Hacktivism—Political Dissent in the Final Frontier

TIFFANY MARIE KNAPP*

ABSTRACT

Hacktivism is the next iteration of civil disobedience, a time honored tradition in our democracy. Civil disobedience, while subversive and illegal, is a means of engaging in political debate and expressing social and political thought. Therefore, as it has been in the past, civil disobedience should continue to be fostered as our society moves into the digital frontier. To do this, we need to reform the Computer Fraud and Abuse Act to take into consideration the motives behind an attack and make the sentences fit the crimes actually committed. Hacktivism, as ordinary civil disobedience, produces real benefits around the world. The current statutory framework overcharges acts of hacking, allows prosecutors to mold pleadings to stack charges and transform misdemeanors into felonies, and ultimately discourages electronic disobedience as a whole. The CFAA should have provisions regarding intent, remove duplicative provisions, and make non-serious first time offenses misdemeanors, so that hacktivism, while still illegal, is not punished more severely than other forms of civil disobedience simply because it takes place in the digital world.

* Candidate for Juris Doctor, New England Law | Boston (2015). B.S., *summa cum laude*, Mathematics and Computer Science, The College of Saint Rose (2012). I would like to thank my family for supporting me in all that I do and always assuring me of my capability to succeed, and my friends for helping me to always move forward. I would also like to thank the entire staff of the *Law Review* for all of their hard work and effort.

INTRODUCTION

In 2004, before the annual Def Con hacking conference, Jeremy Hammond ("Hammond") aptly described the potential for computer hacking as a legitimate means of electronic civil disobedience: "[H]acking is a tool. It is a means to an end .... [H]acking could be used ... as a means of fighting for social justice by putting direct pressure on politicians and institutions. It is a legitimate act of online protest."[1] More commonly referred to as "hacktivism" or "hactivism," this burgeoning form of electronic protest is a means for those with well-developed technological skill sets to advocate for political and social change in a different forum—the Internet.[2] It seems only natural that as our world moves further into the digital realm, social and political activism will follow.[3]

The law, however, has not viewed politically or socially motivated hacking favorably.[4] In January 2013, these issues were brought into the spotlight when Aaron Swartz ("Swartz"), a talented programmer and Internet activist, committed suicide while under the pressure of felony charges for *downloading* (not distributing) millions of scholarly articles from JSTOR,[5] possibly in an attempt to open access to publicly-funded research.[6] Though many argued that Swartz was unfairly prosecuted, the charges

---

[1] theprez98, *Electronic Civil Disobedience and the Republican National Convention*, YOUTUBE (Sept. 7, 2012), http://www.youtube.com/watch?v=XvXk5xCM6PM?t=34s (showing Hammond's filmed speech at the 2004 DefCon); *see also* Joshua Kopstein, *Hacker With a Cause*, NEW YORKER (Nov. 21, 2013), http://www.newyorker.com/online/blogs/elements/2013/11/jeremy-hammond-and-anonymous-hacker-with-a-cause.html.

[2] *See WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, ECONOMIST (Dec. 18, 2010), http://www.economist.com/node/17732839 (discussing the difference between traditional methods of civil disobedience and those undertaken by hacktivists).

[3] *See infra* notes 233–37 and accompanying text.

[4] *See* Kopstein, *supra* note 1.

[5] Paul Wagenseil, *How Computer Hacking Laws Make You a Criminal*, FOXNEWS (Jan. 17, 2013), http://www.foxnews.com/tech/2013/01/17/how-computer-hacking-laws-make-criminal/. Most of the articles that he downloaded, however, were in the public domain. *Id.*

[6] Gerry Smith, *The Year Hacktivists and the Government Went to War*, HUFFINGTON POST (Dec. 20, 2013, 7:34 AM), http://www.huffingtonpost.com/2013/12/20/hacktivists-government_n_4460489.html. It is important to note, however, that this intent was never express; the prosecution inferred it from a document Swartz posted online years prior entitled "Guerilla Open Access Manifesto." *See* Ryan J. Reilly, *Aaron Swartz Prosecutors Weighed 'Guerilla' Manifesto, Justice Official Tells Congressional Committee*, HUFFINGTON POST (Feb. 22, 2013, 12:01 AM), http://www.huffingtonpost.com/2013/02/22/aaron-swartz-prosecutors_n_2735675.html.

against him were valid under the existing statutory framework.[7] Such prosecution is hardly uncommon: In March 2013, Andrew Auernheimer ("Auernheimer") was sentenced to three years in prison for sharing a security problem in AT&T's servers with a journalist in an apparent attempt to protect consumers from identity theft.[8] In November, Hammond was sentenced to ten years in prison for a string of computer crimes, including leaking internal emails of Strategic Forecasting, Inc. ("Stratfor") to Wikileaks, which revealed surveillance of political groups in the United States and abroad; the Occupy Wall Street movement; and various protest activists.[9] These prosecutions are just the famous or noteworthy cases, whose sentences drew criticism from within the legal community.[10] However, the motivations of these and other hackers have not been considered by the courts, despite producing "tangible effects,"[11] including the prosecution of rapists[12] and the overthrow of repressive regimes abroad.[13]

