 Internet Crime Report 8-14, FBI Internet Crime Complaint Center, *available at* http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf (last accessed Feb. 9, 2015).

11 Dara Kerr, *Homeland Security busts child porn ring on Tor network*, CNET, Mar. 18, 2014, http://www.cnet.com/news/homeland-security-busts-child-porn-ring-on-tor-network/ (last accessed Oct. 8, 2015).

12 Michael Riley, *How Russian Hackers Stole the NASDAQ*, Bloomberg Business, July 17, 2014, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq (last accessed Oct. 8, 2015); Candid Wueest, *Targeted Attacks Against the Energy Sector*, Symantec (Jan. 13, 2014), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf (last accessed Oct. 8, 2015).

13 Sean Gallagher, *A hacked DDoS-on-demand site offers a look into mind of "booter" users*, Ars Technica, Jan. 19, 2015, http://arstechnica.com/security/2015/01/a-hacked-ddos-on-demand-site-offers-a-look-into-mind-of-booter-users/ (last accessed Oct. 8, 2015); Brian Krebs, *Spreading the Disease and Selling the Cure*, Krebs On Security, Jan. 26, 2015, http://krebsonsecurity.com/2015/01/spreading-the-disease-and-selling-the-cure/ (last accessed Oct. 8, 2015); Brian Krebs, *Exploring the Market for Stolen Passwords*, Krebs on Security, Dec. 26, 2012, http://krebsonsecurity.com/2012/12/exploring-the-market-for-stolen-passwords/ (last accessed Oct. 8, 2015); Brian Krebs, *The Scrap Value of a Hacked PC, Revisited*, Krebs on Security, Oct. 15, 2012, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/ (last accessed Oct. 8, 2015); Brian Krebs, *The Scrap Value of a Hacked PC*, Security Fix Blog, May 26, 2009, http://voices.washingtonpost.com/securityfix/2009/05/the_scrap_value_of_a_hacked_pc.html (last accessed Oct. 8, 2015).

14 Computer intrusion law is thus far from a specialized form of "cyberlaw" that Frank Easterbrook famously derided as "the Law of the Horse." Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207 (1996).

15 18 U.S.C. § 1030(a)(1)-(4).

16 *See* Restatement (Second) Torts, §§ 217, 218 (1977).

17 18 U.S.C. § 1030(a)(7).

18 *See* Restatement (Second) Torts, §§ 222A, 821D, cmts. b-d (1977); *but see* Intel Corp. v. Hamidi,71 P.3d 296 (Cal. 2003) (rejecting trespass to chattels theory in the absence of injury).

19 18 U.S.C. § 1030(a)(3).

20 18 U.S.C. § 1030(a)(4).

21 18 U.S.C. § 1030(a)(5). Other CFAA provisions define intrusion crimes related to interstate computer threats or extortion. 18 U.S.C. § 1030(a)(7).

22 The CFAA's confidentiality protections reach well beyond the common law tort of breach of privacy, requiring a showing merely that an attacker "obtained information" from the targeted computer. 18 U.S.C. § 1030(a)(1), (2); *see also* Restatement (Second) Torts, § 652A *et seq.* (1977) (discussing common law right of privacy). This has happened several times recently. *Ashley Madison Hackers Release Info of Man Who Paid to Erase His Profile*, Vice News, July 24, 2015, https://news.vice.com/article/ashley-madison-hackers-release-info-of-man-who-paid-to-erase-his-profile (last accessed Oct. 8, 2015); Seal, *Sony's Hacking Saga*, http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

