"THE CYBER"

HARD QUESTIONS IN THE WORLD OF COMPUTER SECURITY RESEARCH

CENTER FOR
DEMOCRACY
& TECHNOLOGY

March 2017

CENTER FOR DEMOCRACY & TECHNOLOGY

"The Cyber:" Hard Questions in the World of Computer Security Research

I. Executive Summary

The U.S. presidential election of 2016 will go down in history as the first to feature cyber issues, and, more particularly, cybersecurity as a defining theme.

From the initial controversy over Secretary Clinton's use of a private email server, to the extraordinary public conclusion of the intelligence community that the Putin regime in Russia tried deliberately to help elect President Trump (though without concluding that the interference had an effect on the actual outcome), "the Cyber," as President Trump called it, has become an issue in the political discourse on par with national security, crime, immigration, or the economy.

One aspect of "the Cyber" that has not received the attention it is due, however, is the role that computer security researchers play in the cybersecurity ecosystem. In an effort to raise the profile of these issues, the Center for Democracy & Technology, through a generous grant from the Hewlett Foundation, is in the midst of a two-year research project to identify both key policy issues in the world of security research and solutions to problems like the chill security researchers often face from laws such as the unduly vague Computer Fraud and Abuse Act ("CFAA"), which creates civil and criminal liability for an array of computer crimes, or the Digital Millennium Copyright Act ("DMCA"), which prohibits researchers from circumventing technological access restrictions.

CDT's security research work is divided into two primary tasks. The first is the production of white papers and other policy analyses to help frame the discussion and identify the topline issues that need to be addressed. The second is a qualitative project to interview security researchers to learn directly from those in the field about what kinds of challenges they face as part of their work.

This white paper is intended as the first step in our issue-spotting exercise. We have divided it into the four central policy discussions in the world of security research (as we see them):

- The legal challenges researchers face under the CFAA, DMCA, and other relevant legal regimes such as export controls;

- The role of federal, state, and local prosecutors, and the need for clear guidance on when computer security research may lead to scrutiny from investigators or to prosecution;

- The importance of vulnerability disclosure regimes and the efficacy and wisdom of "bug bounty" programs that encourage independent researchers to seek out and disclose vulnerabilities; and

- Whether the security research community can identify clear ethical "redlines" (such as experimenting on a live system when it could impact non-consenting bystanders), or, conversely, whether agreeing on such redlines could lead to them being adopted as legal rules, which could lead to unintended consequences.

We have written this white paper as a comprehensive primer on these issues as we see them through our initial research and preliminary interviews with security researchers in the field.[1] We hope the reader will be able to reference individual sections without reading the whole paper (though we certainly encourage those interested in this world to do so). And we hope that by cataloguing these issues—alongside possible policy responses, such as various proposals for CFAA reform, or the creation of a federal bug bounty program—we can help begin to formulate concrete initiatives that CDT and other civil liberties and technology advocates can advance.

We envision that this white paper will be followed by several other deliverables. These will include a white paper that dives into the social benefits that flow from security research, such as hacker-resistant cars and implantable medical devices, more secure critical infrastructure, and, especially in light of the 2016 elections, tamper-proof voting machines.

CDT has already hosted one and will host other convenings of stakeholders in the security research community, government, civil society, and industry to discuss these and other issues. That first convening was extremely helpful in informing the content of this white paper and we are grateful to all who participated.

We hope to conclude this research project with a final white paper that includes concrete policy and legislative proposals to reduce the chill on security research while also identifying potential ethical best practices for security research itself.

---

[1] CDT will release findings from this interview study later this year.

Unfortunately, none of these issues are going away. Growth in connected devices, the precedent set by Russian hacking in the 2016 election, mammoth denial of service attacks through the Mirai botnet, constant data theft and a significant increase in computer crime—these and other elements of "cybersecurity" broadly understood are only becoming more dangerous and more firmly fixed in the public mind.

Sober and deliberative law and policy, which protects civil liberties while improving cybersecurity, is the only defense and the only path to progress. We very much hope that this paper is a productive step on that path.

II. Introduction

This is certainly the election year of "the cyber," as President Donald Trump put it in the first general presidential debate (which, not incidentally, was the first non-primary debate in American history to even feature the word "cyber").[2] Cybersecurity stories continue to dominate the political headlines, and following the historic 2016 election, cybersecurity will undoubtedly be one of the defining issues of the Trump administration.

One issue that has not received the attention it is due, however, is the central role that security research, and security researchers, have played in all of the major cybersecurity stories of this historic election cycle.

To give just one profound example, especially in light of the 2016 race, security researchers continue to demonstrate serious flaws in electronic voting machines, and yet a dozen states still use machines without a paper trail, which can provide a software-independent mitigation against hacking.[3]

This is of particular concern given the January 2017 report by the Office of the Director of National Intelligence ("ODNI") reporting that Russian hackers had attempted to and in some

---

[2] Lester Holt said it in the question that prompted President-Elect Trump's response. Presidential Debate at Hofstra University in Hempstead, New York (Sept. 26, 2016), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=118971.

[3] Zeynep Tufekci, *The Election Won't Be Rigged. But It Could Be Hacked*, N.Y. Times, Aug. 12, 2016, *available at* http://www.nytimes.com/2016/08/14/opinion/campaign-stops/the-election-wont-be-rigged-but-it-could-be-hacked.html.

cases succeeded in accessing state and local electoral boards.[4] (Indeed, we recently learned that this activity, not the email "doxxing" of the DNC and others, is what prompted the Obama administration to publicly denounce the Russian interference.[5]) It is also quite relevant in light of the growing concern among many election security experts that—given the political polarization of the country, and the razor-thin margins that gave the Republicans the electoral college in 2016 (less than a tenth of one percent of the vote)—vulnerabilities in election infrastructure itself could lead to a hack that actually changes the result.[6]

In an environment where one in three Americans—and almost a majority of Republicans—lacks confidence that votes will be counted accurately, anything that prompts a debate about election security, and especially one that leads to improvements, goes directly to the beating heart of American democracy.[7]

And yet, through an initial series of semi-structured qualitative interviews CDT has conducted with security researchers, it has become clear that there is a real chill, in both law and policy, on security research. This white paper addresses some of the hard questions around this chill, and served as a framing document for CDT's first in-person convening on the issue. Input from that convening has helped refine and inform this final white paper.

The chill comes in many forms.

---

[4] Office of the Dir. of Nat'l Intelligence, Assessing Russian Activities and Intentions in Recent US Elections (2017), *available at* https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf.

[5] Matthew Rosenberg et al., *Obama Administration Rushed to Preserve Intelligence of Russian Election Hacking*, N.Y. Times, Mar. 1, 2017, *available at* https://mobile.nytimes.com/2017/03/01/us/politics/obama-trump-russia-election-hacking.html.

[6] *See, e.g.*, Richard Clarke, *Yes, It's Possible to Hack an Election*, ABC News, Aug. 19, 2016, *available at* http://abcnews.go.com/Politics/hack-election/story?id=41489017.

[7] Justin McCarthy & Jon Clifton, *Update: Americans' Confidence in Voting, Election*, Gallup, Nov. 1, 2016, available at http://www.gallup.com/poll/196976/update-americans-confidence-voting-election.aspx; Jake Sherman & Steven Shepard, *Poll: 41 Percent of Voters Say Election Could be Stolen from Trump*, Politico, Oct. 17, 2016, *available at* http://www.politico.com/story/2016/10/poll-41-percent-of-voters-say-the-election-could-be-stolen-from-trump-229871.

Legally, laws like the Computer Fraud and Abuse Act ("CFAA"),[8] which has expanded in scope and the severity of its possible punishments since passage in the mid-1980s, fail to clearly state what is or is not prohibited conduct, and companies often use the civil provision of that law to intimidate researchers into stopping their work.[9] Policy-wise, though many companies and even government agencies are moving to "bug bounties" that encourage the coordinated disclosure of security flaws, these programs are not ubiquitous, nor are they universally successful.[10]

Additionally, regulatory regimes as disparate as copyright and export control also implicate, on the one hand, the "freedom to tinker" and, on the other, whether hackers in the United States should be able to sell surveillance technology or intrusion software and tools that could be and are often used to target dissidents and political opponents.

Finally, the very practice of security research can involve interacting with systems and data that do not belong to the researcher, and that contain or constitute sensitive or private information.[11] That implicates fraught debates about whether some security research—on live

---

[8] The CFAA originally passed as part of the Comprehensive Crime Control Act, Pub. L. No. 98-473, 98 Stat. 2190 (1984), and was codified at 18 U.S.C. § 1030 (2012). It has been amended significantly over the years. Its current structure was created in 1986 in Pub. L. No. 99-474, 100 Stat. 1213. For the amendments (in chronological order), see Pub. L. No. 100-690, § 7065, 102 Stat. 4181, 4404 (1988); Pub. L. No. 101-73, § 962, 103 Stat. 183, 502 (1989); Pub. L. No. 101-647, § 2597, 104 Stat. 4831, 4911 (1990); Pub. L. No. 103-322, § 280005, 108 Stat. 1796, 2097 (1994); Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3491 (1996); Pub. L. No. 107-56, §§ 202, 217, 315, 506, 814, 115 Stat. 272, 278, 291, 309, 366, 382-84 (2001); Pub. L. No. 107-296, §§ 225, 1704, 116 Stat. 2135, 2156-58, 2314 (2002); Pub. L. No. 110-326, §§ 202-09, 122 Stat. 3560-61, 3563-64 (2008).

[9] 18 U.S.C. § 1030(g) (2012). It is important to note that a greater number of CFAA *prosecutions* may be entirely warranted given the explosion in computer use since its passage 30 years ago. Our comment above reflects how the CFAA has been amended to cover numerous activities that it did not when passed in 1986, and how the possible punishments under the law have grown in severity. CFAA critics also do not quarrel with expanding the law to cover new and innovative computer crimes, but they do continue to have concerns with the overbreadth and vagueness in the law.

[10] Fahmida Y. Rashid, Extortion or Fair Trade? The Value of Bug Bounties, InfoWorld, Sept. 9, 2015, *available at* http://www.infoworld.com/article/2981695/security/extortion-or-fair-trade-value-bug-bounty-programs.html.

[11] It is important to note that the CFAA is not just a fraud or trespass law; it is, in a very real way, an important privacy protection that deters cyber-criminals from accessing sensitive private

systems, for instance—should be ethically or legally out of bounds (or whether drawing those lines invites the government and courts to adopt them as legal redlines under the CFAA).

Accordingly, the world of "the cyber" presents some of the most difficult questions in public policy today. We've chosen four of the most controversial ones to address in this white paper. We hope that by surfacing these questions, while not advocating for a particular position (yet), we can help illuminate specific answers.

These four questions are as follows:

- Are legal reforms needed? Many would argue that imprecision in the text of the CFAA is a problem, but how, specifically, should that be addressed? And how can other legal impediments to security research, like export controls on software and the anti-circumvention provisions in the Digital Millennium Copyright Act, be addressed?