This Note argues that the current legal framework under which hacktivism is prosecuted needs to be reformed to account for hacktivism so that civil disobedience of a different skill set is not unfairly punished. Part I of this Note will outline a brief history of hacktivism and its benefits in a modern, increasingly technological democracy. Part II explains the provisions of the Computer Fraud and Abuse Act ("CFAA") and the sentencing guidelines used in prosecution under the CFAA. Part III discusses the problems that arise under the current framework for prosecuting hacktivism, including excessive punishment, discouraging electronic civil disobedience, and the prosecutor's power to shape punishment. This section also discusses well-known prosecutions, the acts of hacking involved in those prosecutions, and the charges in those cases. Part IV proposes reforms to the CFAA so that acts of political or social

---

[7] Orin Kerr, *The Criminal Charges Against Aaron Swartz (Part 1: The Law)*, VOLOKH CONSPIRACY (Jan. 14, 2013, 2:50 AM), http://www.volokh.com/2013/01/14/aaron-swartz-charges/.

[8] Smith, *supra* note 6.

[9] Kopstein, *supra* note 1.

[10] *See* Ken White, *Three Things You May Not Get About the Aaron Swartz Case*, POPEHAT (Mar. 24, 2013), http://www.popehat.com/2013/03/24/three-things-you-may-not-get-about-the-aaron-swartz-case/ (discussing how Swartz's prosecution was not unusual, in either severity or kind, but that it obtained attention because he had been a fourteen-year-old prodigy).

[11] Smith, *supra* note 6.

[12] *See* David Kushner, *Anonymous v. Steubenville*, ROLLING STONE (Nov. 27, 2013, 3:25 PM), http://www.rollingstone.com/culture/news/anonymous-vs-steubenville-20131127.

[13] *See We Are Legion: The Story of the Hacktivists (Full Movie)*, YOUTUBE (Nov. 9, 2012), http://www.youtube.com/watch?v=lSqurTMe7Rw (showing Brian Knappenberger's full movie posted on YouTube) [hereinafter *We Are Legion*].

protest are not unjustly punished simply because they take place on the Internet rather than on a street.

I. Background

Although use of the term in media is varied, "hacktivism" generally refers to the nonviolent use of computer skills (or "digital tools") for political purposes.[14] The methods hacktivists use to support their various causes are often violations of federal law and can result in felony charges.[15] For example, a common hacktivist tactic is the Distributed Denial of Service ("DDoS") attack, which is commonly prosecuted as a felony under the CFAA.[16] Hacktivists are treated harshly within the criminal justice system because the technology they use is generally misunderstood.[17] One famous hacker was granted supervised release from prison on the condition he not use encryption.[18] Though seemingly benign to those less technologically inclined, this condition has been described as "show[ing] a fundamental misunderstanding of how the Internet works."[19] This is because encryption is no longer a tool of the computer savvy; rather, using

---

[14] Noah C.N. Hampson, *Hacktivism: A New Breed of Protest in a Networked World*, 35 B.C. INT'L & COMP. L. REV. 511, 514–15 (2012).

[15] Christie Thompson, *Hacktivism: Civil Disobedience or Cyber Crime?*, PROPUBLICA (Jan. 18, 2013, 11:20 AM), http://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime.

[16] *See infra* notes 68–75, 212 and accompanying text. These attacks use a network of computers to flood a server with requests for a webpage, thus causing legitimate requests for the webpage to go unanswered and essentially make the webpage unavailable. Thompson, *supra* note 15. Software and Internet tools are utilized, which allow even non-technical users to participate in the attack. *See* Francois Paget, *Hacktivism: Cyberspace Has Become The New Medium For Political Voices*, MCAFEE LABS 23 (2012), http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf.

[17] *See, e.g.*, Jaikumar Vijayan, *Court Confiscates Computer for Owner's Claim of Hacking*, PCWORLD (Oct. 26, 2013, 9:45 AM), www.pcworld.com/article/2058289/court-confiscates-computer-for-owners-claim-of-hacking.html (explaining the U.S. District Court judge who "issued the ruling . . . acknowledged it was 'very rare' and 'extraordinary'" but necessary because the defendants were "hackers"); Vivien Lesnik Weisman, *A Conversation With Jeremy Hammond, American Political Prisoner Sentenced to 10 Years*, HUFFINGTON POST (last updated Jan. 23, 2014, 6:58 PM), http://www.huffingtonpost.com/vivien-lesnik-weisman/jeremy-hammond-q-and-a_b_4298969.html (describing a condition of Hammond's supervised release prohibiting him from using encryption as "show[ing] a fundamental misunderstanding of how the Internet works"); Theresa Züger, *Re-thinking Civil Disobedience*, INTERNET POL'Y REV. (Nov. 11, 2013), http://policyreview.info/articles/analysis/re-thinking-civil-disobedience ("The reality is that the disobedient are treated as plain criminals, even more if the disobedience focusses on the internet.").