23 Other federal statutes protect related interests. One taxonomy of these goods distills information security interests into four elements of information security assurance: confidentiality, integrity, availability, and accountability. Gary Stoneburner, *Underlying Technical Models for Information Technology Security*, NIST Spec. Pub. 800-33, Dec. 2001, *available at* http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (last accessed Oct. 8, 2015). An attacker can violate confidentiality interests by eavesdropping, by obtaining and releasing confidential information (subject to the First Amendment), or by transferring intellectual property without consent. *See generally* Department of Justice, Office of Legal Education, *Prosecuting Computer Crimes* (2013), *available at* http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (last accessed Oct. 8, 2015). Information itself may be protected from interference or misuse by several other statutes, which prohibit eavesdropping and trafficking in eavesdropping devices, identity theft, spam, wire fraud, and various forms of communication interference. Several of these criminal statutes, including the CFAA, have an accompanying civil cause of action. *See*, *e.g.*, 18 U.S.C. § 1030(g). According to statistics from the Federal Judicial Center, the CFAA was the major offense in between 93 and 120 criminal prosecutions per year (with no comparable statistics available for the civil cause of action). Federal Judicial Center, *Federal Judicial Caseload Statistics*, Table D-2 at 2 (2014), *available at* http://www.uscourts.gov/uscourts/Statistics/FederalJudicialCaseloadStatistics/2014/tables/D02DMar14.pdf (last accessed Oct. 8, 2015).

24 *See* 18 U.S.C. § 1030(a)(3) (forbidding "access" that "affects" the use of a government computer).

25 18 U.S.C. § 1030(a)(5).

26 18 U.S.C. §§ 1030(a), (e)(6).

27 *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. Rev. 1596, 1598-99 (2003).

28 18 U.S.C. § 1030(e)(2).

29 Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1568 (2010) ("Because every computer connected to the Internet is used in interstate commerce or communication, it seems that every computer connected to the Internet is 'protected computer' covered by 18 U.S.C. § 1030.").

30 Congress need not be involved, of course. The Department of Justice could consider reprioritizing federal resources toward greater threats.

31 18 U.S.C. § 1030(c)(2)(B)(ii). The CFAA's reliance on state law undermines uniformity by making federal enforcement vary from state to state and creating the possibility of notice or vagueness problems. In addition, incorporating tort law into the substance of a criminal statute distorts the cost-benefit tradeoffs of tort law by creating a substantial risk of overpunishment. Whereas remedies for tortious conduct tend to be mostly compensatory, criminal statutes like the CFAA also provide for penalties as retribution and deterrence.

32 18 U.S.C. §§ 1030(a), (e)(6).

33 Kerr, *supra* note 29, at 1571-87.

34 Updated Administration Proposal: Law Enforcement Provisions, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf (last accessed Oct. 8, 2015).

35 *See* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (misuse of Social Security Administration computers); United States v. John, 597 F.3d 263 (5th Cir. 2010) (exceeding authorization in furtherance of a fraud crime); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (Posner, J.) (breach of duty of loyalty and violation of employment agreement); *but see* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203-04 (4th Cir. 2012) (violation of company policy); United States v. Nosal, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc) (Kozinski, J.) (limiting "exceeds authorized access" violations under CFAA to access violations, not use violations).

36 Not all misappropriations would become purely civil matters, however, since federal law also prohibits theft of trade secrets. 18 U.S.C. § 1832.

37 Interestingly, the common law pleading rules forbade the use of an "exceeds authorized access" theory for trespass to chattels in which the defendant remained in contact with a chattel if the original contact was made with the possessor's consent. Restatement (2d) Torts, § 217, cmt. g (1977). Because the distinction between the two was one of pleading, however, the Second Restatement made no such distinction.

38 In one case, an expert exploited a security vulnerability for the purpose of notifying consumers about the existence of the vulnerability. Kevin Poulsen, *Prosecutors admit error in whistleblower conviction*, SecurityFocus, Oct. 14, 2003, http://www.securityfocus.com/news/7202 (last accessed Oct. 8, 2015). Although the researchers was eventually cleared, he no doubt would have preferred to avoid an erroneous prosecution in the first place.

39 *See*, *e.g.*, *Of Privacy, Security, and the Art of Scanning*, Shadowserver Foundation, June 23, 2015, http://blog.shadowserver.org/2015/06/23/of-privacy-security-and-the-art-of-scanning/ (last accessed Oct. 8, 2015); Dan Kaminsky, *RDP and the Critical Server Attack Surface*, Dan Kaminsky's Blog, Mar. 18, 2012, http://dankaminsky.com/2012/03/18/rdp/ (last accessed Oct. 8, 2015).