- Is enforcement policy properly calibrated? The Department of Justice recently released guidance (which was drafted in 2014 but kept secret for two years) for prosecutors on making charging decisions under the CFAA.[12] Does it strike the right balance? Could the DOJ expand it to create a safe harbor? Should Congress mandate that it do so?

- What are the best practices for bug bounty programs, and how can these programs fit into the debate over full versus coordinated disclosure? For instance, should bug bounty programs encourage prompt patching by affirmatively permitting or even encouraging bounty winners to disclose vulnerabilities after a certain window, even if the company hasn't released a fix?

- Finally, and perhaps most controversially, should the security research community seek consensus on the ethical and legal status of certain practices—such as accessing systems on moving vehicles? And does that pose the risk of unintended consequences, as ethical redlines in the security community are adopted as binding rules by courts

---

information—much like the Electronic Communications Privacy Act deters the private interception of communications in transit.

[12] Memorandum from Eric Holder, Attorney Gen., Dep't of Justice, to the United States Attorneys and Assistant Attorney Gens. for the Criminal and Nat'l Sec. Divs., Intake and Charging Policy for Computer Crime Matters (Sept. 11, 2014), *available at* https://www.justice.gov/criminal-ccips/file/904941/download [hereinafter Computer Crime Charging Memorandum].

seeking to, among other things, navigate the overly vague CFAA? Further, could these ethical redlines and concerns about vagueness in the CFAA be addressed in significant part by concerted efforts to educate researchers about the CFAA and how it has been used?

We discuss these in more depth below.

III. The Law. Are Changes Needed?

a. The Computer Fraud and Abuse Act ("CFAA")

As it stands now, the CFAA, codified at 18 U.S.C. § 1030 (2012), has effectively nine separate offenses, summarized with the attendant penalties in Appendix 1.[13] Crucially, most of these offenses are triggered only when access is "without authorization," and a few are triggered when a user "exceeds authorized access."[14] "Without authorization" is undefined in the law, and this flaw is the fatal one that has created such controversy over the CFAA.[15]

---

[13] Subparagraph (a)(2) is really three separate offenses.

[14] "Without authorization" and "exceeds authorized access" are generally thought to cover, respectively, the conduct of an "outsider," versus an "insider" who has authorization to access a system but goes beyond that authorization. All CFAA offenses require that the conduct be "without authorization." The following provisions can be triggered by exceeding authorized access: Paragraphs (a)(1) (national defense information), (a)(2) (obtaining certain information), (a)(4) (computer wire fraud), and Subparagraph (a)(7)(B) (threat to obtain or disclose information). The others apply when the conduct was without authorization. For instance, the "botnet" provision, which applies to the transmission of code that damages another computer, applies when access to the computer is "without authorization." Paragraph (a)(5). It need not extend to actions that exceed authorized access, as, in that context, the language would be redundant. Note that 18 U.S.C. § 1030(a)(5)(A) is triggered by causing "damage" without authorization, and (a)(7) doesn't require access at all.

[15] It is true that much of the recent litigation has revolved around "exceeding authorized access," which is defined in the law as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2012). The issue here, however, is that the definition is keyed to *authorization* and information that the user is not entitled to obtain or alter. Clarifying that both terms require the circumvention of a technical access barrier would reduce the vagueness with respect to both.

Importantly, the CFAA also provides for a civil cause of action for any person who experiences damage or loss, if the conduct involves one of the aggravating factors for offense (a)(5),[16] which include interfering with medical treatment, causing a threat to physical health or safety, or, importantly, loss to one or more persons over $5,000 (a relatively low monetary bar).[17]

The goal of the CFAA is a good one. Hacking a computer, installing malware, and causing deliberate damage to another's computer *should* be a crime. Guessing passwords and accessing someone's Gmail—also not kosher. And, it is important to note that prosecutions against security researchers-qua-security researchers are extremely rare (the Auernheimer case, discussed below, is really the only prosecution for security research that we are aware of).

Nevertheless, as discussed below, uncertainty over the legal definition still can cast a pall over some research, particularly in that we do not have clear information on the number of *investigations* of security researchers that have been conducted pursuant to the CFAA. We also understand from our interviews with security researchers that both criminal and civil exposure under the CFAA are considerations in deciding when and how to do certain research.

The problem with the CFAA is twofold: one, is the aforementioned lack of a definition of "without authorization," and, two, prosecutors can threaten severe penalties because of redundancy in the statute and the ability to bump a misdemeanor to a felony in some cases by, for instance, alleging a violation of a state computer crime statute for the same conduct.

With respect to the first problem, this lack of clarity has led to numerous cases that are highly controversial, not because the target of the prosecution is particularly sympathetic (in many cases, they are not), but because the underlying conduct doesn't involve using a computer to break into a protected computer, or using a computer to commit fraud.

For instance, in *United States v. Drew*, the defendant set up a fake MySpace page to bully a teenage girl, who ultimately committed suicide.[18] Drew was charged with three misdemeanor counts under the CFAA—namely violations of Subparagraph 1030(a)(2)(C), the use of a

---

16 Listed at 18 U.S.C. § 1030(c)(4)(A)(i) (2012).

17 18 U.S.C. § 1030(g).

18 259 F.R.D. 449 (C.D. Cal. 2009).

computer to obtain information without authorization in furtherance of the tort of intentional infliction of emotional distress.[19] The key issue for critics of the case was that the violation of MySpace's terms of service alone led to the criminal prosecution.[20]

Critics of the case, including the judge who overturned the jury verdict and acquitted Drew, noted that terms of service are both rarely read in their entirety, or at all, and can be changed at the whim of the site owner.[21] It is important to note that *Drew* is an older case, and we are unaware of a more recent case where federal prosecutors brought criminal charges based solely on the violation of express terms of service (Auernheimer is close, however).

More recently, a similar issue has come up in two cases in the Ninth Circuit. In one, commonly referred to as *Nosal II*, prosecutors alleged that the use by two former employees of a former colleague's password, which that colleague had authorization to use and had voluntarily provided to the defendants, was "without authorization" in criminal violation of the CFAA.[22] Their former employer had revoked the former employees' access to the employer's network, so they used their colleague's access to obtain information to support their competing company. The court agreed with the prosecutors and upheld the conviction.

In a second, *Facebook v. Power Ventures*, a civil case, the circuit held that the issuance of a cease and desist letter by Facebook to an entity that allowed users to aggregate posts, messages, and other content across many different social networking platforms was enough to revoke authorization (even though the entity had not circumvented a technical access restriction).[23]

---

19 *Id.* at 452.

20 Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, Wired, July 2, 2009, *available at* https://www.wired.com/2009/07/drew_court/.

21 *Id.*

22 *United States v. Nosal* (*Nosal II*), 828 F.3d 865 (9th Cir. 2016).

23 *Facebook v. Power Ventures*, 828 F.3d 1068 (9th Cir. 2016).

Finally, a separate but related issue, which is particularly relevant to security researchers, has arisen in cases involving security research that accesses another system but does not circumvent an authentication requirement.

For instance, in *United States v. Auernheimer*, known as the "Weev" case after the defendant's online nickname, prosecutors brought criminal charges against a hacker who used a flaw in the AT&T login page for first generation iPads (AT&T had exclusivity over cellular-enabled iPad sales initially) to gather users' email addresses.[24] Prosecutors focused on the fact that Auernheimer went in their view beyond pure research by running an automated script that collected over 100,000 addresses. This, they suggested, indicated malicious intent beyond just revealing the security flaw in AT&T's system. He disclosed those addresses to a reporter (who only published a few redacted emails, though he mentioned the names of a few users who were affected), and was charged with two felony counts.[25]

Irrespective of how one feels about the ethics of the disclosure, it's crucial to note that this is a case where federal prosecutors brought serious federal charges for accessing information that was effectively available to the public, and where there was no circumvention of an authentication gate. That said, it is also important to recognize that the case was reversed on venue grounds in 2014 and the Justice Department declined to bring it again.

The second problem noted above is perhaps more straightforward, but still serious. Fines and prison sentences for CFAA offenses can be severe. The most punitive provision, for instance, a violation of Subparagraph (a)(5)(A) (transmission of code that damages a computer without authorization) that knowingly or recklessly causes death may carry a life sentence.

Worse, offenses that arise from the same course of conduct can result in multiple charges under different sections of the law (or other similar offenses such as identity or trade secret theft), which heightens the potential sentence and may add pressure on a defendant to plead out.[26] In the *Auernheimer* case, for instance, in addition to charging the defendant with identity

---

[24] 748 F.3d 525 (3d Cir. 2014).

[25] *Id.* at 531.

[26] The actual sentences that are meted out, however, under the CFAA are largely within the range under the United States Sentencing Guidelines, and often below (at least as of 2012). *See* U.S. Sentencing Comm'n, Economic Crime Public Data Briefing 19 (2015),

fraud under 18 U.S.C. § 1028(a)(7) (2012), prosecutors transformed the CFAA charge—a misdemeanor—into a felony by alleging a violation of the New Jersey state computer crime statute (which is functionally similar to the CFAA) as well.[27]

Likewise, in the Aaron Swartz case the prosecution was strongly criticized for the "riot act" nature of the indictment.[28] Despite JSTOR, the entity allegedly harmed, not wanting to pursue the case, the Department of Justice ultimately charged Swartz with 13 felony counts, carrying a possible sentence of more than 50 years in jail and millions in fines.[29] Many critics of the Justice Department's handling of the case point to the psychological weight of a possible jail sentence as one factor in Mr. Swartz's tragic suicide.[30]

So, what are the options? There are several. All pose significant practical challenges—especially given that the political trajectory for the CFAA has always been toward more severe penalties and a broader sweep as internet use has grown and as the privacy interests in stored data have increased exponentially, as have the practical and financial consequences of

---

http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20150109/fraud_briefing.pdf.

[27] *Id.* at 531.

[28] Orin Kerr, *The Criminal Charges Against Aaron Swartz (Part 2: Prosecutorial Discretion)*, Volokh Conspiracy, Jan. 16, 2013 ("Felony liability under the statute is triggered much too easily. The law needs to draw a distinction between low-level crimes and more serious crimes, and current law does so poorly."), *available at* http://volokh.com/2013/01/16/the-criminal-charges-against-aaron-swartz-part-2-prosecutorial-discretion/.

[29] David Kravets, *Feds Charge Activist With 13 Felonies for Rogue Downloading of Academic Articles*, Wired, Sept. 18, 2012, *available* at https://www.wired.com/2012/09/aaron-swartz-felony/. Having said that, the plea negotiations would obviously have resulted in a sentence much lower (but would have featured jail time, likely six months, and would have required Swartz to plead guilty on the 13 counts against him). Additionally, according to defense counsel, the assistant united states attorney on the case threatened Mr. Swartz with seven years in prison were he to decline the plea offer. Letter from Elliot R. Peters, Keker & Van Nest LLP, to Robin C. Ashton, Office of Prof. Responsibility, U.S. Dep't of Justice at 6 (Jan. 28, 2013), *available at* https://www.scribd.com/document/130344110/Aaron-Swartz-Lawyers-Accuse-Prosecutor-Stephen-Heymann-of-Misconduct#page=3.