[18] Weisman, *supra* note 17.

[19] *Id.*

the Internet essentially requires using encryption.[20] Despite these misunderstandings and the illegality of hacking, there are benefits to hacktivism in a digital world—not all those who break the law are necessarily working against the common good.[21]

A. *Parsing "Hacktivism"*

Broadly, "hacktivism combines the transgressive politics of civil disobedience with the technologies and techniques of computer hackers."[22] In recent years, there has been movement towards defining hacktivists as people to be feared rather than political or social protesters.[23] Because hacktivists are a large, faceless group with many different motivations, it is difficult to define them based on one shared ideology.[24] However, a uniting feature has been a dedication to freedom of information, particularly on the Internet.[25]

Focusing on political dissent or a social cause differentiates hacktivism from what is more broadly denoted as hacking—*hacktivists* do not engage in criminal activity for personal gain, while *hackers* generally intend to profit off their endeavors.[26] Hacktivists, however, focus on bringing attention to a political or social cause or generally voicing dissent.[27] Hacktivist activities include the public release of private documents in order to spread information they believe the public has a right to know or

---

[20] *See* Charles Arthur, *How Internet Encryption Works*, GUARDIAN (Sept. 5, 2013, 3:19 PM), http://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works.

[21] *See infra* Part I.B.

[22] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation, at 1–2 (Sept. 2004) (unpublished Ph.D. dissertation, Harvard University), *available at* http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

[23] *See* Peter Ludlow, *What Is a 'Hacktivist'?*, N.Y. TIMES (Jan. 13, 2013, 8:30 PM), http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?_php=true&_type=blogs&_r=0 (discussing efforts to paint hacktivists in a negative light and the efforts of hackers to combat this fear and negative imagery) [hereinafter Ludlow, *What Is a 'Hacktivist'?*].

[24] *See* Pierluigi Paganini, *Hacktivism: Means and Motivations . . . What Else?*, INFO SEC INST. (Oct. 2, 2013), http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/ ("Trying to frame a wide range of currents of thought with a single term is a limiting approach; in fact, each group is characterized by different ways of hacking, different motivations, and different means used.").

[25] Ty McCormick, *Hacktivism: A Short History*, FOREIGN POL'Y (Apr. 29, 2013), http://www.foreignpolicy.com/articles/2013/04/29/hacktivism.

[26] Hampson, *supra* note 14, at 515–17 (describing the distinction between hacktivism and hacking, which the author uses to denote those who hack for personal gain). There are multiple kinds of hackers, the variations of which are beyond the scope of this Note.

[27] Paganini, *supra* note 24.

to reveal suspicious, possibly illegal activities of governmental agencies.[28] Such exposure involves public accountability, and does not generate income to the person or group releasing the documents.[29] Hacktivists also hack into websites to take down "destructive" messages,[30] personal accounts to reveal evidence of criminal activity,[31] and even to help legitimate public protests against governments in the United States and abroad.[32] On the other hand, "black hat hackers," or those hackers most commonly portrayed in the media, seek information which could bring them a profit—credit card numbers they subsequently use or sell, personal information with which they can extort the owner, or access to personal accounts they can drain.[33]

Another important, though subtle distinction, is between hacktivism and cyberterrorism.[34] Unlike hacktivism, cyberterrorism seeks to coerce a government or the public at large to take particular actions through fear or the potential damage an attack can cause.[35] The goal of hacktivism, however, is not to cause serious damage, but to make a statement or draw

---

[28] *See, e.g.*, Kopstein, *supra* note 1; Peter Ludlow, *The Strange Case of Barrett Brown*, NATION (June 18, 2013), http://www.thenation.com/article/174851/strange-case-barrett-brown# [hereinafter Ludlow, *Barrett Brown*]; Michael Scherer, *Snowden, Manning and the New Generation of Hacktivists*, TIME, http://content.time.com/time/video/player/0,32068,2475814736001_2145538,00.html (last visited Apr. 13, 2015).

[29] *See, e.g.*, Ludlow, *Barrett Brown*, *supra* note 28. Brown was in the process of investigating a systemic issue in the security contracting industry when he was prosecuted: "It was clear to Brown that these were actions of questionable legality, but beyond that, government contractors were attempting to undermine Americans' free speech—with the apparent blessing of the DOJ." *Id.* Brown, as a journalist, sought information for journalistic reasons, not to profit from what he might learn (for example, he never sought to sell the information Hammond gave to him, only to create a story he could later publish). *See id.*

[30] *See, e.g.*, David Pakman Show, *Anonymous Hacks Westboro Baptist Church LIVE*, YOUTUBE (Feb. 24, 2011), http://www.youtube.com/watch?v=OZJwSjor4hM (broadcasting a member of Anonymous hacking Westboro Baptist Church website while on radio show with one of the Church's members).

