University of Miami National Security & Armed Conflict Law Review

7-1-2015

The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work

Kristin Westerhorstmann

Recommended Citation
Kristin Westerhorstmann, *The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work*, 5 U. Miami Nat'l Security & Armed Conflict L. Rev. 145 (2015)
Available at: http://repository.law.miami.edu/umnsac/vol5/iss2/9

The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work

Kristin Westerhorstmann[*]

ABSTRACT

Each year, the frequency and severity of cyber-attacks continue to increase. With each new threat comes more pressure on the government to implement an effective plan for preventing these attacks. The first instinct has been to attempt either to enact more laws, or to broaden the scope of already-existing laws such as the Computer Fraud and Abuse Act ("CFAA"). The CFAA, the federal hacking statute, has been called the "worst law in technology" for its excessively broad scope and vague provisions, which have resulted in arbitrary and discriminatory enforcement, conflicts with the federal private nondelegation doctrine, and in overcriminalization. In addition, significant amendments throughout the past two decades have left the protection of privacy—once a central interest of the original CFAA—minimalized to the point of forgotten. What was once a narrow statute formulated to prevent hackers from stealing government information and breaching critical infrastructure has turned into an unrecognizably broad statute that criminalizes common computer use such as deleting cookies, lying about one's age on Facebook, or checking personal email

[*] Chief Symposium Editor, 2015-2016, University of Miami National Security & Armed Conflict Law Review; Juris Doctor Candidate 2016, University of Miami School of Law. Thank you to Sarah Fowler, Chief Notes Editor 2014-2015, for all of your hard work, commitment, and patience. Thank you to all of my friends and family for your unwavering and constant support. A special thank you to my advisor and internet hero, Professor Mary Anne Franks, for all of your support, direction, and advice.

while at work. In order to actually combat cyber-attacks, protect people's online interests, and remedy the problems facing the current CFAA, this Note argues that the broad, catchall language of the statute must be discarded to make way for a new, more narrow, specific framework.

Table of Contents

I. INTRODUCTION

Since the Computer Fraud and Abuse Act ("CFAA") was adopted in 1986,[1] the internet has grown at an unpredictable speed. What was considered hacking in 1986 was very limited and one-dimensional, and generally aimed only at government and business computers, which outweighed personal computers by a ratio of three to one.[2] Even simple hacking methods used today, such as distributed-denial-of-service attacks

[1] 18 U.S.C. § 1030 (2012).

[2] Charlotte Decker, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. Cal. L. Rev. 959, 960 (2010) [hereinafter *Cyber Crime 2.0*].

(DDoS),[3] were not fully conceptualized when the statute was enacted. Today, personal computers substantially outweigh government computers and the internet has shifted from being a rare commodity to a necessary utility, so Congress has tried to respond by attempting to extend its reach to all possible areas of computer misuse. Once a narrow statute formulated to combat hacking threats to national security and financial data, the CFAA is now used by prosecutors to pile on major charges for minor crimes such as violating a website's Terms Of Service ("TOS") agreement by creating a fake online profile.[4] Its wide breadth, unclear language, and confusing application has branded the statute by some as the "worst law in technology."[5]

Although there are many laws that govern computers and the internet, the CFAA is the primary statute used for hacking. The language in 18 U.S.C § 1030(a)(2)(C) prohibiting the unauthorized use of "information [obtained] from any protected computer" encompasses an immeasurable amount of illicit computer activity without making appropriate distinctions or limitations.[6] The wide breadth provided by this language gives prosecutors extremely broad discretion, which has led to enforcement that arbitrarily targets minor violations.[7] Furthermore, the lack of clarity has also led to a circuit split regarding its scope[8] and to questions of its constitutionality via the void-for-vagueness doctrine and the private nondelegation doctrine.[9] The CFAA's broad purpose has only weakened its practical effect, which is now, seemingly, to arbitrarily stop people from doing generally "bad" things on the internet.

In 2013, hackers stole credit and debit card data from more than 40 million Target customer accounts.[10] In 2014, Community Health Systems Inc. was the victim of an international cyber-attack that saw

[3] A distributed denial-of-service attack is an attempt to make a computer or a network unavailable to users by either crashing or flooding the service. Commonly, an attack involves saturating the target computer or network with external communication requests so that it cannot respond to traffic, leading to a server overload. *See infra* pp. 25-26.

[4] *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[5] *See* Tim Wu, *Fixing the Worst Law in Technology*, The New Yorker (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

[6] The term "protected computer" encompasses all computers with internet access. *See* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc); *see* 18 U.S.C. §1030(a)(2)(C); *see infra* pp. 5-6.

[7] *See infra* pp. 7, 9-10, 13-14.

[8] *See Nosal,* 676 F.3d 854; *contra* United States v. John, 597 F.3d 263 (5th Cir. 2010).

[9] *See infra* pp.8-13.

[10] Elizabeth A. Harris & Nicole Perlroth, *Target Missed Signs of a Data Breach,* N.Y. Times (Mar. 13, 2014), http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html.

personal data and medical records, belonging to 4.5 million patients, stolen.[11] Weeks later, collections of intimate, private pictures belonging to more than 100 celebrities, nearly all women, were stolen from their iCloud accounts and were posted and distributed on websites such as 4chan, Imgur, Reddit, and Tumblr.[12] To combat this demonstration of both inadequate protection from cyber-attacks and ineffective methods of apprehending hackers, Congress has sought to force people to take computer crime more seriously by appearing tough on crime and by appearing to take a proactive step toward taking down cyber-criminals. An effective CFAA reform, however, must incorporate and balance three virtual interests outlined in the statute: (1) the protection of privacy, (2) the facilitation and allowance of a free flow of information, and (3) the security of transactions and data.[13]

This Note will proceed in four Parts. Part I provides a contextual legislative history of the CFAA relevant to the discussion of reform. It provides background information about the harms that Congress originally sought to protect from by its enactment in 1986, an analysis of how those harms today have evolved to become more expansive and complicated, and an overview of how the CFAA is used primarily today in response. Part II examines the major issues that plague the CFAA, including problems due to the broad, vague language of § 1030(a)(2)(C); its tendency to delegate the power of defining criminality to private individuals; and its failure to meet basic criminal justice and crime control goals. Part III presents arguments set forth by advocates of a CFAA reform, which suggest better defining terms such as "unauthorized access," as well as to address the penalization of TOS violations. This Part also argues that these approaches offer only a quick fix that do not adequately address the deep-rooted issues surrounding the statute, and that an effective CFAA reform requires a more specific framework. Finally, Part IV highlights the lack of recognition or protection for individual privacy on the internet and discusses a need for an express provision in the CFAA that better protects this interest. It also

[11] Gail Sullivan, *Chinese Hackers may have Stolen your Medical Records*, The Washington Post (Aug. 19, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/08/19/chinese-hackers-may-have-stolen-your-medical-records/.

[12] Dave Lewis, *iCloud Data Breach: Hacking and Celebrity Photos*, Forbes (Sept. 2, 2014), http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/.

[13] "Assuring the free flow of information, the security and privacy of data . . . are all essential to American and global economic prosperity, security, and the promotion of universal rights." *See* International Strategy for Cyberspace p. 3; *see* Cyber Security Forum Initiative, *Privacy, National Security, and Mass Surveillance,* Tripwire (Apr. 28, 2014), http://www.tripwire.com/state-of-security/government/privacy-national-security-and-mass-surveillance/.

suggests reconstructing the statute to proscribe specific categories of activity, and to focus more on the harms of hacking rather than build on the current framework, which addresses merely the conduct of hacking through a catchall provision.