[30] *See* Jenna Russell, *Hacker's Suicide Triggers Scrutiny of Prosecutor, Law*, Boston Globe, Jan. 14, 2013, *available at* https://www.bostonglobe.com/metro/2013/01/14/hacker-suicide-triggers-scrutiny-prosecutor-law-hacker-prosecution-too-harsh-critics-say/l8Cq70KJXNWwdKlF1V0yoJ/story.html.

damaging computers and networks. But most, with the exception of abolishing the law and starting over, are really very moderate proposals.

Perhaps the most ambitious—finally defining "without authorization" in the law—arguably makes the most sense. This is especially true given how courts have given short shrift in CFAA cases to key civil liberties protections, such as the rule of lenity (basically, when a law is ambiguous, it should be interpreted in the way most favorable to the defendant).[31] It also makes the most sense because it would address a whole host of other problems outside the CFAA, including providing additional clarity when it comes to good faith security research.

Below, and for the sake of discussion, we identify a few of these options.

Option 1: Rely on the Courts to Determine the Constitutionality of Certain Provisions

At least for those provisions that rely on the undefined term "authorization," there may be a path in the courts to challenge their constitutionality.[32]

The lack of clarity on the meaning of "authorization" leads to significant uncertainty among the public as to which conduct is barred, undue discretion for prosecutors, and the significant threat of inconsistent or discriminatory application of the law—all of which are the hallmarks of a "void-for-vagueness" constitutional violation.[33]

That effectively is the theory in *Sandvig v. Lynch*, a lawsuit by a number of researchers seeking to identify online discrimination who often use fake accounts to audit web services.[34] Because

---

[31] *See, e.g.*, *Nosal II*, 828 F.3d at 875, n.6.

[32] Certain provisions, including 1030(a)(7), which covers extortion, do not pose the same concerns as the provisions keyed to unauthorized access. Similarly, the damage provision under 1030(a)(5) (damaging computers without authorization through, for instance, a DDoS attack) is less concerning than a provision like 1030(a)(2)(C) (obtaining information without authorization).

[33] Risa L. Goluboff, *Dispatch from the Supreme Court Archives: Vagrancy, Abortion, and What the Links Between them Reveal About the History of Fundamental Rights*, 62 Stanford L. Rev. 1361, 1362 (2010).

[34] Complaint for Declaratory and Injunctive Relief, *Sandvig v. Lynch*, Case 1:16-cv-01368 (D.D.C. June 29, 2016).

Subparagraph 1030(a)(2)(C) (accessing a protected computer without authorization and obtaining any information) has been repeatedly applied to similar violations of websites' and services' terms of service, the researchers argue that the provision is facially unconstitutional. And, as Judge Reinhardt points out in his dissent in *Nosal II*, mentioned above, the problem in Subparagraph (a)(2)(C) flows from the lack of a definition of "without authorization," a flaw that infects the rest of the statute.

The plaintiffs in *Sandvig* also make the argument that the CFAA is an unconstitutional delegation of law enforcement authority to private parties, as private parties effectively decide what conduct will violate the law by drafting and amending their terms of service.[35]

Sandvig and similar cases could both provide greater clarity on the meaning of authorization, and could conceivably spur reform efforts in Congress to the extent they strike down portions of the CFAA as unconstitutional.

Option 2: Define "Without Authorization"

As noted, the CFAA was, in part, a response to the 1984 blockbuster WarGames. In it, Matthew Broderick plays a teenage hacker who, while "demon-dialing" (automatically dialing numbers until one finds a modem), stumbles onto an open connection to a NORAD supercomputer and almost starts a nuclear war. Interestingly, the fact that the NORAD connection was open illustrates the importance and difficulty of defining "without authorization."[36]

---

[35] *See* Complaint for Declaratory and Injunctive Relief at 41, *Sandvig v. Lynch*, No. 1:16-cv-013698 (D.D.C. June, 29, 2016).

[36] The history of the WarGames screenplay is fascinating. The writers were worried that a teenager just stumbling upon an open port of a NORAD supercomputer was simply implausible given the security they assumed would surround such a system. They consulted with an expert at RAND who had worked on a real-world NORAD system who assured them that it was entirely too plausible. Officers at NORAD would leave ports open so they could work from home on the weekends. *See* Fred Kaplan, WarGames and Cybersecurity's Debt to a Hollywood Hack, N.Y. Times, Feb. 19, 2016, *available at* http://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html.

Many argue that the "without authorization" provisions of the CFAA should operate as a computer trespass law (in other words, the provisions that do not cover fraud or extortion). That said, if you accept the classic common law formulation, trespass requires unlawful entry onto the property of another without consent.[37] Unfortunately, what constitutes trespass in the physical world does not necessarily translate well into the virtual.

Take the WarGames scenario. The physical analog might be trying all the doors in an apartment building to find one that's open, and then walking through. Should that be considered trespass? In the real world, sure. (Interestingly, the digital equivalent of trying doorknobs—port-scanning—has not been considered to be a criminal CFAA violation.)

But, in the virtual world, security researchers often actively look for those open doors, and occasionally walk through to prove that they can. Most penetration testing happens with the consent of the system owner, but there are also research efforts that "scan the internet,"[38] and some vulnerabilities can't be identified easily without gaining unauthorized access to a system or data (Heartbleed can be a good example).[39]

As Professor Orin Kerr points out, the breakdown of analogies between the physical and virtual worlds inevitably leads to a "battle of physical-space analogies" in CFAA litigation with parties using "analogies from physical spaces with the trespass norms that best aid their side."[40] Professor Kerr recently argued that the appropriate response is to adopt, or adapt, basic norms of trespass in the physical world to the virtual world, which could be embodied in a definition of "without authorization" in the CFAA.[41]

---

37 *See, e.g.*, Restatement (Second) of Torts § 158 (1965).

38 Timothy B. Lee, *Here's What You Find When You Scan the Entire Internet in an Hour*, Wash. Post, Aug. 18, 2013, *available at* https://www.washingtonpost.com/news/the-switch/wp/2013/08/18/heres-what-you-find-when-you-scan-the-entire-internet-in-an-hour/.

39 Note that there are "proxy" methods that one could use to detect the unpatched version of OpenSSL without exploiting the vulnerability. But the first method of detecting the flaw required at least de minimis access to the affected site. Erin Fleury, *Is It Illegal to Test Websites for Security Flaws? Heartbleed and the CFAA*, U. Minn. L. School LawSci Forum, Dec. 30, 2014, http://editions.lib.umn.edu/mjlst/2014/12/30/is-it-illegal-to-test-websites-for-security-flaws-heartbleed-the-cfaa/.

40 Orin Kerr, *Norms of Computer Trespass*, 116 Col. L. Rev. 1143, 1154-55 (2016).

41 *Id.* at 1163 ("The protocols of the Web make websites akin to a public forum.").

The first step in doing so is to imagine most web servers as not the equivalent of a home with an open door, but of a public or quasi-public space (this is true even if the server is intended for the use of a certain subset of users, but is not protected by some method of authenticating those users). Simply accessing such a space—walking into a shop during business hours, for instance—cannot be a trespass. However, picking the lock to a back room of course would be. Previously, Professor Kerr argued that the equivalent of lock-picking in the virtual world would be bypassing a "code-based restriction."[42] In hindsight, however, he now argues that such a test is vague, and the appropriate formulation is whether the user bypassed an "authentication restriction."[43]

Many in the privacy and civil liberties community agree with this argument—if something on the web is public facing, it is fair game for access, regardless of whether such access is automated.[44]

This approach would inject new certainty to CFAA prosecution and litigation. That said, intuitively, changing one's IP address, lying when signing up for a website, or clearing one's cookies so as to access 12 articles from the New York Times per month, when it wants you to pay for more than 10—these all may seem shady. Consider, however, the real-world analogy. If we assume that public websites are the equivalent of a shop during business hours, it would be no trespass to enter using a fake name (investigative journalists do it, for instance), or to do so multiple times with a different appearance or disguise.[45]

---

[42] Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1644-46 (2003).

[43] *Norms*, *supra* note 40, at 1164.

[44] Hanni Fakhoury & Kurt Opsahl, *EFF Amicus: Accessing a Public Website is Not a Crime*, Elec. Frontier Found., June 29, 2013, *available at* https://www.eff.org/deeplinks/2013/06/eff-access-public-website-not-crime. And, this would be true when the site tries to obscure its location by using, for instance, very long addresses.

[45] *See, e.g.*, *Desnick v. Capital Cities/ABC, Inc.*, 851 F. Supp. 303, 306 (N.D. Ill. 1994).

This approach still raises significant questions, however. Professor Kerr, for instance, argues that accessing a computer by using a "command in a way contrary to its intended function" is a proper CFAA violation.[46] For instance, Professor Kerr gives the example of SQL ("Structural Query Language") injections, where appending code to data you properly submit to a website improperly spits back more information than it should, or executes code remotely on the other system.

He argues that the physical analogy would be entering a home through a window or chimney—a violation of trespass norms. But, if you have authorization to enter the home from the friend you're attempting to visit (that is, to send a command to the website), would it be trespass to climb in through the window?

While SQL injections and similar exploits are properly controversial, and many even among the CFAA reform community argue they should be violations of the law, there may be equities that argue in favor of providing some liability protection for remote SQL code execution in certain cases.[47]

Again, Heartbleed also provides a good example. Practically speaking, it is difficult to test whether a website has the Heartbleed vulnerability without using the Heartbleed exploit. Similar to a SQL injection, Heartbleed involves sending extra language along with a normal communication that prompts the vulnerable system to do something it shouldn't. There is extreme social value in identifying systems susceptible to that or other similar vulnerabilities.[48] Is it possible to calibrate the CFAA to recognize socially valuable uses of such exploits?[49]

---

[46] *Norms*, *supra* note 40, at 1172.

[47] *See, e.g.*, Robert Graham, *Do Shellshock Scans Violate CFAA?*, Errata Security, Sept. 26, 2014, *available at* http://blog.erratasec.com/2014/09/do-shellshock-scans-violate-cfaa.html#.WDSiEqIrKRs. Graham gives the example of adding tick marks to URLs to *test* for SQL injection. "That's technically code execution," he says. "By pasting strings, website programmers have implicitly authorized us to run some SQL code, like tick marks." *Id.*

[48] CDT will be releasing an additional white paper that explores the social value of security research.

[49] One question that has been raised on the other side of this discussion is how to treat something like the Mirai botnet, which uses publicly available default passwords to infect connected devices and assemble them into a bot army (that is, should accessing the connected device with the default password constitute a CFAA violation?). A possible response to this is that the violation here is the

A similar situation arises in *Nosal II* and password sharing. In that case, a current employee of the relevant firm with full access rights to its database shared her password with two former employees, who proceeded to access the database and take valuable, confidential information.[50]

The *Nosal II* court stated, flatly, that "without authorization" is an "unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[51] The dissent argued that the majority failed to provide a "workable line which separates the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners. There simply is no limiting principle in the majority's world of lawful and unlawful password sharing."[52]

Indeed, Judge Reinhardt's dissent hits on the fundamental question at issue in this brief discussion: what limiting principle is appropriate when and if the proper option is to reform the CFAA by defining "without authorization"? The majority in *Nosal II* held that the current employee with authorized access had no authority to authorize third parties to use her password.