40 *See* United States v. Drew, 259 F.R.D. 449, 458-62 (C.D. Cal. 2009) (creating profile on MySpace containing false age, picture, and pretending to be a juvenile violated CFAA); *see also* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62-63 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access. (Whether public policy might in turn limit certain restrictions is a separate issue.) Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers."); *see also* Kerr, *supra* note 29, at 1617-21 (discussing access and authorization).

41 Indeed, the private-sector coalition that fought the Conficker Worm identified "lack of authority" to fix the infected computers as one of the many problems that hindered the fight against the worm. The Rendon Group, Conficker Working Group: Lessons Learned 46 (Jan. 2011), *available at* http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf (last accessed Oct. 8, 2015). The Shadowserver Foundation plays a central role in tracking and investigating botnets, which are networks of computers owned by innocent parties that are nevertheless under the control of some malicious user. *See* Shadowserver Foundation, https://www.shadowserver.org/wiki/ (last accessed Oct. 8, 2015).

42 Ed Felten, *Why were CERT researchers attacking Tor?*, Freedom to Tinker, July 31, 2014, https://freedom-to-tinker.com/blog/felten/why-were-cert-researchers-attacking-tor/ (last accessed Oct. 8, 2015).

43 *See* Brian Krebs, Spam Nation 233-36 (2014); *Microsoft takes on global cybercrime epidemic in tenth malware disruption*, The Official Microsoft Blog, June 30, 2014, http://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption/ (last accessed Oct. 8, 2015); Department of Justice Press Release, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator, June 2, 2014, *available at* http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (last accessed Oct. 8, 2015); Department of Justice Press Release, *Department of Justice Takes Action to Disable International Botnet*,

Apr. 13, 2011, *available at* http://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet (last accessed Oct. 8, 2015).

44 Kelly Jackson Higgins, *How to Avoid Collateral Damage in Cybercrime Takedowns*, InformationWeek DarkReading, June 25, 2015, http://www.darkreading.com/cloud/how-to-avoid-collateral-damage-in-cybercrime-takedowns/d/d-id/1321040 (last accessed Oct. 8, 2015).

45 Tal Klein, *The Tao of Responsible Disclosure*, Wired, http://www.wired.com/insights/2014/10/the-tao-of-responsible-disclosure/ (last accessed Oct. 8, 2015).

46 In addition to legal questions, such activities raise ethical questions about informed consent. Ethical guidelines for federal research of this type are still in their infancy. *See* The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research 13 (2012), *available at* http://www.dhs.gov/sites/default/files/publications/CSD-Menlo-PrinciplesCORE-20120803.pdf (last accessed Oct. 8, 2015).

47 Andrea Peterson, *Find a security bug in your GM car? The automaker wants to hear about it.*, The Switch, The Washington Post, Oct. 5, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/10/05/find-a-security-bug-in-your-gm-car-the-automaker-wants-to-hear-about-it/ (last accessed Oct. 8, 2015); *Google Vulnerability Reward Program (VRP) Rules*, Google Application Security, https://www.google.com/about/appsecurity/reward-program/ (last accessed Oct. 8, 2015); *see generally The Bug Bounty List*, Bugcrowd. https://bugcrowd.com/list-of-bug-bounty-programs (last accessed Oct. 8, 2015).

48 *See*, *e.g.*, Richard A. Epstein, Intel v. Hamidi*: The Role of Self-Help in Cyberspace?*, 1 J.L. Econ. & Pol'y 147 (2005).

49 Summary, CSIS/DOJ Active Cyber Defense Experts Roundtable, Mar. 10, 2015, *available at* http://www.justice.gov/criminal/cybercrime/docs/CSIS%20Roundtable%205-18-15.pdf (last accessed Oct. 8, 2015); *The Hackback Debate*, Steptoe Cyberblog, Nov. 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (last accessed Oct. 8, 2015).

50 *The Hackback Debate*, Steptoe Cyberblog, Nov. 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ (last accessed Oct. 8, 2015).