II. Legislative History: From Narrow Statute to "Worst Law in Technology"

Despite the wide breadth allotted to the CFAA today, it was originally enacted as a very narrow statute. Congress passed an omnibus Comprehensive Crime Control Act in 1984, which included the first ever federal computer crime statute in response to the development of the internet and to various new technologies.[14] The Act established three new federal crimes: misusing a computer to (1) obtain national security secrets, (2) to obtain personal financial records, or (3) by hacking into U.S. government computers.[15] Rather than the broad and mostly ambiguous spectrum of interests the CFAA caters to today, its precursor was tailored to specific and corresponding government interests: national security, financial record security, and government property. The first significant amendment to the Act came in 1986, in what was first recognized as the Computer Fraud and Abuse Act.[16] The amendment detailed three additional computer crimes, prohibiting unauthorized access (1) with the intent to defraud; (2) in damaging, altering, or destroying information, thereby causing $1,000 or more in losses or impairing a medical diagnosis, treatment, or care of another; or (3) in trafficking passwords.[17] Computers covered under the first two subsections were limited to "Federal interest" computers, either used by the U.S. government or financial institutions, or used by computers in two or more states.[18] While this seems like a broad range of computers, it was actually quite limited, as very few computer crimes reached over an interstate network at the time.[19]

[14] Sarah A. Constant, *The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare—The Case Against Aaron Swartz and the Need to Reform the CFAA*, 16 Tul. J. Tech. & Intell. Prop. 231, 232 (2013); *see* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 1976.

[15] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1564 (2010).

[16] *Id.*

[17] *Id.* at 1565.

[18] *Id.*

[19] *Id.*

In 1986, only 8.2% of American households contained a computer.[20] The internet grew out of the Defense Department and was originally a tool for only the federal government and certain academic institutions.[21] Today, 84% of American households own a computer, and 73% have an internet connection.[22] With the unprecedented and rapid expansion of computer technology, the methods and sophistication of computer crime, as well as the pool of people capable and willing to commit such hacking, grew correspondingly. To combat this constantly-growing trend of expansion, Congress passed several amendments to the CFAA, a pair of them notoriously and dramatically widening its scope to result in the ever-broad range of activity that the CFAA prohibits today.[23]

Perhaps the most dramatic amendment to the CFAA came from the Economic Espionage Act of 1996.[24] The original 1984 statute provided § 1030(a)(2), which prohibited unauthorized access in obtaining financial records from financial institutions, card issuers, or consumer reporting agencies; but the 1996 amendment expanded this section to bar unauthorized access that obtained *any* information of *any* kind, if involved in interstate or foreign communication, effectively criminalizing all interstate computer "misuse."[25] Legislative history clarified that "obtaining information" included simply reading it or viewing an image.[26] The second major change came from replacing the category of "Federal interest computers" with "protected computers" in § 1030(a)(2), only requiring that the computer be "used" in interstate commerce, rather than be physically located in two or more states, as well as removing the requirement that it be used by a government or financial institution.[27] Because almost every computer connected to the Internet is "used" in interstate commerce by that definition, the term "protected computer" covered nearly all computers with an internet connection.

Twelve years later, the most recent significant expansion came from the Identity Theft Enforcement and Restitution Act of 2008, again

[20] *Cyber Crime 2.0*, *supra* note 2 at 960.

[21] *Id.*

[22] Lee Rainie & D'Vera Cohn, *Census: Computer Ownership, Internet Connection Varies Widely Across U.S.*, Pew Research Center (Sept. 19, 2014), http://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s/.

[23] *See infra* pp. 5-6.

[24] Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

[25] *Id.*

[26] Kerr, *supra* note 15, at 1567 (citing S. REP. NO. 99-432, at 6 (1986) *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (noting that "obtaining information" in the statute includes "mere observation of the data")).

[27] *Id.*; Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488.

triggering a heavy impact.[28] First, it removed the requirement of interstate communication under § 1030(a)(2), and effectively solidified the CFAA's broadest section, § 1030(a)(2)(C), which prohibits *any* unauthorized access to *any* protected computer that retrieves *any* information of *any* kind.[29] The amendment also, once again, expanded the definition of "protected computer" from computers simply "used" in interstate commerce, to computers "used in *or affecting*" interstate commerce.[30] Modern interpretation of the commerce clause allows Congress to regulate any class of economic activities that in its aggregate, simply affect interstate commerce.[31] This means that the term "protected computer" now applies to all computers that can be regulated under the commerce clause, regardless if actually used in interstate commerce—essentially, all computers.

The current version of the CFAA prohibits seven types of illicit computer activity: (1) obtaining national security information; (2) accessing, without or by exceeding authorization, a computer and obtaining information; (3) trespassing in a government computer; (4) accessing a computer with intent to defraud; (5) damaging a protected computer or data; (6) trafficking in passwords; and (7) using computers for extortion.[32] While most of the government's interests in prohibiting hacking are enumerated in these categories, § 1030(a)(2)(C) acts essentially as a broad catchall for all other interests recognized after 1986, including the interest in protecting privacy, serving as the response to the exponential computer and internet growth. The increased skill and sheer number of people capable and willing to commit these kinds of computer crimes has led to extreme difficulty and frustration in locating and apprehending high profile hackers.[33] As a result, law enforcement today has mostly relied on the broad scope of § 1030(a)(2)(C) to demonstrate the CFAA's power, seemingly to save it from appearing completely ineffective.

First, the CFAA is often used to express that the government is "tough on [computer] crime." In 2011, Aaron Swartz was charged under the CFAA, facing up to 35 years in prison as well as a fine of up to $1 million for "exceeding authorization" by downloading academic articles

[28] *See* Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 108-275, Tit II, 122 Stat. 356.

[29] *Id.;* Kerr, *supra* note 15, at 1569.

[30] *Id.;* Kerr, *supra* note 15, at 1570.

[31] Kerr, *supra* note 15, at 1570; *see* Gonzales v. Raich, 545 U.S. 1, 17 (2005).

[32] Constant, *supra* note 14, at 235.

[33] The year 2014 saw an unprecedented amount of highly visible hacks and almost no arrests or convictions of those involved. Hackers responsible for the Target breach, the iCloud breach, and the Sony breach are all still at large. *See infra* pp. 24-26.

from JSTOR.[34] Despite JSTOR's statements that it did not wish to see Aaron prosecuted and the minimal, if any, harm Aaron caused, United States Attorney Carmen Ortiz sought full repercussions to "deter others from committing similar offenses."[35] Second, it is also common for law enforcement to use the CFAA to go after, without more, those who the government dislikes or considers unpopular. Widely known internet "troll" Andrew Auernheimer, nicknamed "weev," was sentenced to 41 months in prison in 2013 for noticing a hole in AT&T servers, allowing him to collect email addresses of 110,000 iPad users, which were then published by *Gawker* in redacted form.[36] While weev has a long, ugly history of internet controversy and harassment, federal prosecutors used this incident to charge him for "accessing data without authorization" under § 1030(a)(2)(C), despite the fact that AT&T made the information publically available.[37] Finally, it seems as though the government has attempted to use the CFAA to punish non-criminal, yet morally reprehensible, acts that just happen to involve a computer. In a widely publicized cyberbullying case from 2009, Lori Drew created a fake Myspace profile of a fake sixteen-year-old boy named Josh Evans, and then made hurtful comments to a neighbor, thirteen-year-old Megan Meier, who committed suicide later that same day.[38] Because Drew's conduct did not implicate any other criminal statute, prosecutors used her violation of Myspace's TOS agreement to bring charges under § 1030(a)(2)(C).[39]

III. Issues: Void-For-Vagueness, Delegation, and Crime Control

The most common criticisms of the broad scope of the CFAA come from its catchall provision in § 1030(a)(2)(C), and its absence of definitions for the terms "without authorization" and "exceed[ing] authorized access" from § 1030(a)(2). Read together, these sections criminalize "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and obtains information from any protected computer."[40] This section is potentially so broad as to classify as federal criminals those who share Netflix accounts, employees

[34] Timothy P. O'Toole, *Digital Defense: Meeting the Challenges That the Computer Fraud and Abuse Act Poses,* 37-OCT Champion 44, 45 (2013).

[35] *Id.* at 45.

[36] *Id.* at 45-46.

[37] *Id.*

[38] Kerr, *supra* note 15, at 1578-79.