[31] *See* Kushner, *supra* note 12.

[32] *We Are Legion*, *supra* note 13 (describing assistance given to protests in Libya, Egypt, and the Occupy Wall Street movement in the United States).

[33] *See* Chris Hoffman, *Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats*, HOW-TO GEEK (Apr. 20, 2013), http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/.

[34] DOROTHY E. DENNING, ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY, *reprinted in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY 239, 241 (2001), *available at* http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.

[35] *See The Difference Between Hacktivism and Cyber Terrorism*, INFOBARREL (Dec. 18, 2009), http://www.infobarrel.com/The_Difference_Between_Hacktivism_and_Cyberterrorism.

attention to a concept.[36] This distinction is similar to the distinction between ordinary civil disobedience and acts of "civil unrest" or domestic terrorism in the Unites States or abroad.[37]

Recently, the hacker collective Anonymous has become the most visible group associated with hacktivist activities, such as: combating rapists, Mexican drug cartels, American law enforcement, and oppressive foreign regimes.[38] Due to its meritocracy-like structure, Anonymous has no set organization or leader, allowing it to pursue a variety of causes without a public "face."[39] Individuals can also be associated with hacktivist activities, though this is usually due to subsequent prosecution for their involvement rather than voluntarily linking their name with their actions.[40] For example, Hammond was sentenced to the ten-year maximum under a plea agreement for his involvement in Anonymous' hacking and destruction of Stratfor servers and the subsequent dissemination of the information acquired.[41] Additionally, late Internet activist Swartz acted in his own capacity, unassociated with a larger organization.[42]

B. *Controversial Benefits*

Hacktivism may be controversial, but some argue it is a beneficial means of protest.[43] Security strategist Joshua Corman stated: "individual, young, nameless, faceless folks are having geopolitical impact. It's both

---

[36] DENNING, *supra* note 34.

[37] *Compare Domestic Terrorism: The Benefits of Hindsight*, ECONOMIST (Aug. 18, 2012), http://www.economist.com/node/21560566 (describing domestic terrorism in the U.S., the causes of which range from the first black, U.S. president and gun laws), *with infra* note 234 and accompanying text. The purpose of the violence in domestic terrorism, then, is to attract attention and fear to "the cause." *See* ECONOMIST, *supra*.

[38] *See* Quinn Norton, *Anonymous 101: Introduction to the Lulz*, WIRED (Nov. 8, 2011, 5:30 AM), http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1.

[39] *CNN Presents: Amber Lyon Profiles Anonymous*, YOUTUBE (Jan. 14, 2012), http://www.youtube.com/watch?v=pj-Sp_GNMg4 [hereinafter *CNN Presents*].

[40] *See* Somini Sengupta, *The Soul of the New Hacktivist*, N.Y. TIMES (Mar. 17, 2012), http://www.nytimes.com/2012/03/18/sunday-review/the-soul-of-the-new-hacktivist.html ("Those who affiliate with the movement use a variety of tools to cloak their identities and the devices on which they work. They rarely know one another's offline identities.").

[41] Kopstein, *supra* note 1.

[42] *See* Indictment at 3–9, United States v. Swartz, No. 11-cr-10260 (2011), http://www.documentcloud.org/documents/217117-united-states-of-america-v-aaron-swartz.

[43] *See* GABRIELLA COLEMAN, CTR. FOR INT'L GOVERNANCE INNOVATION, ANONYMOUS IN CONTEXT: THE POLITICS AND POWER BEHIND THE MASK 17–18, (2013) *available at* http://www.cigionline.org/publications/2013/9/anonymous-context-politics-and-power-behind-mask ("Dissent of the sort Anonymous specializes in allows citizens to exercise their rights and demonstrate on behalf of the causes they embrace.").

exhilarating to realize that and terrifying to realize that. It kind of depends on how that power is wielded."[44] Discourse about hacking and hacktivism in popular media often overlooks potential social benefits.[45] Hacktivists have produced real, tangible results in recent years that have led to political discourse, justice for wronged parties, and even the ousting of repressive regimes abroad.[46] However positive these results may be, the methods used to achieve them, and sometimes the results themselves, are frequently opposed.[47]

During the Arab Spring, Anonymous helped Tunisians fight their repressive government by taking down government-run websites, combating government theft of citizens' passwords, and bringing media attention to the conflict.[48] In Egypt, members of Anonymous used Twitter accounts to deliver messages after Egyptians lost Internet access.[49] Additionally, Anonymous helped Egyptians avoid detection and subvert the government—digitally and on the ground—after it shut off the Internet.[50] Anonymous members helped Egyptians obtain Internet connections during the blackout, which in turn helped both the spread and success of protests.[51] Egyptians' Internet access was crucial, as Twitter and other social media have contributed to the success of Egyptian protests.[52]

Anonymous also participates in political protest in the United States, such as publicizing the Occupy Wall Street Movement.[53] They served as an impromptu "public relations weapon"—placing citizen journalists on the

---

[44] *We Are Legion*, *supra* note 13.