Professor Kerr would draw the line on the "zone of permission" conferred by the authorized account holder.[53] But, in *Nosal II*, it seems clear that the current employee agreed to give her password, presumably knowing that it would be used to access the database (in a way that would not have violated the CFAA's "exceeding authorized access" prong were she to have done it herself, based on the Ninth Circuit's previous holding in *Nosal I*).[54]

---

actual damage caused by the botnet, not the unauthorized access. That is, using a botnet is properly punishable under 18 U.S.C. § 1030(a)(5)(A) or (B) (2012).

50 *Nosal II*, 828 F.3d at 869.

51 *Id.* at 868.

52 *Id.* at 889 (Reinhardt, J., dissenting).

53 *Norms*, *supra* note 40, at 1153.

54 *See Nosal II*, 828 F.3d at 889 (Reinhardt, J., dissenting) ("It would not have been a violation of the CFAA if they had simply given FH step-by-step directions, which she then followed. Thus the

As the above discussion shows, even if one comes down on the side of addressing CFAA's problems by defining "without authorization," the hard question here is *how*? Computers benefit and infect every second of our lives, with complexity that reflects the human condition itself. These hard questions clearly reflect that complexity.

Option 3: Eliminate the "Exceeds Authorized Access" Provision

There is currently a (deep) circuit split on the meaning of the phrase "exceeds authorized access." The Second, Fourth, and Ninth Circuits have held that, so long as a user is authorized to use a system or access data, doing so for an improper purpose is not a CFAA violation.[55] And, the First, Fifth, Seventh, and Eleventh Circuits have gone the other way, finding that accessing information that you are otherwise authorized to access for an improper purpose is "exceed[ing] authorized access."[56]

The Department of Justice has specifically argued in favor of retaining the distinction, so as to allow the DOJ to go after "insiders" who exceed authorized access as well as "outsiders" who hack in.[57] But, were Congress (or the Supreme Court) to clarify the definition of "without authorization" to require the circumvention of some technical access control (or an "authentication requirement," per Professor Kerr), the phrase "exceeds authorized access" would no longer be necessary. In other words, by defining "without authorization" to require

---

question is whether because Jacobson and Christian instead used FH's password with her permission, they are criminally liable for access 'without authorization' under the Act."); *United States v. Nosal (Nosal I)*, 676 F.3d 854, 860 (9th Cir. 2012) ("Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.").

[55] *See United States v. Valle*, 807 F.3d 508 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *Nosal I*, 676 F.3d 854 (9th Cir. 2012).

[56] *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1259 (11th Cir. 2010).

[57] Leslie R. Caldwell, *Prosecuting Privacy Abuses by Corporate and Government Insiders*, U.S. Dep't of Justice, Mar. 16, 2015, *available at* https://www.justice.gov/opa/blog/prosecuting-privacy-abuses-corporate-and-government-insiders.

bypassing some access control, an individual who does so to access a restricted part of a system that she otherwise has access to would qualify as accessing a system "without authorization."

Granted, this would not cover two scenarios that the Justice Department has pointed to as reasons why it needs an expansive definition of exceeds authorized access.

The first is where the "insider" has authorization to access some data on a system but not other data, *but* where there is no technical barrier to accessing the latter. One example of that could be a user of a classified government database who accesses information that is readily accessible, but where the user does not have "need to know." The second is where a user has authorization to access the information, but does so for an improper purpose (such as in the *Valle* case).[58]

To be very clear, no one would condone government officials misusing government databases to invade the privacy of anyone. There is an ongoing problem with law enforcement accessing police databases for nefarious unofficial purposes (and not being disciplined appropriately).[59] The question is not whether such activity should be subject to criminal sanction (it should), but whether the vagueness in the current definition of exceeds authorization should be tolerated to allow the use *of the CFAA* to punish the misuse of official government databases.

CDT has argued that more tailored laws could be drafted to punish rogue government workers who inappropriately access sensitive government records (such as the very strict prohibition on improper access and disclosure of tax records).[60] And, in the private sector, numerous harassment and stalking laws currently exist that are broad enough to cover the improper use of information that an individual is otherwise authorized to access. The federal cyber-stalking

---

[58] *Valle*, 807 F.3d at 512-13.

[59] *See, e.g.*, David Kravets, *Fearing No Punishment Denver Cops Abuse Crime Databases for Personal Gain*, Ars Technica, Mar. 17, 2016, https://arstechnica.com/tech-policy/2016/03/fearing-no-punishment-denver-cops-abuse-crime-databases-for-personal-gain/.

[60] *See* 26 U.S.C. § 7213 (2012) (unauthorized disclosure of returns or return information); 26 U.S.C. § 7213A (2012) (unauthorized inspection of returns or return information).

law, for instance, is broad enough to cover any use of a computer that could conceivably cause emotional distress (even if it does not!).[61]

Again, the response to the "insider" argument presented by the Justice Department is not that such improper access or use of government or private sector information should be legal—quite the contrary. The objection is solely to the use of the CFAA as the tool to punish that activity.

Option 4: Eliminate the Civil Cause of Action, Or Require Proof of Significant Damage

Finally, Congress could address the civil provision, which would be a relatively light lift compared to abolishing the law or significantly amending it. First, it could eliminate the civil provision altogether. There are numerous alternatives to it in other state and federal laws, including trade secret theft, conversion, misappropriation, and a myriad of contract remedies. Or, at the very least, Congress could raise the requisite level of damages beyond $5,000, and define more precisely what constitutes "damage" and how to value it.

b. The Digital Millennium Copyright Act ("DMCA")

Much like the CFAA, the DMCA has also been repeatedly used by rightsholders to stifle security research.[62] Section 1201(a)(1)(A) prohibits circumventing a "technological measure that effectively controls access" to copyrighted works.[63] And Section 1201(a)(2) bars manufacture, importation, any offer to the public, or otherwise trafficking in circumvention technology.[64] Both provisions have significantly chilled security research.

Although Sections 1201(f), (g), and (j) contain express exemptions for reverse engineering, encryption research, and security testing, the exemptions are exceedingly complex, and turn on

---

61 *See* 18 U.S.C. § 2261A(2) (2012) (covering any use of a computer that "causes, attempts to cause, *or would be reasonably expected* to cause substantial emotional distress" to a person).

62 Pub. L. No. 105-304, 112 Stat. 2860 (1998).

63 17 U.S.C. § 1201 (2012), which was added as part of Section 103 of the DMCA.

64 *Id.*

certain factors that are difficult to pin down in advance of a particular piece of research.[65] Additionally, Section (j) only permits security testing that does not constitute a violation of the CFAA, meaning that the same uncertainty that infects the CFAA applies to the DMCA.[66]

Several important public safety research projects have been conducted over the past several years under the overhang of possible DMCA liability, including research showing that insulin pumps and vehicles could be hacked to control essential functions.[67] Actual litigation has also clearly chilled security research. For instance, Sony has sued researchers and hackers numerous times to prevent the disclosure of security vulnerabilities or for reverse-engineering its products.[68] The Electronic Frontier Foundation filed for a declaratory judgment in September 2016 to ensure that the mere publication of a book on vulnerabilities would not be prosecuted as a criminal violation of the anti-trafficking DMCA provision.[69]

Currently, researchers who want to experiment on many access controls, even on devices that they own or control, must rely on the triennial review process at the Copyright Office for exemptions.[70]

Fortunately, the Copyright Office approved an exemption in October 2015, which took effect in October 2016, that permits "good faith security research" with respect to consumer devices

---

65 *Id.*

66 *Id.*

67 *See* Michelle Cortez & Tatiana Darie, *J&J Warns Diabetic Patients About Hacking Risks of Insulin Pumps*, Bloomberg, Oct. 4, 2016, *available at* https://www.bloomberg.com/news/articles/2016-10-04/j-j-warns-diabetic-patients-about-hacking-risks-of-insulin-pumps; Andy Greenberg, *The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse*, Wired, Aug. 1, 2016, *available at* https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

68 *See* David Kravets, *Sony Asks Court to Remove Playstation 3 Jailbreak From Net*, Wired, Jan. 12, 2011, *available at* https://www.wired.com/2011/01/playstation3-hack-lawsuit/.

69 Press Release, Elec. Frontier Found., EFF Asks Court to Block U.S. from Prosecuting Security Researcher for Detecting and Publishing Computer Vulnerabilities (Sept. 30, 2016), *available at* https://www.eff.org/press/releases/eff-asks-court-block-us-prosecuting-security-researcher-detecting-and-publishing.

70 17 U.S.C. § 1201(a)(1)(B)-(D) (2012).

(including voting machines), motorized land vehicles, and implantable medical devices.[71] "Good faith" research is defined as "accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates."[72]

Unfortunately, that exception will last only until the next triennial review—in 2018—when it will have to be reviewed again *de novo*. Future Copyright Offices may not be as receptive to these considerations, and it remains to be seen whether the definition of "good faith" above will serve as an impediment to important research. Accordingly, DMCA reform is long overdue.

Option 1: Make the 2015 Exception Permanent (Or At Least Renew It)

This is somewhat self-explanatory. Congress could, as it did with cell phone "jail-breaking" and the Unlocking Consumer Choice and Wireless Competition Act, mandate that the Copyright Office adopt the security research exception in the 2018 triennial review.[73]

It could also amend Section 1201(j), the security research exemption, to achieve the same effect. That is, Congress could take the language in new 17 C.F.R. § 201.40(b)(7)(i)-(ii) (2016), which codified the final exceptions in the 2018 review, and append it with minor tweaks as a new paragraph in Section 1201(j). That would codify in statute the ability of security researchers to conduct good faith testing, including circumvention, with specific controls against unintended harm (doing so in a way, for instance, that is designed to avoid harm to the public).

Even if Congress does not act, the Copyright Office should certainly continue to renew these exceptions, and should continue to explore ways to encourage and protect security research through the triennial review process.[74]

---

[71] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,955-56 (Oct. 28, 2015).

[72] *Id.* at 65,956.

[73] Pub. L. No. 113-144, 128 Stat. 1751 (2014).

Option 2: Define "Without Authorization" in the CFAA

As noted, both the security research exemption in Section 1201 and the exception adopted in the 2015 triennial rulemaking are both limited by the CFAA.[75] So, even if a security research project would be permitted under the DMCA, it still may not involve unauthorized access to a computer system or data. The lack of a definition of "without authorization" therefore infects the DMCA just as it does criminal and civil liability under the CFAA proper.

In other words, were the CFAA properly limited with a clear definition of "without authorization" that required the circumvention of an technical access control or authentication requirement without authorization, researchers would have a better sense of what would be permitted under the DMCA. Granted, this would not solve the problem of, for instance, researchers reverse engineering systems that they own but that require the circumvention of an access restriction to do so.