[39] *Id.* at 1579-80.

[40] *See* 18 U.S.C. § 1030(a)(2)(C).

who check their personal email at work, or the man who violates a dating website's TOS agreement by describing himself as tall, dark, and handsome, when he is actually nothing of the sort.

There are generally two ways to interpret what the statute refers to as "unauthorized access." First, narrowly, this could mean accessing a computer by circumventing its security system or breaking through code-based restrictions.[41] Second, the broader interpretation, the contract-based approach, defines "exceeding authorized access" in a way that violates norms of computer use or a contract, such as violating a website's TOS conditions or using a work computer to access Facebook.[42] What is considered "access" and what makes it "unauthorized" is universally unclear. This lack of clarity in the authorization terminology often implicates the void-for-vagueness doctrine, as well as the federal private nondelegation doctrine, while the scope of the catchall § 1030(a)(2)(C) provision runs contrary to the goals of the CFAA, and against basic, essential goals of crime control.

A. Void-For-Vagueness

Broadly, the void-for-vagueness doctrine requires Congress to specify exactly what is prohibited. This doctrine, rooted in the Due Process Clause, is designed to combat the traditional problems suffered by vague statutes, including arbitrary and discriminatory enforcement, problems of notice, and apparent irrationality or absurdity.[43] Void-for-vagueness questions are evaluated based on two inquiries. First, whether the law is "so vague and standardless that the public is unsure of what it prohibits," in which "it leaves courts free to decide what is prohibited" in each particular case.[44] The second inquiry addresses arbitrary and discriminatory enforcement, asking whether the statute "establishes minimal guidelines to govern law enforcement."[45] Rather than its effect on the public, this test focuses on how much discretion the statute gives to police. If the statute leaves enforcement up to the "whim of any police officer," it is unconstitutionally vague.[46]

[41] Kerr, *supra* note 15, at 1571-72.

[42] *Id.*

[43] *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 751 (2010) [hereinafter *Private Nondelegation*].

[44] Kerr, *supra* note 15, at 1573 (quoting Giaccio v. Pennsylvania, 382 U.S. 399, 402 (1966)).

[45] *Id.* at 1574 (quoting Kolender v Lawson, 461 U.S. 352, 358 (1983)).

[46] *Id.* (quoting Shuttlesworth v. City of Birmingham, 382 U.S. 87, 90 (1965)); An anti-gang congregation ordinance in Chicago prohibited people from "remain[ing] in any one place with no apparent purpose." The Court deemed the ordinance unconstitutionally vague because "apparent purpose" does not have a common meaning that an ordinary

In one of the most infamous cases involving the CFAA, a Federal District Court in California overturned a conviction for creating a fake Myspace profile in *United States v. Drew* via the void-for-vagueness doctrine.[47] The government's theory was that Lori Drew's creation of the false profile, "Josh Evans," had violated Myspace's TOS conditions, which rendered her access to Myspace's network without authorization under § 1030(a)(2)(C).[48] TOS contracts are written at the complete discretion of the website creator, are long and mostly unread by the vast majority of users, and are subject to change without prior notice or without any notification whatsoever. To extend § 1030(a)(2)(C) to simple TOS violations would have required permitting the criminalization of otherwise lawful conduct solely based on an agreement between private parties, subject to change at any time. Although the court did not explicitly agree with this particular line of reasoning, it held that under this interpretation, ". . . federal law enforcement entities would be improperly free to 'pursue their personal predilections,'" and that all manner of situations could be prosecuted.[49] The court in *Drew* took the more narrow approach to defining the authorization terminology to save the statute from being unconstitutionally vague, however, not all courts have followed suit. The Fifth Circuit in *United States v. John* took the broader interpretation of "exceeds authorization," by holding that an employee violates § 1030(a)(2)(C) when she uses her work computer beyond the scope of employment.[50] The court, relying on an agency approach to interpretation, held that the CFAA prohibited both unauthorized acquisition of information from a computer and information obtained after authorized use but which is outside the realm of authorization.[51] As discussed again in *United States v. Nosal* by the Ninth Circuit, this interpretation allows for criminalizing any kind of non-work related computer access, such as checking personal email.[52]

person would know with regard to whether or not their conduct violated the ordinance. In addition, the ordinance would provide absolute discretion to police officers to determine which actions were without an "apparent purpose." *see* City of Chicago v. Morales, 527 U.S. 41 (1999) (plurality opinion).

[47] *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[48] *Id.* at 453; *see also* 18 U.S.C. § 1030(a)(2)(C).

[49] *Id.* at 467.

[50] *See* United States v. John, 597 F.3d 263 (5th Cir. 2010) (holding that an employee had exceeded authorized access when she provided another company customer accounts, in the form of scanned images of checks or printouts of computer screens, belonging to the company of which she was employed with at the time).

[51] *Id.*

[52] *See* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (holding that an employee does not violate the CFAA when he violates the company computer terms of

One of the leading proponents of CFAA reform, Professor Orin Kerr, argues that the wide scope requires courts to adopt the narrow interpretation to avoid invalidating the statute completely, precisely because of the surprisingly uncertain meaning of "access without authorization" and "exceeds authorized access" as well its "remarkable breadth."[53] Because the scope of the CFAA falls entirely on the meaning of unauthorized access, courts must adopt the definition that does not criminalize common use of computers because this would give police the power to arbitrarily arrest any typical "protected" computer user at their discretion.[54] However, even a narrow reading of the statute would present many of the same overcriminalization problems that run afoul of the interests and goals of the statute.

B. Delegation

In addition to the void-for-vagueness doctrine, challenges to the scope of the CFAA can be framed under the federal private nondelegation doctrine. The nondelegation doctrine prevents Congress from delegating federal lawmaking power to self-interested, unsupervised, and democratically unaccountable private parties.[55] The Supreme Court originally addressed this issue in *Carter v. Carter Coal Co.* in 1936, although lower courts have since identified three primary factors that drive the question of whether or not a statute violates the private nondelegation doctrine:[56] First, whether the delegation of power authorizes private actors to make a law in a non-neutral, transparent way;[57] second, whether affected parties are adequately represented in the private lawmaking process;[58] and finally, the analysis asks whether the state retains control over the private delegate, which seems to be the most important factor.[59] For example, courts will typically allow a delegation of rule-making power that is subject to governmental approval, disapproval, or modification, which allows the government to retain responsibility.[60] In contrast with all of these factors, a broad reading of the CFAA delegates lawmaking power directly to private website creators, allowing them complete latitude to create, modify, or

use agreement by downloading "highly confidential and proprietary" data for purposes of starting a competing business); *contra John*, 597 F.3d 263.

[53] Kerr, *supra* note 15, at 1562.

[54] *Id.* at 1577.

[55] *Private Nondelegation, supra* note 43, at 761.

[56] *Id.* at 763-64; *see* Carter v. Carter Coal Co., 298 U.S. 238 (1936).

[57] *Id.* at 764-65.

[58] *Id.*

[59] *Id.*

[60] *Id.* at 766; *see* Sunshine Anthracite Coal Co. v. Adkins, 310 U.S. 381 (1940).

delete sections of their TOS agreements without any notice or notification to users.