[45] *See generally* Ludlow, *What Is a 'Hacktivist'?*, *supra* note 23 ("[T]here has been an effort to tarnish the hacktivist label so that anyone who chooses to label themselves as such does so at their peril.").

[46] Quinn Norton, *How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down*, WIRED (July 3, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/.

[47] *See, e.g.*, Jay Weiser, *Aaron Swartz: A Tragic Suicide, But His 'Hacktivism' Actually Hurt the Goals He Claimed to Promote*, AM. ENTERPRISE INST. IDEAS (Jan. 15, 2013, 11:23 AM), http://www.aei-ideas.org/2013/01/aaron-swartz-a-tragic-suicide-but-his-hacktivism-actually-hurt-the-goals-he-claimed-to-promote/ (arguing that Swartz's actions hurt, rather than furthered, his overarching purpose).

[48] *See CNN Presents*, *supra* note 39.

[49] *We Are Legion*, *supra* note 13.

[50] *See id.*

[51] *Id.*

[52] *See* P.N. Howard et al., *Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?* 2 (Project on Info. Tech. & Political Islam, Working Paper No. 2011.1, 2011) ("Social media played a central role in shaping political debates in the Arab Spring."), *available at* http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

[53] *CNN Presents*, *supra* note 39.

streets to document potential police misconduct, then "doxing" the police officers filmed.[54] Perhaps most famously, Anonymous placed a video clip online featuring a University of California Davis police officer pepper spraying peacefully protesting students.[55] Anonymous effectively structured the narrative of the Occupy Movement by publicizing acts of police brutality and amplifying the message of protesters in the process.[56]

Other acts of hacktivism are arguably more detrimental to society, even though those performing them claim to do so for public benefit.[57] This category of hacktivism commonly revolves around the theft and subsequent public release of private or secure documents, such as government communications.[58] Hammond, for example, hacked into Stratfor's database and stole internal emails and client account information, some of which was later released.[59] Stratfor, an "intelligence contractor," was targeted because the firm had previously targeted Anonymous' operation against the Mexican drug cartels.[60] Hammond also wished to reveal particular spying operations in which Stratfor was engaged.[61] The leaked information showed that Stratfor was spying on members of the Occupy Wall Street Movement, Anonymous, and WikiLeaks, as well as taking actions in opposition to WikiLeaks.[62] In this way, Hammond achieved one of his goals and arguably did a public service.[63] However, the government classified him as essentially nothing more than a miscreant causing havoc: "While he billed himself as fighting for an anarchist cause, in reality, Hammond caused personal and financial chaos for individuals

---

[54] *Id.* "Doxing" involves acquiring the private information of the target (individual or company) and publishing or distributing it. Thompson, *supra* note 15.

[55] *CNN Presents*, *supra* note 39.

[56] *Id.*

[57] *See Sentenced to 10 Years in Prison, Jeremy Hammond Uses Allocution to Give Consequential Statement Highlighting Global Criminal Exploits by FBI Handlers*, SPARROW PROJECT (Nov. 15, 2013, 12:01 PM) http://www.sparrowmedia.net/2013/11/jeremy-hammond-sentence/ (arguing in his allocution, Hammond stated that his acts, though detrimental to some, were done in protest and for the betterment of society at large).

[58] *See, e.g.*, The Stream Team, *'Hacktivist' Pioneers [Infographic]*, AL JAZEERA AM. (Nov. 12, 2013), http://america.aljazeera.com/watch/shows/the-stream/multimedia/2013/11/-hacktivist-pioneersinfographic.html (depicting hacktivist activities that have "pushed the boundaries" of hacktivism as a legitimate form of protest—all those acts depicted are document leaks/thefts).

[59] Matt Sledge & Alyona Minkovski, *Jeremy Hammond Sentenced To 10 Years In Prison*, HUFFINGTON POST (Nov. 15, 2013, 12:23 PM), http://www.huffingtonpost.com/2013/11/15/jeremy-hammond-sentenced_n_4280738.html.

[60] Weisman, *supra* note 17.