Option 3: Require an Underlying Copyright Violation in the DMCA

One of the foundational issues with the DMCA is how it interacts with traditional defenses to copyright infringement, like fair use and the first sale doctrine. Congress, or the courts, could, once and for all, clarify that a DMCA circumvention violation must also include an underlying copyright infringement to be cognizable.

c. Wassenaar and Export Controls

The Wassenaar Arrangement ("Wassenaar") is a multi-lateral export control regime that limits the export of munitions, which are solely military, and "dual-use" goods and technologies, which can be used for both military and civilian purposes.[76] In 2013, the U.S. Department of

---

[74] *See* Harley Geiger, Joint Comments of Rapid7 et al. to U.S. Copyright Office Notice of Inquiry, Section 1201 Study: Request for Additional Comments, U.S. Copyright Office, Library of Congress, 81 Fed. Reg. 66,296 (Sept. 27, 2016), *available at* https://www.regulations.gov/document?D=COLC-2015-0012-0111.

[75] 17 U.S.C. § 1201(g)(2)(D), (j)(2) (2012).

[76] *See* The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Guidelines & Procedures, Including the Initial Elements (Dec. 2015), *available at* http://www.wassenaar.org/wp-content/uploads/2016/01/Guidelines-and-procedures-including-the-Initial-Elements-2015.pdf.

State agreed to a proposal at the Wassenaar Plenary Meeting to make intrusion and surveillance technology subject to control for the first time, in response, understandably, to reports that technology developed by member states was being acquired by countries with poor human rights records.[77]

In May 2015, the Bureau of Industry and Security ("BIS") at the Department of Commerce, which implements Wassenaar and administers dual-use export controls, issued a proposed rule to effectuate that change.[78] The comments to the rule were overwhelmingly critical, with concern from civil liberties groups and the technology community at large that the proposed rule would unintentionally sweep in technology that is instrumental in security research (which serves, among other things, to harden communications technologies in repressive countries against surveillance or intrusion).[79]

In particular, many of the tools and technologies that the rule proposed to control—meaning that export, including "deemed" exports (where the technology is simply discussed with a foreign national), would require a license from BIS—are used to identify, not exploit, vulnerabilities. Researchers routinely develop (and publish online) proofs of concept, for instance, to demonstrate a vulnerability, which would be subject to control under the proposed rule.

In March 2016, the Department of Commerce pulled the proposed rule and announced that it would be reengaging with the Wassenaar members to address the potential unintended consequences cited by commenters.[80] In particular, Secretary Pritzker stated that the United States would push to eliminate controls on technology required for the development of intrusion software. That process is currently underway. Suggestions for improvement vary, but

---

77 *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015).

78 *Id.*

79 *See* Joe Uchill, *State Department Reverses Course on Cybersecurity Exports*, Christian Sci. Monitor, Mar. 2, 2016, http://www.csmonitor.com/World/Passcode/2016/0302/State-Department-reverses-course-on-cybersecurity-exports.

80 Sean Gallagher, *US to Renegotiate Rules on Exporting "Intrusion Software,"* Ars Technica, Mar. 2, 2016, http://arstechnica.com/tech-policy/2016/03/us-to-renegotiate-rules-on-exporting-intrusion-software-under-wassenaar-arrangement/.

we list here a few of the options for improving the base text of the actual Wassenaar arrangement, and for limiting the next proposed regulation.

Option 1: Control Only Exports to Governmental Entities

The revised arrangement could exempt mass-market, consumer-focused goods and technologies. That would ensure that only exports that are intended for security, military, or law enforcement agencies of a foreign country are subject to license restrictions.

To the extent that nation-states are bypassing these license requirements by purchasing surveillance technology from the mass market or through an intermediary, that could, itself, be an export control violation. Further, much of the technology that would be of interest to a nation-state would not be of the type to be made available to the public (as it would contain, for instance, zero day exploits that could be reverse engineered).

Option 2: Base License Decisions on the Human Rights Records of the Country To Which the Product Would Be Exported

The concern that led Wassenaar to revisit the arrangement's language is absolutely valid. Surveillance technologies and intrusion tools can be used to abuse human rights, which was on stark display during the Arab Spring crackdowns in 2011.[81] The Department of Commerce could base license decisions on the human rights record of the country of importation.

Option 3: Exempt Systems Designed to *Enhance* Security

As Rapid7 recently suggested, Wassenaar could be amended to explicitly look at the design of the software at issue. Software, even if it contains exploits, is often designed to be used by administrators to identify security vulnerabilities in a given system. Wassenaar could exempt software that is designed specifically for that use.[82]

Option 4: Adopt Language Similar to the Proposed Definition of "Without Authorization"

---

[81] *See* Sari Horwitz, *Trade in Surveillance Technology Raises Worries*, Wash. Post, Dec. 1, 2011, *available at* https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html.

[82] Harley Geiger, *Wassenaar Arrangement – Recommendations for Cybersecurity Export Controls*, Rapid7Community, Mar. 18, 2016, https://community.rapid7.com/community/infosec/blog/2016/03/18/wassenaar-arrangement-recommendations-for-cybersecurity-export-controls.

Another option could be to adopt language in Wassenaar similar to the suggested definition of "without authorization" under the CFAA, discussed above. That is, members could limit the definition of "intrusion software" to software that is specifically designed to access a system without the authorization of a user or administrator and that extracts or modifies data, or denies access to the system.[83]

Option 5: Limit Controls on "Deemed Exports" in Research and Academic Contexts

One other issue that will likely persist regardless of the outcome in the new round of negotiations is the problem of deemed exports.[84] Even with the limitations proposed above, a license will be required for the written or oral transmission of controlled information, which may affect security researchers who share, for instance, proofs of concept at academic conferences or even the vast number of research groups (independent, academic, or commercial) that include foreign nationals.

Given the particular sensitivity with respect to the First Amendment and free expression in the United States, there should be a broad exception for disclosure of information about vulnerabilities in academic or research contexts.

IV. The Enforcer. Should the DOJ or Congress Formalize Prosecutorial Forbearance?

Shortly before publication of this white paper, in connection with unspecified ongoing litigation, the DOJ released a 2014 memorandum from the attorney general titled "Intake and Charging Policy for Computer Crime Matters."[85] The document offers non-binding guidance for federal prosecutors in CFAA cases, and provides eight non-exhaustive factors that prosecutors are directed to consider in making charging decisions.[86] The eight factors are summarized below:

---

83 *Id.*

84 15 C.F.R. § 734.13 (2016).

85 *See* Leslie R. Caldwell, *Department Releases Intake and Charging Policy for Computer Crime Matters*, Justice Blogs, Oct. 25, 2016, https://www.justice.gov/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters.

86 Computer Crime Charging Memorandum, *supra* note 12.

- The sensitivity of the affected computer system or information and the likely harm in disclosure (such as unauthorized access to personally identifiable information, intimate photographs or documents, intellectual property, or classified material);[87]

- The potential for impact on significant national or economic interests, including federal prosecution for activity that affects sizeable portions of the country or populace and deference to state or local authorities for conduct with a geographically limited effect;[88]

- Connection to other criminal activity or risk of bodily harm;[89]

- The impact of the crime or the prosecution on the victim;[90]

- Whether the conduct consists of exceeding authorized access, and if it does, notably, whether the prosecutor can prove that the defendant knowingly violated restrictions on her authority to access the system or data, and not that the defendant merely misused information that she was otherwise authorized to access;[91]

- Whether particularly egregious conduct weighs in favor of federal prosecution as a deterrent matter, especially in light of technological advances;[92]

- The extent of harm specific to one federal district (where prosecution may be warranted when the harm to a single district is significant);[93] and

---

87 *Id.* at 2-3.

88 *Id.* at 3.

89 *Id.* at 3-4.

90 *Id.* at 4.

91 *Id.* at 4-5.

92 *Id.* at 5.

93 *Id.*

- The possibility of effective prosecution in another jurisdiction.[94]

These factors certainly make sense when deciding whether to prosecute a bad actor, but provide little guidance on how to address a case like *Auernheimer*, which implicates bona fide security research. Indeed, the attorney general's memorandum does not include any direct discussion of security research or security researchers. And certain factors could arguably skew the charging decision in a direction that furthers the chill against security researchers.

For instance, the first factor—the sensitivity of the affected system—is particularly relevant given that one would want security researchers to be hunting for vulnerabilities in the most sensitive systems. It is precisely for that reason that many bug bounty programs will offer the largest award for bugs that affect the most personally sensitive data (such as Google, which offers the highest reward for a bug that allows remote code execution that permits taking over a Google account).[95]

Similarly, some of the most significant security research in recent years has uncovered bugs in cars and implantable medical devices, and precisely because of the real danger of severe physical or economic harm one would hope for aggressive vulnerability hunting in critical infrastructure.[96] In all of these cases, at least in the abstract, "unauthorized access" under the CFAA implicates a threat of bodily harm or a significant national economic or security interest.

Likewise, some of the most important research will have the broadest geographic effect. For instance, the Mirai botnet has made headlines repeatedly over the fall of 2016 as being responsible for some of the largest distributed-denial-of-service ("DDoS") attacks ever.[97] In late

---

94 *Id.*

95 *See* Google Application Sec., Google Vulnerability Reward Program (VRP) Rules, https://www.google.com/about/appsecurity/reward-program/.

96 *See, e.g.*, Booz Allen Hamilton, Industrial Cybersecurity Threat Briefing (2016) (noting that, of 314 industrial control system operators surveyed worldwide, 34 percent of respondents reported being breached more than twice in the last year).

97 *See* US-CERT, Alert (TA16-288A), Heightened DDoS Threat Posed by Mirai and Other Botnets, Oct. 14, 2016, https://www.us-cert.gov/ncas/alerts/TA16-288A.

October, an attack against the DNS services company Dyn rendered a number of major websites, including Twitter, Netflix, and Amazon, unreachable.[98]

The Mirai botnet works by constantly scanning for connected devices with default passwords, including devices with hard-coded firmware passwords that cannot be changed by the user or administrator.[99]

In response, security researchers have developed a proof of concept that could be used to crash Mirai infected bots and disrupt attacks. The same exploit could also change the default passwords of the devices, rendering them unusable by both the botnet controller—and the user. The point here isn't that executing this exploit should be immune from the reach of the CFAA (though that may be a conversation worth having), but that some of the most important security research has the longest reach geographically.

Two potentially positive aspects of the DOJ's guidance are worth noting.

One, the guidance does make clear that in "exceeding authorized access" cases, the prosecutor should be prepared to prove that the user knowingly violated restrictions on the user's ability to access the relevant data. That may prove a check on prosecutorial discretion in close cases. It doesn't, however, quite get to the clearest formulation of exceeds access, which is that an insider exceeds authorized access when they have authorization to use a system, but circumvent authentication gates that protect other parts of the system.[100]

Two, the guidance does require consultation with the DOJ's Computer Crime and Intellectual Property Section ("CCIPS") before a prosecutor makes a charging decision.[101] This seems like an

---

98 Nicky Woolf, *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say*, The Guardian, Oct. 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

99 Brian Krebs, *Source Code for IoT Botnet 'Mirai' Released*, KrebsonSecurity, Oct. 16, 2016, https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

100 Importantly, especially in the government context when a government employee has access to sensitive personal data, this is not to say that unauthorized access to information in the broader sense, and especially disclosure, cannot be criminalized. For instance, it is a (potentially serious) crime for employees of the Internal Revenue Service to access or disclose confidential taxpayer information without specific authorization. *See* 26 U.S.C. §§ 7213, 7213A (2012). All that CFAA critics argue is that such activity should not be a CFAA violation.