Most notably from the opinion in *Drew*, the court explicitly stated it was not deciding "whether or not Congress *could* base criminal liability on violations of a company or website's computer use restrictions," but rather on the particular issues of notice and potential for arbitrary and discriminatory enforcement presented specifically by the unclear language of the statute.[61] The CFAA as written, given the lack of clear definitions, may violate the void-for-vagueness doctrine, although if the Supreme Court were to set a clear precedent via even the broadest interpretation, this could cure the vagueness. In this scenario, or under any broad reading of unauthorized access, it may be appropriate to frame the challenge as violating the private nondelegation doctrine. At a minimum, courts have required at least some kind of review or collaboration with government to assure fair and rational restrictions, while TOS agreements or employee computer use stipulations involve none whatsoever.[62] These essentially-unilateral contracts also establish significant disparities in power between TOS drafters and service users.[63] For example, users must agree to Facebook's TOS conditions before they are able to create an account. Users have no negotiation power if they oppose the terms, and Facebook has no affirmative duty to alert users when these terms change. Additionally, whether or not the contract drafters will exercise power fairly and transparently is completely at the will of the drafter. Undoubtedly, not all user agreements and employee computer usage rules are one-sided or unfair, but there is no way to distinguish these under the CFAA from those that would abuse their broad power to impose arbitrary violations that would be considered federal crimes.[64]

C. Interests and Crime Control

Since the CFAA was first enacted, the sheer number of hackers have grown and their methods have evolved, so Congress has responded by adding new sections to the CFAA that reflect a need for additional protection for the sake of its interests, which can now loosely be considered security, both national and of financial data and transactions; privacy; and a free flow of information. While most of the additional sections can be traced directly back to interests in security or a free flow of information, or sometimes both, the development of the catchall

[61] *Id.* at 756; *see* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[62] *Id.* at 770.

[63] *Id.* at 771.

[64] *Id.*

language in § 1030(a)(2)(C) seems to be Congress' only answer to both protecting privacy, and generally, to controlling the continuously growing internet. By generally prohibiting unauthorized access and obtaining information from "protected computers," rather than creating new sections, § 1030(a)(2)(C) gives broad power for the law to reach whatever future hazards may arise, and with it simply an *implied* protection for privacy. Despite this presumed intention, this language is egregiously overinclusive and broad, and without specific parameters it criminalizes almost all computer "misuse."

Aaron Swartz wrote a script that allowed him to quickly download a large number of articles from JSTOR, presumably with the intent to make them freely available to the public.[65] Rather than hack into or circumvent JSTOR's system, Aaron used his authorized access as a student to download articles.[66] Despite JSTOR's refusal to pursue the case or to press civil charges, the United States Attorney's office charged Aaron with thirteen felony counts, including wire fraud and computer fraud under the CFAA, largely due to the fact that he simply used fake names and IP addresses to conceal his identity.[67] Facing charges that carry a penalty of up to 35 years in prison and a $1,000,000 fine, Aaron committed suicide in his apartment shortly before proceedings began.[68] Similarly, weev's AT&T follies were intended to highlight AT&T's faulty network security and to demonstrate its carelessness in protecting its customer's personal information.[69] Like Aaron, weev did not bypass any kind of security system or obtain passwords, but merely noticed the hole that was leaking email addresses.[70] After *Gawker* published the email addresses in redacted form, AT&T closed the hole and notified its customers.[71] weev was convicted in New Jersey for accessing data, the email addresses, without authorization under § 1030(a)(2)(C).[72]

In an interesting twist, the Department of Justice recently used the *exact same* tactic as weev, collecting information through a leak, to locate and prosecute Ross Ulbricht, the apparent mastermind behind an illegal narcotics website called "Silk Road."[73] In *Auernheimer,* the DOJ

[65] Constant, *supra* note 14, at 241-43.

[66] *Id.* at 240.

[67] *Id.* at 241-42.

[68] *Id.* at 242-43.

[69] O'Toole, *supra* note 34, at 45.

[70] *Id.* at 45-46.

[71] *Id.*

[72] The Third Circuit eventually dismissed his conviction because New Jersey was an improper venue. *Id.* at 46.

[73] *See* Orin Kerr, *Does Obtaining Leaked Data from a Misconfigured Website Violate the CFAA?*, The Washington Post (Sept. 8, 2014), http://www.washingtonpost.com/

argued that public data on a server was protected if an ordinary user could not find it and if it was not intended to be seen by the public.[74] In the Silk Road case, however, the DOJ has expressed the opinion that there is nothing unlawful about taking advantage of a server misconfiguration to obtain data inadvertently leaked by the server because that information is fully accessible to the public.[75] The disparity in these two conflicting statements, spoken less than two years apart, illustrates perfectly how the vague and broad language of the CFAA is used to give complete discretion to law enforcement and the government to decide exactly which ambiguous "violation" to criminalize. The court in *Nosal*, referring to *Drew*, foresaw this difficulty when it explained: "It's not clear we can trust the government when a tempting target comes along . . . The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after."[76]

In another somewhat ironic twist, the broad language of the CFAA, in its current form, prohibits techniques that users commonly utilize to protect their own privacy, and to enhance their computer security. Deleting cookies is a popular method in both maintaining privacy and computer security. Cookies are essentially trackers that websites use to monitor user activity, especially searches, preferences, and page visits.[77] In addition to burdening user privacy and security, cookies also slow computer speed.[78] Cookies are commonly used by websites for targeted advertising based on searches or clicks, or for their paywalls.[79] For example, *The New York Times,* which imposes a 10 articles-per-month limit for nonsubscribers, uses cookies to track the number of articles a particular user has read.[80] This limit is easily circumvented by deleting

news/volokh-conspiracy/wp/2014/09/08/does-obtaining-leaked-data-from-a-misconfigured-website-violate-the-cfaa/.

[74] *Id.*; *see* U.S. v. Auernheimer, 748 F.3d 525 (3rd Cir. 2014).

[75] *Id.*

[76] O'Toole, *supra* note 34, at 48 (quoting United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (referring to United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009))).

[77] *See* Electronic Frontier Foundation, *The Computer Fraud and Abuse Act Must Allow Anonymity and Privacy to Protect the Security of Ordinary Users and Promote Human Rights Around the Globe*, https://www.eff.org/files/filenode/cfaa-privacy-anonymity.pdf.

[78] Ashkan Soltani, *Protecting Your Privacy Could Make You the Bad Guy,* Wired (Jul. 23, 2013), http://www.wired.com/2013/07/the-catch-22-of-internet-commerce-and-privacy-could-mean-youre-the-bad-guy/.

[79] *Id.*

[80] *Id.*; *see also* Jennifer Granick, *Thoughts on Orin Kerr's CFAA Reform Proposals: A Great Second Step*, The Center for Internet and Society (Jan. 23, 2013), http://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step.

cookies periodically, as the FTC even recommends.[81] It is by no means a stretch to consider exceeding the 10 articles-per-month limit, even unintentionally, by deleting cookies as "unauthorized" access under the CFAA. Additionally, not all hacking is malicious, some even benevolent. In fact, it is common for companies to offer rewards, or "bug bounties" for hackers who can successfully circumvent their security system due to a flaw, or "bug," and then bring it to their attention.[82] Under the CFAA, there is no way to distinguish these "white hat" hackers, from those with more sinister "black hat" motives.

Finally, the catchall language from § 1030(a)(2)(C) is much too broad and inconsistently enforced to provide any kind of deterrence. The CFAA's deterrent effect is analogous to deterrence due to laws proscribing media downloading. With dozens of downloading host websites and torrent software, incredibly difficult to find moderators and creators of websites,[83] and plenty of willing users, the government has found it nearly impossible to deter and control the millions of people who, often on a daily basis, illegally download or upload media.[84] Traffic laws illustrate a similar principle. Not even the most law-abiding citizen could claim she obeys every traffic law, all of the time. Traffic laws are analogous to the CFAA because it is difficult to drive 10 miles without violating a traffic law, while it is also difficult to click a mouse ten times in a row without violating the CFAA. In either scenario, the government cannot hope to deter violations without consistent enforcement, and in the CFAA's case, narrower provisions.

[81] *Id.*

[82] Rather than use internet security companies to protect their data, some websites offer "bug bounties" for any hacker who can successfully circumvent their security system, and then bring it to their attention to be patched. Parisa Tabriz, a white-hat hacker in charge of Google Chrome's security, helped introduce the bug bounty system to Google which allows hackers from the larger community to help recognize flaws and to patch them. *See* Josie Ensor, *This 'Security Princess' is Google's Secret Weapon*, Business Insider (Oct. 4, 2014), http://www.businessinsider.com/this-security-princess-is-googles-secret-weapon-2014-10.