[61] *Id.*

[62] *Id.*

[63] *Id.*

whose identities and money he took and for companies whose businesses he decided he didn't like."[64] It is important to note, however, that although credit card information was stolen and used to make $700,000 in fraudulent charges to charitable organizations, none of the intended recipients actually received the money.[65] In other words, no actual financial harm was realized.[66]

Another controversial tactic hacktivists deploy is the DDoS attack.[67] These attacks are frequently used in announced, organized protests,[68] but they still interfere with public access to websites.[69] The fear is that if these attacks were deployed against a server or website considered publically crucial, the effects could be devastating.[70] However, hacktivists, unlike cyberterrorists, do not seek to maximize harm caused to their target or the public at large.[71] Rather, their tactics are focused on making a point.[72] Subsequently, DDoS attacks and targets are usually announced before they occur and are accompanied by a statement explaining the reason behind the attack.[73] Although the attacks can be a nuisance, they are no more disruptive than traditional passive sit-ins.[74] Generally, they are also effective at achieving results and drawing attention to a cause.[75]

---

[64] Sledge & Minkovski, *supra* note 59.

[65] Kopstein, *supra* note 1.

[66] *Id.*

[67] *See infra* notes 68–75 and accompanying text.

[68] *See, e.g.*, Tracy Kitten, *DDoS: Attackers Announce Phase 4: Cyber Fighters Say New Strikes Will Be 'Different'*, BANK INFO SECURITY (July 23, 2013), http://www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1 (discussing the announcement of a fourth wave of attacks on US banks by a hacktivist group).

[69] Thompson, *supra* note 15.

[70] *See* Mathias Klang, *Civil Disobedience Online*, J. INFO., COMM., & ETHICS IN SOC'Y, no. 2, 2004 at 75, 81, *available at* http://www.digital-rights.net/wp-content/uploads/2008/01/klang_ices_disobedience.pdf ("Personal violence or physical harm can be caused if, for example, a user is dependent upon a website for information however, to this author's knowledge; [sic] no such cases have been reported.").

[71] *See* DENNING, *supra* note 34; *The Difference Between Hacktivism and Cyber Terrorism*, *supra* note 35.

[72] *See* DENNING, *supra* note 34, at 241–42.

[73] *See, e.g.*, Kitten, *supra* note 68.

[74] *See* Klang, *supra* note 70, at 82.

[75] *We Are Legion*, *supra* note 13 ("Cyber protest, sit-ins, however you want to look at it, DDoS is a tool that is like driving a finish nail in with a sledge hammer.").

II. Hacktivism Prosecution Under the Computer Fraud and Abuse Act

> "The Computer Fraud and Abuse Act is the most outrageous criminal law you've never heard of. . . . It is, in short, a nightmare for a country that calls itself free."[76]

Before considering how hacktivists are prosecuted under the CFAA,[77] it is noteworthy that the CFAA was introduced shortly after the movie *War Games* was released.[78] The film, about a teen who accidentally comes close to starting a nuclear war, sparked fear in Americans who were unfamiliar with computer technology (*i.e.*, most legislators), and placed a narrative in popular culture about the power of computers, as well as the irresponsibility of the young persons wielding it.[79] The House Report supporting the CFAA specifically discussed the movie, referencing it as a "realistic representation" of the capabilities of personal computers and, therefore, of the security risks they posed.[80] But the report made only vague reference to computer functions and did not indicate how they could threaten national security (or cause nuclear war).[81] Nevertheless, there were legitimate reasons for passing the law: the House Report also referenced annual losses caused to businesses because of computer crime.[82] However, significantly more time was devoted to expounding on the dangers of personal computer proliferation.[83] Such fear mongering has only escalated since the CFAA was enacted.[84]

Despite being mostly the product of fear, the CFAA continues to be the go-to law for prosecuting hacking crimes at the federal level.[85] Initially passed in 1984, the CFAA has since been amended nine times.[86] Each

---

[76] Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html.

[77] 18 U.S.C. § 1030 (2012); The Consumer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986).

[78] Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 596–97 (1997).

[79] *Id.*

[80] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696.

[81] Olivenbaum, *supra* note 78, at 597.

[82] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695.

[83] *See, e.g., id.* at 3696–97 (discussing how the spread of personal computer use increased the "hacker problem").

[84] *See, e.g., Blackhat – Official Trailer (Universal Pictures HD)*, YOUTUBE (Sept. 25, 2014), http://www.youtube.com/watch?v=Q1HO07bKGhU

[85] Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 978 (2008).