101 Computer Crime Charging Memorandum, *supra* note 12, at 5-6.

appropriate safeguard, though it would be helpful for the DOJ to release more information on how and when CCIPS guidance influences prosecutors' charging decisions (especially if CCIPS is suggesting that prosecutors add or stack charges).

In any event, we suggest a few options for discussion here.

Option 1: Add a Discussion of Security Research in the Existing Guidance

The DOJ has done an admirable job of outreach to the security community. It could expand on that outreach by revising the attorney general's guidance to include a section on security research, with specific examples of conduct that the department does not believe rises to the level of a chargeable CFAA offense. Similarly, it could game out some of the possible charging strategies with an eye to limiting duplicative or draconian charges. It could even do so in a formal rulemaking with practical examples illustrating what will or will not lead to an investigation and possible prosecution.[102]

Option 2: Require a Showing of Damage for the "Obtaining Information" Offense

One option for CFAA reform, noted above and incorporated into Aaron's Law, would be to slightly modify the penalties for one of the most controversial provisions, Section 1030(a)(2)(C), which covers unauthorized access, or exceeding authorized access, to a protected computer and obtaining any information. The proposed change would amend Section (c)(2)(B)(i) and (ii), which trigger felony liability under that section.[103]

It would set a dollar amount of predicate damage for clause (i), which right now simply reads "if the offense was committed for purposes of commercial advantage or private financial gain."[104] And, it would limit the trigger in clause (ii) to a federal or state crime (as opposed to a tort).[105]

---

102 *See, e.g.*, Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 73 Fed. Reg. 70,702, 70,716-29 (Nov. 21, 2008) (including illustrative examples throughout the final rule governing review by the Committee on Foreign Investment in the United States ("CFIUS")).

103 *See* Aaron's Law Act of 2015, S. 1030, 114th Cong. § 4 (2015).

104 *Id.* § 4(a)(2).

105 *Id.* § 4(a)(3).

The DOJ could adopt these requirements as a matter of discretion and list them in the guidance. Additionally, as noted in Option 1 above, the DOJ could conduct a formal rulemaking to create a regulation perhaps similar to 28 C.F.R. § 50.10 (2016), which governs when and how prosecutors may issue subpoenas for information on members of the news media.

That regulation could use a formulation similar to the carve out under the 2015 DMCA triennial review to provide greater certainty that research in a controlled environment that is designed to avoid harm will not be subject to prosecution under the CFAA. And it could include illustrative examples throughout the rule to give researchers greater clarity.[106]

V. The Incentives. What Are Best Practices for Bug Bounty Programs?

The debate over vulnerability disclosure is as old as security engineering itself. The notion of "security by obscurity" dates back at least as far as the extraordinary efforts the Byzantine Empire deployed to maintain the secret of "Greek Fire"—an incendiary weapon system the formula for which remains a mystery to this day.

During the 19th century, locksmiths engaged in a spirited debate over the importance of "full disclosure" of physical vulnerabilities in locks. That debate mirrors both the full disclosure security research debate today, and, in many ways, the American concept of free expression generally—that a "marketplace" of ideas will prove more efficient in elevating truth, suppressing falsehood, and promoting innovation and invention.

This discussion continues today in the digital realm. By this point, the battle lines are generally firm. While there are still arguments out there in favor of non-disclosure,[107] much of today's conversation centers around what actually constitutes coordinated or "responsible" disclosure

---

[106] For instance, one could imagine an example such as this: "Example 1: Security Researcher A uses tick marks to test Website B for vulnerability to SQL injections. Even though use of tick marks technically constitutes unauthorized access to a protected computer under the CFAA, and utilizes resources without authorization on Website B's server, such activity is a standard method of testing for online vulnerabilities, presents little risk of harm, and uses only a de minimis amount of Website B's resources. In such cases, these three factors will counsel against any action by the department."

[107] Arguments in favor of non-disclosure tend to question whether vulnerability disclosure actually has the desired effect—the improvement of computer security by prompting vendors to fix vulnerabilities as quickly as possible. *See, e.g.*, Marcus J. Ranum, *The Vulnerability Disclosure Game: Are We More Secure?*, CSO, Mar. 1, 2008, http://www.csoonline.com/article/2122977/application-security/the-vulnerability-disclosure-game--are-we-more-secure-.html.

versus full disclosure ("responsible" is a loaded term in that it suggests that anything else is *ir*responsible disclosure).[108]

There is also a subspecies of coordinated disclosure supporters who believe that it is only effective when backed by the threat of full disclosure in the face of a dilatory vendor. For instance, Bruce Schneier argues that coordinated disclosure is a "good idea . . . but one that was possible only because full disclosure was the norm. And it remains a good idea only as long as full disclosure is the threat."[109]

These conversations are by now old hat. What is relatively new is the growth in the computer security economy. This new economy includes vulnerability merchants, who sell exploits to governments or private companies, and "bug bounty" programs, in which vendors will compensate security researchers who abide by certain guidelines when disclosing a vulnerability (with a variety of awards, both monetary and reputational).

The first "bugs" bounty program was launched by Netscape in 1995 right before the release of its Navigator 2.0 beta.[110] Notably, the program applied to the Navigator beta with pre-beta (or "alpha") Java code, so Netscape and Sun Microsystems (with Eric Schmidt as chief technology officer) collaborated on the program. They offered cash prizes (which even now are somewhat rare) for the most serious bugs. Users finding any bug would receive merchandise, and those finding other serious bugs would be eligible to win items from the Netscape General Store.

Interestingly, the Netscape Bugs Bounty prompted an early "full disclosure" debate in 1997. A Danish researcher discovered a flaw in Netscape browsers that allowed administrators of websites to access files on the hard drive of someone visiting their site.[111] The researcher then

---

108 Accordingly, we use the term "coordinated" here. *See* Chris Evans et al., *Rebooting Responsible Disclosure: A Focus on Protecting End Users*, Google Security Blog, July 20, 2010, https://security.googleblog.com/2010/07/rebooting-responsible-disclosure-focus.html.

109 Bruce Schneier, *Full Disclosure of Security Vulnerabilities a 'Damned Good Idea*,' Schneier on Security, Jan. 2007, https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html.

110 Press Release, Netscape, Netscape Announces "Netscape Bugs Bounty" With Release of Netscape Navigator 2.0 Beta (Oct. 10, 1995), *available at* http://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html.

111 *Netscape Mum on Bug Details*, CNET, June 14, 1997, *available at* http://www.cnet.com/uk/news/netscape-mum-on-bug-details/.

went to CNN with the story because, he claimed, Netscape was not paying appropriate attention to the problem (the researcher also refused to disclose the technical details of the flaw, which required Netscape to identify the problem and engineer a fix on its own).[112]

Even then, 20 years ago, the ethical issues surrounding the disclosure were prominent in the story. PC Magazine, which had worked with the researcher in identifying the flaw, said, "If you're in the computer industry and you find a flaw in a [popular] software program, should you give the information to the company? We're using Navigator all the time; we have an interest in seeing it fixed."[113]

Despite early enthusiasm for the program, including a New York Times story on the front page of the business section highlighting the emerging security economy and a generation of researchers that seem more "vigilant than vigilante,"[114] the Netscape model failed to take off during the early years of the web.

The "modern" era of bug bounty programs probably started with Mozilla's Security Bug Bounty Program, launched in 2004, which has paid out more than $1.6 million to date.[115] Mozilla has two distinct programs—one for Mozilla software (the client bounty program)[116] and another for Mozilla websites and services.[117]

---

112 *Netscape to Fix Flaw*, CNNMoney, June 13, 1997, http://money.cnn.com/1997/06/13/technology/netscape_bug/.

113 *Id.*

114 John Markoff, *The New Watchdogs of Digital Commerce*, N.Y. Times, Oct. 16, 1995, at D1, *available at* http://query.nytimes.com/gst/fullpage.html?res=990CEFDC1131F935A25753C1A963958260&pagewanted=all.

115 Mozilla, Bug Bounty Program, Mozilla.org, https://www.mozilla.org/en-US/security/bug-bounty/.

116 Mozilla, Client Bug Bounty Program, Mozilla.org, https://www.mozilla.org/en-US/security/client-bug-bounty/.

117 Mozilla, Web and Services Bug Bounty Program, Mozilla.org, https://www.mozilla.org/en-US/security/web-bug-bounty/.

It is worth briefly reviewing the basic ground rules, which share many characteristics with other major bug bounty programs, including those of Google, Facebook, and Microsoft (though Microsoft and Facebook are slightly more aggressive in terms of requiring and rewarding coordinated disclosure).[118]

The client program requires that the bug be a "remote exploit, the cause of a privilege escalation, or an information leak." The web and services program requires that the bug "[allow a] remote exploit, compromise user data, allow access to Mozilla infrastructure or resources, or easily manipulate a user." Both require that the bug be original and unreported, and that the submitter not be the author of the "buggy" code or otherwise involved in its creation. Mozilla employees and volunteers are ineligible.

The client program is much more remunerative than the web and services program. The payouts in the former range from $500-$2500 for a medium vulnerability to more than $10,000 for a novel vulnerability and exploit, a new form of exploitation, or an exceptional vulnerability. Submitters to the latter are eligible for bounties of between $500 and $3000 (or higher for critical sites like Bugzilla, Mozilla's bug reporting portal).

Interestingly, Mozilla has also prepared formal guidelines for the handling of Mozilla bugs. They explicitly give the reporter of the bug the power to deflag a bug as "security sensitive" in the Bugzilla system, which will make the bug public. The guidelines do not require the signing of a non-disclosure agreement or other binding contract. They merely ask that the reporter follow a number of voluntary guidelines, including giving the relevant "bug group" a few days' notice of the disclosure, and that the reporter be "understanding and accommodating if a Mozilla distributor has a legitimate need to keep the bug in the security-sensitive category for some reasonable additional time period, e.g., to get a new release distributed to users."[119]

---

[118] Facebook, for instance, has an express "responsible disclosure policy" with five prongs. The researcher: (1) must give Facebook "reasonable time" to investigate and fix a bug; (2) may not interact with an individual account without consent; (3) must make a "good faith" effort not to infringe on the privacy of users, disrupt services, or harm data; (4) may not exploit a vulnerability for any reason; and (5) may not violate any other laws or regulations. Facebook Bug Bounty Rules, Facebook.com, https://www.facebook.com/whitehat.

[119] Mozilla, Handling Mozilla Security Bugs, Version 1.1., Mozilla.org, https://www.mozilla.org/en-US/about/governance/policies/security-group/bugs/.