[83] Peter Sunde, the co-founder of popular media file-sharing website, ThePirateBay, was not apprehended until in 2014, eleven years after the website was first launched in 2003. ThePirateBay was also shut down briefly in the same year, but was re-opened shortly after. *See* Nolan Feeny, *Pirate Bay Co-Founder Arrested in Sweden*, Time (Jun. 1, 2014), http://time.com/2804948/pirate-bay-peter-sunde-arrested/.

[84] An online-piracy survey from 2011 indicated that 95% of music downloaded online is illegal, that more than 75% of computers contained at least one downloaded illegal application, and that websites hosting pirated content receive more than 136 million visitors per day. Despite these overwhelming statistics, it is rare for illegal downloaders to be charged or convicted. This is mostly because the highly sought after hosts and moderators are very difficult to locate, often taking years of hard work and resources to find. *See Online Piracy in the Numbers*, Go-Gulf (Nov. 1, 2011), http://www.go-gulf.com/blog/online-piracy/.

IV. CURRENT CFAA REFORM PROPOSALS

Every year, cyber-attacks become more common, more visible, and more damaging, and coupled with an inability to locate and apprehend those involved, it has sparked an urgent outcry for a cybersecurity reform in the United States. While government reform activists find the answer in even further broadening the scope of the CFAA and increasing its penalties, almost all non-government proponents of a reform agree that narrowing the statute and focusing on its actual interests would be much more effective in regulating cyber-crime.[85] A reform could come from either Congress passing another amendment, or from the Supreme Court invalidating the statute all together or choosing a clear interpretation.[86] Unfortunately, it does not seem like Congress has taken any initiative to attempt to narrow or refine the statute, and have instead swung the opposite way for fear of appearing "soft on crime," as well as to project the assertion that they are capable of preventing attacks.

A. Aaron's Law

Although distant calls for a CFAA reform have been around for a while, Aaron Swartz's tragic death in 2011 was the catalyst that sparked a heated discussion and a movement toward making a change. Only four days after Aaron's death, Representative Zoe Lofgren (D-Calif.) announced that she was proposing changes to the CFAA, which in 2013 would come to be appropriately titled, "Aaron's Law."[87] The final draft of the proposal explicitly calls for excluding crimes from the CFAA that amount to a breach of contract, such as violating a website's TOS conditions, as well as to exclude efforts to prevent identification of a computer user, such as changing an IP or MAC address.[88] Specifically Aaron's Law would replace the phrase "exceeds authorized access" with "access without authorization," defined as knowingly obtaining or altering information from a protected computer that the accesser lacks authorization to obtain or alter, by circumventing one or more technological measures designed to exclude unauthorized individuals

[85] *See infra*, pp. 16-20.

[86] *See* Kerr, *supra* note 15, at 1562-63.

[87] Constant, *supra* note 14, at 244.

[88] *Id.*; *see also* Mark Jaycox, et al., *Aaron's Law Introduced: Now is the Time to Reform the CFAA*, Electronic Frontier Foundation (Jun. 20, 2013), https://www.eff.org/deeplinks/2013/06/aarons-law-introduced-now-time-reform-cfaa.

from obtaining that information.[89] This essentially codifies the Ninth Circuit's holding in *United States v. Nosal.*[90]

Tor Ekeland, one of weev's attorneys, has stated, "[a]mending the definition of unauthorized access to exclude [TOS] violations is just putting a band aid on a gaping, gushing wound."[91] While the criminalization of TOS violations is one of the largest problems of the CFAA, it certainly is not the only problem. This scheme does not distinguish between circumventing serious security protections and working around minor annoyances, and thus leaves the government still free to pursue relatively benign "misuse" such as deleting cookies. Additionally, Aaron's Law provides a definition of "access without authorization" that runs into the same problems as the current definition of "exceeds authorized access." Both definitions basically state that a person is not allowed to do what they are not authorized to do, but it is still unclear of what a person *is* authorized to do, subjecting it to the same vagueness issues as the current CFAA.[92] Also notable is that Aaron's Law gives no consideration to the overinclusive, broad, and illusive privacy protections found in § 1030(a)(2)(C).

B. Orin Kerr's Code-Based System

At the forefront of CFAA reform proposals lies Orin Kerr's code-based restriction test.[93] Fundamentally, Kerr proposes that courts interpret "access" broadly, but limit the phrase "without authorization" to the circumvention of code-based restrictions.[94] He suggests that "access" be defined as whenever a user sends a command or information and the computer executes it; essentially, any successful interaction with a

[89] Mark Jaycox, et al., *Aaron's Law Introduced: Now is the Time to Reform the CFAA*, Electronic Frontier Foundation (Jun. 20, 2013), https://www.eff.org/deeplinks/2013/06/aarons-law-introduced-now-time-reform-cfaa.

[90] *See* 676 F.3d 854, 859 (9th Cir. 2012) (en banc); *see* 18 U.S.C. §1030(a)(2)(C).

[91] Andy Greenberg, *'Aaron's Law' Suggests Reforms to Computer Fraud Act (But Not Enough to Have Protected Aaron Swartz),* Forbes (Jan. 16, 2013), http://www.forbes.com/sites/andygreenberg/2013/01/16/aarons-law-suggests-reforms-to-hacking-acts-but-not-enough-to-have-protected-aaron-swartz/.

[92] Orin Kerr, *Drafting Problems with the Second Version of "Aaron's Law" from Rep. Lofgren*, The Volokh Conspiracy (Feb. 2, 2013), http://volokh.com/2013/02/02/drafting-problems-with-the-second-version-of-aarons-law-from-rep-lofgren/.

[93] *See* Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. Rev. 1596 (2003); *see also,* Kerr, *Investigating and Prosecuting 21st Century Cyber Threats*, United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigators (Mar. 13, 2013).

[94] *Id.* at 1598-99.

computer.[95] Kerr balances the broad definition of "access" with a much narrower definition of "without authorization."[96] There are generally two ways that a user can exceed privileges on a computer: by breaching a regulation by contract or by circumventing regulation by code, essentially "tricking" the computer into giving the user more privileges than entitled.[97] Kerr proposes to limit "access without authorization" to only those that circumvent code, and to ensure that breaches of regulation by contract be insufficient to hold a user criminally liable.[98]

Kerr's proposal does the best job of curing many of the broadness and vagueness issues that make the current CFAA problematic. Limiting "unauthorized access" to only those who circumvent code limits the government's ability to arbitrarily prosecute people who it does not like, or people whose acts just happen to involve a computer. The code-based system also draws a balanced line between openness and privacy and security that allows users to visit websites without the fear and the chilling effect of potential prosecution arising from a breach of an arbitrary TOS contract. Additionally, it encourages users to protect their privacy and security in a more technically effective way, rather than by contractual agreements which essentially operate on the honor system, by prodding them to lock away data and protect their networks via code-based barriers such as a password gate.

The inherent problem, however, with this method of protecting privacy is that, much like in the physical world, it is reserved only for people who have the skill and resources to implement these barriers.[99] In fact, this is analogous to limiting the protections of physical trespass to only those who have a fence or a wall around their property. It puts the burden on the user to implement a code-based barrier that encompasses all of her privacy and security concerns, which may require extra costs and requisite skill that may be unavailable. To require the entire wide range of internet users to become technologically literate enough to implement code-based barriers in order to protect their private data or information is contrary to the democratic ideology of the United States.

[95] A broad definition of "access" is necessary in the current environment where the internet and technology change so rapidly and where a typical user may inadvertently communicate with five different servers just by checking her email, which might force courts to draw lines to determine exactly how much "access" is sufficient to implicate the CFAA. *Id.* at 1619-21.

[96] *Id.* at 1622-24.

[97] Circumvention may occur by using another user's, with greater privileges, username and password, or by exploiting an error in the software. *Id.* at 1599-60.

[98] *Id.* at 1596.

[99] *See* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement,* 103 J. Crim. L. & Criminology 907, 943-44 (2013).