[86] Reid Skibell, Article, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud*

amendment has broadened the statute, and some have even increased punishment for particular violations.[87] Many of these amendments were made "in response to changes in technology and Congressional perception of what constitutes a crime, without any apparent understanding of how the changes will impact the law as a whole."[88] Similarly, more recent proposed amendments are also based in fear: those who want to strengthen the Act argue that it "should be strengthened to reflect the increased threat of international computer hackers."[89] However, until very recently, the CFAA had *never* been used to prosecute a foreign hacker—it had only been used against American citizens.[90] Additionally, there are strong arguments that increasing penalties under the CFAA will not reduce foreign threats.[91]

A. *Provisions of the CFAA*

The CFAA creates seven categories of computer crime.[92] The statute also proscribes conspiracy and attempt to commit the seven outlined crimes.[93]

Section 1030(a)(1) deals specifically with obtaining national security information.[94] As such, it is infrequently used.[95] This section makes it a felony to obtain national security information either without authorization or in excess of granted authorization, and to then provide or attempt to

---

and Abuse Act, 18 BERKELEY TECH. L. J. 909, 912 (2003).

[87] *See generally id.* (describing the evolution of computer fraud and The Computer Fraud and Abuse Act of 1986).

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

[89] *Id.*

[90] *See* David Kravets, *Indicted: China's Army Hacked Into U.S. Companies, Stole Trade Secrets*, ARS TECHNICA (May 19, 2014, 11:32 AM), http://arstechnica.com/tech-policy/2014/05/indicted-chinas-army-hacked-into-us-companies-stole-trade-secrets/ ("Legal experts said this was a precedent-setting case, the first time the US levied hacking charges (some the same as those brought against the late Swartz) against a foreign government.").

[91] *See* Mark Jaycox, *Increasing CFAA Penalties Won't Deter Foreign "Cybersecurity" Threats*, ELECTRONIC FRONTIER FOUND. (Apr. 11, 2013), https://www.eff.org/deeplinks/2013/04/increasing-cfaa-penalties-wont-deter-foreign-cybersecurity-threats.

[92] H. MARSHALL JARRETT ET AL., EXEC. OFFICE FOR UNITED STATES ATTORNEYS, PROSECUTING COMPUTER CRIMES 3, *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited Apr. 13, 2015).

[93] *Id.*

[94] 18 U.S.C. § 1030(a)(1) (2012).

[95] JARRETT ET AL., *supra* note 92, at 12.

provide that information to another source.[96] Simply "willfully retaining the information" is also a violation of this provision.[97]

Section 1030(a)(2) has three subparts that define three overlapping crimes.[98] Any violation of this provision is a misdemeanor unless aggravating factors are proven.[99] It is a violation to intentionally access a computer without authorization, or in excess of granted authorization, and obtain information: (1) in financial records of a financial institution, card issuer (defined in 15 U.S.C. § 1602(n)), or from files of a consumer reporting agency; (2) from any U.S. department or agency; or (3) from any protected computer.[100] A violation under one subsection may violate another subsection, allowing for multiple charges.[101] Simply reading information meets the definition of "obtaining" under this provision.[102] Further, "protected computer," under subsection (3) and later sections, has been broadly interpreted, which also allows for more actions to be charged.[103]

Section 1030(a)(3) prohibits trespass into government computers, regardless of whether information is obtained.[104] This provision does not apply to federal employees, meaning federal employees who violate their authorization are subject to administrative sanctions rather than criminal prosecution.[105] Section 1030(a)(4) criminalizes using a computer without authorization or in excess of granted authorization with the intent to defraud, if the use of the computer furthers the fraud.[106] If the goal of the fraud is more than using the computer itself (meaning the person is using the computer to further a different criminal purpose beyond access to the information on the computer), using a computer to commit fraud would violate this provision; if the computer use itself is the object of the fraud, the value of the use must be more than $5,000 in any one-year period.[107]

---

[96] *Id.*

[97] *Id.*

[98] *Id.* at 16.

[99] *Id.*

[100] 18 U.S.C. § 1030(a)(2) (2012).

[101] JARRETT ET AL., *supra* note 92, at 17.

[102] RALPH D. CLIFFORD, CYBERCRIME: THE INVESTIGATION, PROSECUTION AND DEFENSE OF A COMPUTER-RELATED CRIME 195 (2d ed. 2006).

[103] *See* JARRETT ET AL., *supra* note 92, at 4 ("[I]t is enough that the computer is connected to the Internet; the statute does not require proof that the defendant also used the Internet to access the computer or used the computer to access the Internet.").

[104] *See* § 1030(a)(3).

[105] *See* JARRETT ET AL., *supra* note 92, at 23.

[106] § 1030(a)(4).