The following half decade or so has seen a proliferation of bug bounty programs, as well as the creation of companies like Bugcrowd or HackerOne that can implement a bounty program for other companies. Recent years have also seen the emergence of "private" bounty programs that operate by invitation only. Bugcrowd notes that the growth of private programs is due to two factors: (1) companies looking to start a public program want to start small and beta test their ability to respond; and (2) organizations with complex technology tend to pay higher bounties and want to attract top talent.[120]

So, the question then is, with the maturation of the computer security "economy," can we identify any best practices, or other ways to further improve bug bounty efficacy?

Option 1: Professionalize White Hat Hacking

In 2015, United Airlines launched the first airline bug bounty program, and somewhat controversially awarded bounties in the form of airline miles.[121] Though many security researchers hunt bugs as a hobby, or for community recognition (several bounty programs expressly permit the researcher to donate the award to charity), others do it as a source of income.

Indeed, with the creation of companies like Bugcrowd and HackerOne, which are turning bug bounty programs into a saleable turn-key service, is there a way to make computer security research focused on identifying vulnerabilities in key systems and sites a long-term vocation?

Obviously security research is a vocation, but the idea here would be to create and enforce certain norms like rates of pay; objective, accepted methods of categorizing the seriousness of the vulnerability; timelines for disclosure; and an expectation of disclosure for serious vulnerabilities or for vulnerabilities that are being actively exploited. The same norms could also pressure companies that have bug bounty programs that disqualify participants for

---

120 Bugcrowd, The State of Bug Bounty 10 (2016), *available at* https://pages.bugcrowd.com/2016-state-of-bug-bounty-report.

121 *See* Liam Tung, *This Dutch Hacker Can Fly a Million Miles on His United Airlines Bug Bounty*, ZDNet, Aug. 9, 2016, http://www.zdnet.com/article/this-dutch-hacker-can-fly-a-million-miles-on-his-united-airlines-bug-bounty/.

disclosure to change their approach (i.e., a professional class of hunters would refuse to participate in any program that disqualifies participants for disclosure at all).[122]

Option 2: Create a Government Bug Bounty and Buy-and-Disclose Entity

Government agencies are also getting into the bug bounty game. In partnership with HackerOne, the Pentagon launched in 2016 the first ever bug bounty program in the federal government.[123] The pilot program covered only certain public-facing Defense Department websites such as defense.gov. HackerOne recruited more than a thousand participants (who had to undergo a criminal background check). The program generated about 1200 vulnerability reports, 138 of which were deemed valid. The total cost was $150,000 and payouts accounted for about half.[124]

Other government agencies could launch their own permanent bug bounty programs, and do so beyond just public-facing websites. One potential home for the program could be the United States Computer Emergency Readiness Team ("US-CERT"), a division of the Department of Homeland Security, which already publicly disseminates security information.

Indeed, the government could go further. For instance, as a counter-weight to the intelligence community and military, a civilian agency could be created to run a government-wide bug bounty program that would have clear and public rules for when a vulnerability will be disclosed publicly, a formal presumption in favor of disclosure, and a seat at the table in the controversial "vulnerabilities equities process," or VEP.[125]

Option 3: Develop and Clarify Rules Around Publication in the Absence of a Fix

Existing bug bounty programs currently reflect the split of opinion between advocates of coordinated disclosure and full disclosure. Though disclosure deadlines have long been an

---

122 United Airlines was criticized for precisely this rule. Rene Millman, *Security Researcher Blasts United Airlines Bug Bounty Program*, SC Magazine, Nov. 23, 2015, http://www.scmagazineuk.com/security-researcher-blasts-united-airlines-bug-bounty-programme/article/455550/.

123 Hack the Pentagon Fact Sheet, Defense.gov, http://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf.

124 *Id.*

125 *See generally* Ari Schwartz & Rob Knake, Government's Role in Vulnerability Disclosure (2016), *available at* http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

industry standard, there is some variation among different disclosure regimes. Google, for instance, has adopted Project Zero's (Google's in-house bug hunter) 90-day deadline with a few exceptions for holidays and when a vendor asks for a short grace period.[126]

There are also exceptions for extreme circumstances, including active exploitation (meaning when a bad actor is actually exploiting the vulnerability "in the wild"). One option would be for the government, or potentially an Information Sharing and Analysis Center ("ISAC"), to convene a multi-stakeholder process to come up with a formal industry standard for disclosure deadlines, and to identify specifically those extreme circumstances where disclosure is perhaps mandated, not just permitted.

During CDT's December convening, several participants raised the point that there are some equities that weigh in favor of patching on a periodic basis (as opposed to immediately when a fix is available), as constant patches may be ignored. This, they argued, is a point in favor of not publishing in the absence of a fix. Similarly, some argued that publication under the full disclosure approach, or the coordinated disclosure under threat of publication, is not necessarily a good fit for some companies, especially those who may not have full control of how their products are being used by their customers.

Similarly, another point that was raised is what happens when there's an intractable disagreement between the researcher and the vendor concerning whether, for instance, the vulnerability is actually a vulnerability or a design choice. Some suggested that a third-party organization tasked with resolving those disputes might be a viable solution. Others argued that disagreement over the third party could confuse things and delay appropriate disclosure.

Option 4: Encourage Coordinated Disclosure Policies Without Bounties

Even in the absence of bug bounties, companies should adopt coordinated disclosure policies that provide a mechanism and ground-rules for security researchers to disclose vulnerabilities. Some companies may not want to encourage security research, but they would still benefit from having an express policy for receiving, processing, and mitigating security vulnerabilities, which gives security researchers comfort that disclosing a vulnerability will not invite legal action.

---

126 *See* Chris Evans et al., *Feedback and Data-Driven Updates to Google's Disclosure Policy*, Project Zero, Feb. 13, 2015, https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html.

For instance, though it does not have a bug bounty program (unless you count public acknowledgment of the researcher in the patch), Rapid7 provides for intake, processing, mitigating, and coordinating with the researcher through a formal policy.[127]

Oracle has a very similar process. If the researcher does not publish the vulnerability prior to Oracle releasing a fix, Oracle will credit the researcher in the critical patch advisory. Oracle also goes further and requires that the researcher not divulge the exact details of the exploit, such as proof-of-concept code.[128]

Although these policies run counter to the full disclosure paradigm (or the coordinated disclosure, backed up by full disclosure, approach), they nevertheless may be helpful for researchers seeking to avoid potential civil exposure for disclosures.

VI. The Rules. Can or Should Security Researchers Agree on Ethical Redlines?

There are actually a couple of separate debates, each with several facets, about the ethics of security research. These go far beyond the typical "white hat" versus "black hat" paradigm with which most of the general public is familiar.

At the far extreme, is an active conversation about the ethics of teaching offensive cyber-tactics—the use of vulnerabilities and exploits to harm a military adversary, extort money or something else of value, or steal information.[129]

On the defensive side, there is some tension between the "hacker ethic"—which emphasizes sharing, free access to computers, and hostility to authority—and a more aggressive "white hat" approach that, for instance, would draw an ethical line at experimenting on live systems or

---

127 *See* Rapid7, Vulnerability Disclosure, https://www.rapid7.com/disclosure/.

128 *See* Oracle, Vulnerability Handling, https://www.oracle.com/support/assurance/vulnerability-remediation/reporting-security-vulnerabilities.html.

129 *See* Ellen Nakashima & Ashkan Soltani, *The Ethics of Hacking 101*, Wash. Post, Oct. 7, 2014, https://www.washingtonpost.com/postlive/the-ethics-of-hacking-101/2014/10/07/39529518-4014-11e4-b0ea-8141703bbf6f_story.html.

altering data on a remote system without authorization.[130] And, there is a related, but separate, conversation about the ethics, propriety, and effectiveness of "hacking back."[131]

Finally, and crucially, there is a pragmatic concern with even trying to identify clear ethical lines in the computer security context. As has been shown with the history of CFAA enforcement, generalist courts are desperate for guidance from the technical community on what "without authorization" even means. There is legitimate fear that identifying ethical redlines in the computer security context will lead to improper applications of the CFAA in tougher cases.

One clear example of this fear manifested is the "Weev" case noted above, *United States v. Auernheimer*.[132] The facts are worth recounting.

AT&T was the exclusive carrier for the first-generation, cellular-connected iPad in 2010. As a matter of convenience, AT&T engineered the login site for its iPad data service to recognize whether the iPad seeking access had already been registered with AT&T.[133] If so, AT&T redirected the user to another login page, which included the iPad device identifier in the web address. Once there, AT&T auto-filled the associated email address, so users would just have to enter their password.[134]

Auernheimer, and a colleague, discovered that if you changed a digit in the iPad identifier, the webpage would auto-fill a different email.[135] They then wrote software that automatically tried different iPad identifiers in the URL, and then collected the emails as they discovered them.[136]

---

130 *See, e.g.*, Steven Johnson, *Robin Hoods of Cyberspace*, N.Y. Times Book Rev., Mar. 4, 2001, *available at* http://www.nytimes.com/books/01/03/04/reviews/010304.04johnsot.html.

131 *See, e.g.*, Ctr. For Cyber and Homeland Sec., George Washington Univ., Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats, app. 1 (2016) (incorporating additional views of Nuala O'Connor and discussing the debate over "active defense" and "hacking back"), *available at* https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

132 748 F.3d 525 (3d Cir. 2014).

133 *Id.* at 529.

134 *Id.*

135 *Id.* at 530.

136 *Id.* at 530-31.

In total, they "scraped" more than 110,000 email addresses, and then notified the press, transmitting the list of addresses to the website Gawker. Reporters notified AT&T, which fixed the breach. Gawker then published the story, including the names of some of the iPad owners who were affected (though it only included a few redacted images of emails and iPad identifiers).[137]

Auernheimer was charged with two felonies, both of which turned on an underlying violation of the CFAA. (The Auernheimer case also demonstrates how charges under the CFAA can be creatively stacked to dramatically heighten penalties.)

Count one alleged a conspiracy to violate Section (a)(2) of the CFAA (obtaining information from a protected computer without authorization), which was bumped up to a felony under Section (c)(2)(B)(ii) because, the prosecution alleged, the CFAA offense was also a violation of New Jersey's state computer crime law, which is similar in design to the CFAA.[138] Count two alleged a violation of 18 U.S.C. § 1028(7) (2012), an identity fraud provision that covers transmitting any identity information in furtherance of another crime (in this case the CFAA violation).[139]

At trial, Auernheimer was sentenced to three years in prison. His conviction was overturned on appeal because the alleged crime had insufficient ties to New Jersey, where the indictment was initially brought. But many in the criminal defense, civil liberties, security research, and cybersecurity communities objected to the underlying theory of the case: that accessing information that is made publicly available on the internet can ever be a violation of the CFAA.

This is not a suggestion that the conduct here was "ethical" or proper. There is no dispute that the "scraping" violated the privacy expectations of first generation iPad owners (consider what would happen if the scrape was of an adult subscription website or an "alt-right" message board).