Additionally, merely favoring code-based circumvention as the baseline for defining "without authorization" does not solve the delegation problem.[100] Rather than by setting the terms of the contract, it still allows private individuals to define what conduct makes a user a federal criminal by implementing code-based barriers.[101] The only difference is that users will constantly be on notice of when their activity is without authorization because they will be physically blocked by a code barrier.[102] The code-based test also begs the question: what does it mean to circumvent? In the previous *New York Times* example, would a user "circumvent" the paywall barrier by deleting their cookies after their 10-articles a month limit has been reached? JSTOR permitted MIT students to download a certain number of articles before the service would block that user's IP address.[103] Did Aaron Swartz circumvent JSTOR's code-based barrier by changing his IP address? Outrage over the way Aaron's prosecution was handled shows that very few felt that his actions amounted to a federal crime.

C. 2013 House Judiciary Draft

In 2013, the House Judiciary Committee proposed a bill that would amend the CFAA in significant ways.[104] Under the draft bill, virtually any offense under § 1030(a)(2) would be considered a felony, including the ever-broad "protected computer" language.[105] At present, violations of this section constitute a felony only when (1) the offense was committed for purposes of financial gain, (2) the offense was committed in furtherance of any criminal or tortious act, or (3) the value of information obtained exceeds $5,000.[106] In addition, the new bill would treat violations of this section as a felony if the offense involves information obtained from a computer used by or for a government entity, and also increases most of the maximum statutory penalties, including increasing the statutory maximum for the section that Aaron Swartz's conduct would have fallen under.[107]

[100] *See Private Nondelegation, supra* note 43.

[101] *Id.*

[102] *Id.*

[103] *See* Jennifer Granick, *Thoughts on Orin Kerr's CFAA Reform Proposals: A Great Second Step*, Center for Internet and Society (Jan. 13, 2013), http://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step.

[104] Peter J. Toren & Weisbrod Matteis, *Amending the Computer Fraud and Abuse Act,* Bloomberg BNA (Apr. 9, 2013), http://www.bna.com/amending-the-computer-fraud-and-abuse-act/.

[105] *Id.*

[106] *Id.*

[107] *Id.*

The proposal to turn virtually all violations of § 1030(a)(2) into felonies is a significant change. Since prosecutors are somewhat reluctant to charge misdemeanors for a variety of reasons, this change is likely to lead to an increase in prosecuting run-of-the-mill violations of the CFAA. Also, because the draft bill makes no effort to address the problematic vague and broad language, the increase in prosecutions would almost certainly be aimed at the CFAA's current favorite target, unpopular people on the internet. Although deterrence is often cited as a justification for such harsh consequences, when the unclear and vast range of prohibited conduct is to blame for the lack of the deterrence, the solution would seemingly lie in clarity and narrower tailoring rather than in simply increasing already draconian penalties. It is not difficult to imagine the level of abuse the 2013 House Judiciary Draft would initiate.

V. A Comprehensive Solution

While it might be hard to imagine why Congress would feel that the CFAA's broad reach needs to be extended further, the 2013 House Judiciary Draft is hardly the first, and nor will it be the last proposed piece of legislation to call for these changes. The growing threat and current phenomenon of damaging and visible cyberattacks, coupled with the startling lack of results in apprehending major hackers is primarily what has prompted government action. The rush of action taken to combat hacking threats to the United States is comparable to the response after the September 11th World Trade Center attacks. Because the September 11th hijackings were so visible, damaging, and emotionally jarring, the public looked to the United States government for an immediate response or solution. Rather than appear to do nothing, the Transportation Security Administration ("TSA") almost immediately increased its airport security regulations.[108] TSA regulations are notorious and have been heavily criticized for being invasive, costly, incompetent, and ineffective in locating terrorists or hijackers, yet they give the public the illusion of safety.[109]

Expanding the CFAA's scope would have the similar effect of appearing to the public that the government is being proactive or aggressive in its effort to stop cyberattacks, but an expansion would do very little in practice to stop real hacking threats. If anything, expanding the scope of the CFAA would divert valuable resources into prosecuting arbitrary TOS violations, which could instead be used for locating and

[108] *See* Charles C. Mann, *Smoke Screening,* Vanity Fair (Dec. 20, 2011), http://www.vanityfair.com/culture/2011/12/tsa-insanity-201112.

[109] *Id.*

apprehending notoriously difficult to find, damaging, “black hat” hackers. While there is strong pressure to take some kind of action in response to recent cybersecurity failures, the government must move away from simply editing or building on the vague and unclear language of the current CFAA and reconstruct it specifically to respect and balance the CFAA’s interests, to target actual wrongdoers and real harms, and to endorse specific frameworks.[110]

A. Balancing Interests: The Case for Privacy

First and foremost, any effective CFAA reform needs to include a stronger, and an express privacy provision. Despite the fact that § 1030(a)(2)(C) was included in the CFAA specifically to protect privacy, the interest is nearly always placed on the backburner or simply not recognized at all.[111] For example, the government reacted very strongly when members of online “hacktivist” group, Anonymous, launched a series of DDoS attacks that disrupted and destroyed the Church of Scientology’s ability to communicate online.[112] Additionally, intrusions into government or military computers are treated with the utmost urgency and severity yet invasions of non-government related privacy are seen as a second tier priority, and sometimes even considered a mitigator when “only” contact or personally identifiable information is compromised.[113]

Furthermore, even when privacy is given some kind of recognition in regards to the CFAA, it is most often in reference to financial, rather than individual, privacy. In 2014, JPMorgan Chase was the victim of a massive hack that compromised the private information of 76 million account holders.[114] The attack was targeted at financial data, but instead, hackers were “only” able to obtain names, addresses, phone numbers,

[110] *See* Steven Titch, *Four Principles for Effective Cybersecurity Law and Policy,* RStreet (Apr. 25, 2014), http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy/.

[111] *See, e.g.,* S. REP. NO. 104-357, at 7 (1996)(“The bill would amend section 1030(a)(2) to increase protection for privacy and confidentiality of computer information.”); S. REP. NO. 99-432, at 6 (1986)(“the premise of this subsection is privacy protection . . . “); Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 U. Pitt. J. Tech. L. & Pol’y 1 (2012).

[112] The group launched a series of damaging online attacks against the Church of Scientology, titled “Project Chanology,” an attempt to expel the Church of Scientology from the internet. Patrick Barkham, *Hackers Declare War on Scientologists Amid Claims of Heavy-Handed Cruise Control,* The Guardian (Feb. 4, 2008), http://www.theguardian.com/technology/2008/feb/04/news.

[113] *See infra* pp. 21-22.

[114] David E. Sanger et al., *White House Monitored JPMorgan Breach with Alarm,* N.Y. Times (Oct. 8, 2014).

and email addresses of consumers.[115] Rather than seriously address the fact that significant, private information was stolen from millions of people, both the government and JPMorgan were much more concerned that the company's internet security system was breached in general, and were purely relieved that no financial data was compromised.[116] In fact, under both federal and state law, JPMorgan did not even have to alert customers about the attack because "only contact information was breached."[117] The cavalier attitude toward violations of individual privacy, backed-up by the lack of recognition from CFAA itself, sets a dangerous precedent of belittling and devaluing privacy, which is especially concerning in the era of the internet. The lack of an express privacy provision in § 1030(a)(2)(C) directly endorses this attitude by giving the impression that privacy can be efficiently protected by simply being thrown in with the rest of the immeasurable myriad activities covered by the catchall provision.

There is a common belief that once something has been uploaded, posted, or written on the internet, it is there "forever." Put more precisely, it is common for people to argue that there is no expectation of privacy online; however, this is not entirely true. Consumers enter their credit card information into websites all the time and absolutely expect it to remain private. It seems that this common belief is only applicable when personal information is at issue. In 2014, a significant amount of private, intimate pictures were stolen from over 100 celebrity women and were posted and widely distributed on the internet.[118] These pictures were all stolen via their iCloud accounts, which contained data that had been automatically transferred from their phones.[119] As expected, the iCloud breach added more fuel to the cybersecurity discussion, although in this instance, parties jumped to place blame squarely on the victims and to say that the debate should be more focused on the actual conduct of hacking rather than the extremely personal and invasive information that was stolen.[120]

Additionally, individual privacy needs to be better protected in the CFAA because it is much easier to violate online, and there are countless

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *See* Dave Lewis, *iCloud Data Breach: Hacking and Celebrity Photos*, Forbes (Sept. 9, 2014). http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/.

[119] *Id.*

[120] *See* Mary Anne Franks, *The Internet's Privacy Hypocrisy*, Daily Dot (Sept. 3, 2014). http://www.dailydot.com/opinion/celebgate-privacy-hypocrisy-nude-photos-nsa-edward-snowden/.

online privacy threats that do not have a physical world equivalent. In the physical world, constantly monitoring, following, and watching someone's every move presumably requires a great deal of effort and time. Online, a typical user can accumulate countless amounts of spyware, malware, viruses, cookies, and other tracking software in a single day that can monitor and may allow recording of their every keystroke or Google search. While in the real world, this activity would probably be more aptly called stalking, in the online world, this is simply routine. Technology makes it immeasurably easier to track someone online or to discover private information about them. Simply the fact that violations that involve financial data or the disruption of information are met with panic and outrage, while these types of privacy violations are seen as normal or expected is evidence enough that individual privacy must be better addressed and balanced in the CFAA.

Not only is individual online privacy largely ignored by the CFAA, but it is currently being threatened and further minimalized by new proposed cybersecurity, information-sharing, legislation such as the Cybersecurity Information Sharing Act (CISA),[121] and even by popular CFAA reform proposals that seek to narrow its scope. For example, Kerr's proposal allows users to protect their privacy only when they have constructed code-based barriers around it.[122] This is essentially a form of conditional privacy, only reserved for those who are technologically savvy enough to implement these barriers. Those who are not are left with the choice between using the internet and adequately protecting their privacy, which, in the era of the internet, is not a choice at all. Privacy is a recognized fundamental right, and a right recognized as a protected interest by the CFAA.[123] In order for this right to be taken seriously and respected, it needs to be addressed in a strong, express privacy provision.

[121] CISA seeks to solve the cybersecurity crisis by encouraging information sharing between businesses and the government by protecting businesses from lawsuits if they share "cyber threat indicators" with the government. Cyber threat indicators can come from as little as a user connecting to Starbucks' Wi-Fi while that user has spyware on his computer. The bill also does not require personal information to be removed before data is shared with the government unless there is verifiable knowledge that the information is present. Much like proposals to expand the CFAA, this legislation comes as a hasty response to the imminent threat of cyber-crime that emulates the common theme of sacrificing privacy for security, and sometimes for just the illusion of security.

[122] *See* Thaw, *supra* note 99, at 943-44.

[123] Griswold v. Connecticut, 381 U.S. 479 (1965); *see also supra* note 112.

B. Targeting Wrongdoers

Although much about the internet, cybersecurity, and the CFAA is murky, it is abundantly clear that real and extremely destructive cyber-threats do actually exist, and very little has been effective in preventing these attacks. These actual, dangerous threats can broadly be divided into three categories.[124] The first category, as illustrated by the Target breach in 2013, the Home Depot breach a year later, and countless others who have fallen victim to this particular motivation, encompasses theft or fraud that is financially- or profit- motivated.[125] This kind of breach mostly involves commercial businesses or banks, and affects both the targeted company and the individuals whose information is stolen. Many times, breaches of this category are very large and visible, sometimes affecting millions of consumers. Like most forms of serious hacking, the government has found it incredibly difficult to apprehend hackers who steal financial information.[126]

The second category includes hackers who seek to acquire private or protected information through espionage.[127] This can include attaching viruses, spyware, or malware to specific, or a series of, computers, and can also include simply stealing or guessing passwords to access private data. This particular threat affects all internet users across the board, from government computer users, to individual users, to businesses, and to the military. In addition to the aforementioned iCloud breach and the Community Health Systems breach, an international hacker group managed to break into Sony Pictures' network, also in 2014, and steal a number of unreleased films as well a multitude of company emails, which were published and circulated online.[128] The incident caused the suspended release of the movie, "The Interview," and the resignation of co-chair Amy Pascal due to several of her personal emails being made public.[129] Even the White House has not been immune to hackers searching for private information.[130]

[124] Titch, *supra* note 110.

[125] *See* Harris & Perlroth, *supra* note 10; *see* Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, Wall Street Journal (Sept. 18, 2014). http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[126] *See supra* note 33.

[127] Titch, *supra* note 110.

[128] *See* Lewis, *supra* note 12; *see* Sullivan, *supra* note 11; *see* Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know so Far*, Wired (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know/.

[129] Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know so Far*, Wired (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know/.

[130] In October of 2014, representatives admitted that the White House network had been breached, believing the attack was "state-sponsored." *White House Computer Network 'Hacked,'* BBC News (Oct. 29, 2014), http://www.bbc.com/news/technology-29817644.

Finally, the third legitimate threat to cybersecurity includes disruption or destruction designed to cause harm through an attack that slows, disables, or destroys essential systems.[131] This type of cyberattack is commonly orchestrated through DDoS attacks.[132] DDoS attacks are a preferred weapon of hacktivist groups, because they are very effective and are extremely easy to launch.[133] The purpose of these attacks is to overload the server and to render the target victim unable to communicate online.[134] It is estimated that in 2014, there were 28 DDoS attacks every hour.[135] Popular targets of DDoS attacks include websites hosted on high-profile servers such as banks or credit card payment gateways, as well as business competitors, although they can technically happen to anyone.[136] In a very publicized cyberattack from 2011, two members of the infamous hacking group, LulzSec, launched a DDoS attack that took down the Serious Organised Crime Agency (SOCA) website in the United Kingdom, and the Central Intelligence Agency (CIA) website in the United States.[137]

Much of what is proscribed and prosecuted today by the CFAA does not fall into one of these categories. The sliding scale allotted by the "unauthorized access" language allows benign or trivial conduct, which amounts to no real harm, to be criminalized, and turns non-hacker computer users into federal criminals.[138] Aaron Swartz may have used a minor workaround to get access to JSTOR articles, but the harm stemming from his conduct is still unclear, even to JSTOR, the alleged victim of Aaron's "attack."[139] Similarly, Lori Drew's motivation, although perhaps petty and malicious, was not a motive that has sparked fear in the hearts of those concerned with computer crime. Today, the

[131] *See* Titch, *supra* note 110.

[132] Generally, this method involves taking over "bot" or "zombie" computers to overload the target computer with external communication requests. Deepanker Verma, *LOIC (Low Orbit Ion Cannon)—DOS Attacking Tool,* InfoSec Institute (Dec. 20, 2011), http://resources.infosecinstitute.com/loic-dos-attacking-tool/.

[133] DDoS attacks are commonly launched via the Low Orbit Ion Cannon (LOIC) application, which was originally adapted as a stress testing device for website traffic. Launching an attack or a stress test is as easy as downloading the application and inputting the link to the target website. *Id.*

[134] *Id.*

[135] NSFOCUS Information Technology Co., Ltd., *DDos Threat Report 2013.*

[136] Verma, *supra* note 132.

[137] The group has also taken responsibility for attacks against News International, Sony, Nintendo, the Arizona State Police, 20th Century Fox, HBGary Federal, Infragard, Bethesda, Eve Online, and many others. Fahmida Y. Rashid, *LulzSec Duo Plead Guilty to DDoS Against CIA*, SC Magazine (Jun. 25, 2012), http://www.scmagazine.com/lulzsec-duo-plead-guilty-to-ddos-against-cia/article/247284/.

[138] *See* Constant, *supra* note 14.

[139] *Id.*

government looks to punish only the conduct of hacking rather than focus on the resulting harm or motivation. Each of the aforementioned categories has different motivations or objectives, and requires a solution that adequately addresses that particular motivation or result, rather than a one-size-fits-all approach.