---

137 *Id.* at 531.

138 Criminal Complaint, *United States v. Auernheimer*, Mag. No. 11-4022, at 2 (CCC) (D.N.J. Jan. 13, 2011).

139 *Id.*

Rather, the issue here was that, under the government's theory, there would be no limiting principle, and the fact that Auernheimer "ought to have known" that what he was doing was unauthorized by AT&T was enough to support a serious federal charge.[140] It also raised concerns that a company could transform "icky" conduct into a federal crime by simply saying that a particular use of the internet is "unauthorized."

The point of this discussion is not to suggest that ethical lines cannot be drawn. Rather, it is to suggest that if those ethical lines are improperly drawn, they may then be adopted by courts and the Department of Justice as guidelines for when prosecution is warranted, which could make the existing chill on security research worse.

On the flip side, there are very real instances of abusive security research that may not constitute a CFAA violation, but may be worthy of criticism by the community.

Take just one recent, high-profile example: the bombshell story that appeared in Slate shortly before the November 2016 presidential election suggesting that a Trump server may have a dedicated line of communication with a Russian bank.[141] Irrespective of the merits of the story, the actual data used by the anonymous researcher was data shared by ISPs with security researchers specifically for the purpose of detecting and helping to design mitigations against malware and spam. This is particularly sensitive data that ISPs generally keep very close. This kind of data can be used to trace internet activity, in some cases even if it is encrypted, using those DNS lookups (which is precisely what the researcher did).

Normally that information would be used to identify malicious activity. Here, however, it was used to say merely that this server is pinging another server, which is a significant invasion of privacy.[142]

---

140 *See* Orin Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, Wash. Post, Jan. 14, 2015 ("[U]se of a computer might be deemed an illegal act of unauthorized access if it is simply beyond the pale of accepted social practices."), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/?utm_term=.64a3f3742c73.

141 Franklin Foer, *Was a Trump Server Communicating With Russia?* Slate, Oct. 13, 2016, http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html.

142 Robert Graham, *Debunking Trump's "Secret Server,"* Errata Sec., Nov. 1, 2016 ("The big story isn't the conspiracy theory about Trump, but that these malware researchers exploited their privileged

Another good example of this tricky line is the recent story of Muddy Waters Capital LLC releasing a report that relied on cybersecurity research by a company called MedSec that certain implantable devices manufactured by St. Jude Medical contained serious vulnerabilities. Prior to releasing the report, Muddy Waters shorted St. Jude stock, presumably hoping to profit from the report. St. Jude then sued, alleging that the report had relied on false information.[143]

There are no ready answers to these questions. It is entirely conceivable that somewhat objectionable or "icky" research will uncover very serious security vulnerabilities, which should be reported. In that case, the equities are not as clear cut (one example might be the remote hacking of Jeeps with the permission of the driver, but not the company). The underlying research may be problematic (in the Jeep case, experimenting on a live vehicle on a public highway).[144] But the dramatic demonstration may result in added pressure for the vendor to fix the problem (and the recall of 14 million vehicles to mitigate the remote access problem).

As we have done throughout this white paper, we offer a few options with respect to ethical redlines below.

Option 1: Track an Amended CFAA

The fundamental problem with the CFAA is that no one knows what "without authorization" means. Again, an amended CFAA, with a clear definition of "without authorization," along with precise damage and loss amounts, could provide some clarity to security researchers as well.

Option 2: Adopt a Pre-Existing Ethical Framework

The security researcher community could expressly adopt broader computer research codes of ethics, such as the Association for Computing Machinery's 1992 code, which expressly requires ACM members to "avoid harm," "be fair," "honor property rights," and "respect the privacy of

---

access for some purpose other than malware research."), http://blog.erratasec.com/2016/11/debunking-trumps-secret-server.html#.WDtmZfkrJhG.

143 Tess Stynes, *St. Jude Medical Sues Short Seller Over Device Allegations*, W.S.J., Sept. 7, 2016, *available at* http://www.wsj.com/articles/st-jude-medical-sues-short-seller-over-device-allegations-1473258343.

144 Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, Wired, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

others."[145] Indeed, the ACM code specifically bars using computing resources without approval.[146]

The ACM code is the outgrowth of several decades worth of thinking around computer ethics more broadly, especially with respect to hardware or software design. Security research, focused as it is on identifying flaws in another's creation, offers unique ethical challenges that remain, as we have seen, in a state of development—in many ways because security research itself is evolving into both a business and a vocation, not just a hobby.

Accordingly, as articulated by James Moor in his 1985 article, "What is Computer Ethics?," the development of an ethical code around security research suffers from the same issue as any other code of ethics in an emerging technological space.

As Moor put it, "[a] typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate."

Consequently, the ethics of security research are, in many ways, in flux because new security challenges arise with every major technological advancement like the smartphone or the connected car. Our hope is that this paper will help identify some of the core emerging issues that demand some thinking around an ethical framework.

Option 3: Adopt only the Brightest of Bright Lines

Even in the professions, which share many of the same characteristics of security research in terms of clashing equities, there are very few bright lines.

For instance, there really is no good, clear rule on when a criminal defense attorney is permitted to present false evidence at trial. The rules differ from jurisdiction to jurisdiction, but the general gist is that (1) the lawyer must know the contemplated testimony is false, (2) the lawyer must attempt to dissuade the client from presenting the false testimony, and, if the

145 Assoc. for Computing Mach., ACM Ethics, http://ethics.acm.org/code-of-ethics.

146 *Id.*

lawyer is unsuccessful, (3) the lawyer may withdraw as long as withdrawal would not prejudice the client. In practice, application of the rule is a fact-intensive bear of a problem.[147]

By contrast, there are a few bright line rules in the legal profession. And they share two key characteristics: they are easy to enforce, and violations are easy to spot. For instance, lawyers may not commingle client funds and attorney funds. Similarly, lawyers may not take a criminal case on contingency.

There may be similar practices in the security research context. For the sake of discussion, we offer a few below:

- Are there limits that can be placed on testing live systems? Would any risk of physical harm, or disruption to the system, create a bright line?

- Would the interception of actual communications content be a viable bright line, the legality of such activity aside?

- What about unauthorized access? Is there a way to articulate a *de minimis* quantum of data for which unauthorized access would not cross an ethical line? Is unauthorized access to another system, period, an appropriate bright line?

- On the flip side, what if unauthorized access is necessary to stop a major threat to computer security generally (disrupting a Mirai botnet, for example[148])? Is there a way to articulate a threat so significant that the ends justify the means to disrupt it, even if they would otherwise violate a bright line rule on the other side?

Option 4: Formalize Legal and Ethics Training for Engineers and Computer Scientists

During CDT's December convening on this topic, there was a significant amount of attention paid to legal and ethical training for engineers, computer scientists, and other technical trades that feed into computer security research. Many argued that—especially with the uncertainty surrounding the scope of the CFAA and other unresolved legal questions—lawyers, let alone

147 *See, e.g.*, D.C. Bar Ethics Op. 234 (1993), *available at* https://www.dcbar.org/bar-resources/legal-ethics/opinions/opinion234.cfm.

148 *See* Scott Tenaglia, *Killing Mirai: Active Defense Against an IoT Botnet (Part 1)*, Invincea Labs, Oct. 22, 2016, https://www.invincealabs.com/blog/2016/10/killing-mirai/.

researchers, have a difficult time spotting the various issues that may arise in the course of security research.

One option presented would be to formulate pedagogical best practices for legal and ethical courses in the various technical disciplines relevant to security research. Having such courses be mandatory—similar to a professional responsibility class in law school—could serve as a way to improve security ethics while avoiding "one-size-fits-all" legal rules that could impinge on rights in the harder cases. (Additionally, legal and ethical training could help crystallize difficult concepts such as a "controlled environment" for testing.)

VII. Conclusion

"The cyber" is going to be with us for a long time, and in ways that we cannot even imagine now. As this past election starkly demonstrated, anxiety over the integrity of the actual mechanics of our election is corrosive to public trust in our system of government. Security research and security researchers, when given the breathing room to do their work, and financial incentives to do it in a way that promotes optimal cybersecurity, are key to protecting that public trust by identifying vulnerabilities and lighting fires that lead to important fixes.

We have offered four areas here of possible inquiry: whether legal changes could lead to greater certainty for researchers, whether a structured approach to charging decisions under computer crime laws could also provide greater clarity, whether it's possible to further refine bug bounty programs and possibly create a civilian government entity that could promote vulnerability disclosure, and whether the community can identify ethical redlines in security research.

We very much hope that the quest to answer these "hard questions" leads to policies that promote cybersecurity, privacy, and, consequently, greater faith in our digital civic lives.

CENTER FOR DEMOCRACY & TECHNOLOGY

APPENDIX 1: TABLE OF CFAA OFFENSES

Offense	Section	Sentence
Knowingly accessing and willfully communicating or retaining national defense information (with reason to know it could harm U.S.)	(a)(1)	Max 10 (1st), Max 20 (w/ prior conviction)
Intentionally accessing information from a financial institution, credit card issuer, or credit agency	(a)(2)(A)	Max 1 (1st), Max 5 (for special (a)(2)), Max 10 (w/ prior)
Intentionally accessing information of the U.S. government	(a)(2)(B)	Same
Intentionally accessing information from "any protected computer"[149]	(a)(2)(C)	Same
Intentionally accessing a nonpublic computer of the U.S. government	(a)(3)	Max 1 (1st), Max 10 (w/ prior)
Using a computer to commit fraud (unless the thing obtained is just the use of the computer and the value of that use is less than $5000)	(a)(4)	Max 5 (1st), Max 10 (w/ prior)
Causing damage intentionally (subparagraph (A)), recklessly (B), or, irrespective of intent or recklessness, if causes damage *and* loss (C)	(a)(5)(A)-(C)	Ranges from 5 to life, depending on aggravating factors[150]

[149] As noted in the body of the paper, while the CFAA, when passed, only applied to certain sensitive computers, the definition of "protected computers," as expanded over the years, effectively applies to any computer or device that is connected to the internet. Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1568 (2010).

[150] Paragraph (a)(5) is one of the more complicated, and one of the more important, CFAA provisions. It has a range of penalties. Intentional damage under Subparagraph (a)(5)(A), without a prior conviction, carries a maximum 10-year sentence if it results in, for instance, modification or

Trafficking in a password or access restriction with intent to defraud	(a)(6)	Max 1 (1st), Max 10 (w/ prior)
Extorting money or anything of value through threats to computers	(a)(7)	Max 5 (1st or attempt), Max 10 (w/ prior)

impairment of medical services, threat to public safety, or damage to 10 or more protected computers in any one-year period. Reckless damage under Subparagraph (a)(5)(B) carries a maximum five-year sentence, without a prior conviction, if it causes the same types of damage. With a prior conviction, the maximum sentence under both provisions is 20 years. An offense that results in physical injury under either provision carries a 20-year sentence, or life if it results in death. Damage or loss under Subparagraph (a)(5)(C) carries a maximum one-year sentence without a prior conviction, and a maximum 10-year sentence with a prior.