C. Endorsing a Specific Framework

The "unauthorized access" language that defines the CFAA creates a sliding scale of federal illegality that puts all of the focus on the conduct of hacking, gives too much discretion to prosecutors and police officers, delegates power to individuals, and is too broad and vague to allow a normal person to diligently follow the law. In order for a CFAA reform to be effective, a more specific framework that describes exactly what is prohibited is needed. The proscription must focus on actual, destructive harms that pose a real threat to the security and privacy of internet users, as well as their ability to freely communicate and to have access to information online.

The first step in achieving this goal is to eliminate the nature of purely prohibiting certain online conduct, and to focus more on the harms that stem from that conduct, as well as the motivation for engaging in such conduct. To do this, the entire framework of the statute must be reworked, and specifically, language from § 1030(a)(2)(C), criminalizing whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,"[140] must be removed entirely, in favor of criminalizing, specifically, the three aforementioned broad categories of cyber-threats: (1) theft or fraud where the intent is financial gain or profit; (2) espionage where the intent is the theft of private information, or the result is exposure; and (3) disruption where the intent is to cause harm through an attack orchestrated to slow, disable, or destroy systems or networks.[141] Whoever knowingly engages in actions that fall into either the first or the third category, as well as anyone who knowingly acquires private information, would be culpable under the CFAA, while whoever knowingly *or recklessly* causes the type of private information exposure described in the second category would be culpable as well.

The first category of harms is fairly self-explanatory. A person violates this provision when they knowingly engage in theft or fraud where the motivation is financial gain. This section, however, should be limited to actual monetary loss, rather than the idea of attributing a

[140] 18 U.S.C. § 1030(a)(2)(C).

[141] Titch, *supra* note 110.

financial value to the loss of certain information. For example, hackers who are responsible for the Target breach would violate this section because they sought to steal credit card information, but a user who circumvents *New York Times* website to exceed their 10-articles-per-month limit would not, regardless of whether *New York Times* estimated the amount of money lost due to the circumvention. While perhaps the aggregate effect of all of the users who circumvent *New York Times* for this purpose is financially damaging and should be punished, speculative financial losses due to improperly acquiring information should not be addressed by the CFAA, and will not be addressed in this Note.

The "exposing information" provision is somewhat of an outlier because the damage done by exposing private information is often irreversible, while damage from theft or fraud or from disabling or slowing essential systems can be remedied. As previously stated and as history has indicated, once something has been posted on the internet, it is virtually impossible to remove it completely, especially if it is private. One need only look to the iCloud breach to recognize this unfortunate truth.[142] It is for this reason that the mens rea for exposing private information includes recklessness, while the theft of private information without exposure requires knowledge. Additionally, because it is so difficult to draw a bright line that differentiates private versus public information, this entire category requires a subjective test. Although there are very clear examples of exposure or theft of private information, such as the iCloud breach, less clear situations also commonly arise, such as weev's case in which he merely facilitated the exposure of private information that had negligently been made public by AT&T.[143] These more difficult cases demonstrate the need for a subjective test that takes into consideration a number of factors including, but not limited to, the nature of information that is exposed and its significance or repercussion to the victim, the reputational or personal damage to the victim, and the methods used to obtain the information. Private information, however, should not include published information or articles that are public to users with a subscription or who fall within a viewing limit, such as JSTOR or *New York Times* articles, because the harm due to exposure or acquisition in these scenarios is *de minimis*.

Similar to the first category, knowingly engaging in disruption that is meant to cause harm by slowing, disabling, or destroying essential systems is generally straightforward. However, for harms that fall into this category, consent would be a complete defense. Conduct intended to slow, disable, or destroy would be presumed unauthorized, so the burden

[142] *See* Franks, *supra* note 120.

[143] *Id.*; O'Toole, *supra* note 34.

would be on the defense to demonstrate this consent. Consent can be assessed through a multitude of factors, including, but not limited to; whether there was a contract in which an alleged victim knowingly consented, such as a TOS agreement; whether there was a code-based barrier in place; whether there was verbal consent; and the relationship of the parties. For example, many high-traffic websites use stress-testing software that is often also used for launching DDoS attacks.[144] While launching a DDoS attack against a website would violate the statute, when done with legitimate consent for purposes of stress-testing, it falls into the consent exception.

This framework allows for adequate balancing and protection of the interests of the CFAA. First, privacy is given express recognition and protection from both, a financial and an individual standpoint. Rather than a catchall provision, the express protection from both theft and from private information exposure would directly address the aforementioned privacy concerns and attitudes that have fallen through the cracks of the CFAA. The CFAA's interest in security is also not diminished by this framework. Because these categories are broad, more specific violations that are already prohibited by the current CFAA can be reworked or added into one, or several, of these categories, including current security protections for password trafficking, extortion, or violations that involve a government or military computer (specifically, data theft from these government networks).[145] This categorical framework would ground the security interest in all three provisions. Finally, the interest in preserving and facilitating a free flow of information is also expressly protected by the third category, as well as implicitly protected by the framework itself by excluding minor computer misuse. The wide threat of prosecution that stems from criminalizing TOS violations and minor workarounds has the effect of diminishing the availability of much of the information online, and also of chilling efforts to facilitate it, illustrated precisely by Aaron Swartz's case.[146]

Targeting specific harms and actual wrongdoers has the effect of eliminating from the statute minor time- and resource-consuming, computer misuse that should not be the focus of federal legislative attention, such as TOS violations, an employee's non-work-related internet searches, or a typical user's cookie or internet history clearing habits. This framework would make sure only legitimate cyber-threats are able to be charged under the statute to avoid overcriminalization. Additionally, other potentially damaging activity that is does not relate

[144] Verma, *supra* note 132.

[145] *See* 18 U.S.C. § 1030 (2012).

[146] *See* Constant, *supra* note 14.

specifically to the interests of the CFAA, such as employee damage or sabotage, can be better addressed under other existing laws. Furthermore, by eliminating the sliding scale and the catchall aspect of the CFAA, resources could be freed up and able to be used toward better understanding, tracking, and preventing cyber-threats.

In addition to better protecting the interests of the CFAA, the framework of proscribing specific categories of harm also corrects the multitude of problems that currently plague the statute, including: (1) void-for-vagueness issues; (2) delegation issues; and (3) the issue of running contrary to general goals of criminal justice. The vagueness problems with the CFAA stem from its absent definitions, and unclear interpretations, of both "unauthorized access" and "exceeding authorized access."[147] Removing this terminology and instead inserting specifically-prohibited provisions that describe exactly what is not allowed, eliminates this problem. Additionally, the same argument can be made for delegation issues. By simply not allowing violations of TOS agreements to fall under the CFAA, delegation falls squarely back on lawmakers. Finally, a strong impact of this proposal would include its adherence to criminal justice goals. Rather than a catchall provision that criminalizes a broad and unclear range of activity, most of which is of no real concern to the government, specific provisions put citizens on notice of exactly what is prohibited. Additionally, implementing this proposal would eliminate the clear lack of respect people feel toward a law that is simply too broad to have any kind of deterrent effect, that is arbitrarily and discriminatorily enforced, and that makes it nearly impossible to carry on with daily online activities without somehow violating it.

VI. CONCLUSION

Computer networks and the internet are heavily relied upon for the full range of activities that support our economy, political system, social order, and communication.[148] The United States' national stability is threatened when key networks are threatened, and grounding interests in security, privacy, and a free flow of information into a statute with an egregiously wide scope that glorifies excessive penalties is not the appropriate solution. A comprehensive solution that specifies exactly what is prohibited is necessary to assure that actual harmful activity, rather than routine computer use, is criminalized, and that our rights and interests as citizens are adequately protected. CFAA reform is necessary

[147] Kerr, *supra* note 15.

[148] George B. Delta & Jeffrey H. Matsuura, *Controlling Network Access,* 2013 WL 3924193 (C.C.H.), CCH Law Of Internet §10.02 at 21.

for better understanding, preventing, apprehending, and prosecuting hackers who pose a serious threat to the United States.