[107] *Id.*

Section 1030(a)(5) was written specifically to criminalize hacking.[108] There are two articulated offenses under this provision: (1) *knowingly* transmitting a code or program that *intentionally* causes damage to a "protected computer" (it does not matter whether or not the user has authorized access); and (2) unauthorized access of a protected computer that causes damage (regardless of intent).[109] The first subsection requires intent and unauthorized access; the second requires unauthorized access, but damage caused can be accidental.[110] Again, "protected computer" is broadly interpreted, so this places little restraint on which actions can be charged under this provision.[111]

Section 1030(a)(6) prohibits password trafficking with the intent to defraud.[112] This provision is fairly narrow and is limited to password trafficking that (1) allows unauthorized access; (2) affects interstate or foreign commerce; and (3) compromises computers used by or for the U.S. government.[113] Finally, § 1030(a)(7) criminalizes extortion using a computer.[114]

B. *Sentencing under the CFAA*

The CFAA also contains provisions outlining the punishment for violating each section of the Act.[115] In addition to these penalties, courts look to the Sentencing Guidelines ("Guidelines") when making decisions, as the Supreme Court has stated that consulting the Guidelines is mandatory (though the Guidelines themselves are advisory).[116] However, the Guidelines take very little information into consideration: the defendant's previous record and the "severity" of the crime.[117] Further, though the Guidelines are supposed to reflect "empirical data and national experience,"[118] Congress can and has explicitly directed the U.S. Sentencing Commission to heighten suggested sentences in conjunction with

---

[108] Hampson, *supra* note 14, at 525.

[109] § 1030(a)(5).

[110] *See id.*; Hampson, *supra* note 14, at 525–26.

[111] *See supra* note 103 and accompanying text.

[112] Hampson, *supra* note 14, at 526.

[113] *Id.*

[114] § 1030(a)(7).

[115] *See* §§ 1030(b)–(c).

[116] *See* United States v. Booker, 543 U.S. 220, 233 (2005); Hanni Fakhoury, *How the Sentencing Guidelines Work Against Defendants in CFAA Cases*, ELECTRONIC FRONTIER FOUND. (Apr. 9, 2013), https://www.eff.org/deeplinks/2013/03/41-months-weev-understanding-how-sentencing-guidelines-work-cfaa-cases-0.

[117] Fakhoury, *supra* note 116.

[118] *Id.*

congressional maximums.[119] This makes sentencing less a reflection of data or national experience, as it is supposed to be, and more a reflection of congressional attitudes toward crime.[120] In particular, these sentences reflect the fear behind the technology used to commit the crimes.[121]

On its face, the CFAA appears more lenient than it is in practice because many of the crimes are initially defined as misdemeanors.[122] However, two out of the four misdemeanor provisions contain aggravating factors that, if present, transform the crime into a felony, such as § 1030(a)(2) (access of a computer and obtaining information).[123] The aggravating factors for § 1030(a)(2) are if: (1) the crime was committed for commercial advantage or private financial gain; (2) the crime was committed to further any other crime or tort; and (3) the value of the information obtained exceeds $5,000.[124] Section 1030(a)(5) shares this last element.[125]

Under the CFAA's aggravating factors, the $5,000 loss element is the most controversial.[126] It is also the most commonly charged sentence enhancement by prosecutors.[127] This is because the statute defines loss very broadly: "*any* reasonable cost to *any* victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and *any* revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[128] Currently, prosecutors can calculate damages in a variety of ways, including the prorated salaries of those who restore data or check databases to make sure the information is the same, as well as the cost of reinstalling software or

---

[119] *See* Identity Theft Enforcement and Restitution Act, Pub. L. No. 110-326, 122 Stat. 3560, 3564 (2008).

> The United States Sentencing Commission shall review its guide lines and policy statements . . . under section[] . . . 1030 . . . of title 18, United States Code . . . in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guide-lines and policy statements.

Id.; Fakhoury, *supra* note 116.

[120] *See* Fakhoury, *supra* note 116.

[121] *Cf.* Olivenbaum, *supra* note 78 (explaining that an introductory force behind the CFAA was fear created by the movie *War Games*).

[122] *See* 18 U.S.C. § 1030(b)–(c) (2012) (providing penalties for violations of the crimes in (a)).

[123] *See* §§ 1030(c)(2), (c)(4); *see also* JARRETT ET AL., *supra* note 92, at 19–21, 47–49.

[124] *See* § 1030(c)(2)(B); *see also* JARRETT ET AL., *supra* note 92, at 19–20.

[125] *See* § 1030(a)(5); *see also* JARRETT ET AL., *supra* note 92, at 47–49.

[126] *See, e.g.*, Fakhoury, *supra* note 116.

[127] JARRETT ET AL., *supra* note 92, at 42.

[128] § 1030(e)(11) (emphasis added).

even installing *new security measures* to "resecure the computer to avoid further damage from the offender."[129] Further, advertising revenue, sales revenue, and business goodwill lost due to website outage have also been used in loss calculations.[130]

Section 2B1.1 of the Guidelines applies specifically to the CFAA, as the crimes are treated as basic economic offenses.[131] The sentencing range given is based on the crime's "offense level."[132] The starting point in calculating a defendant's offense level is the "base offense level," determined by the maximum punishment authorized.[133] The base offense level for conviction under the CFAA is level six, unless the defendant has a previous conviction under the statute for which there was a statutory maximum of twenty years or more.[134]

At this offense level, suggested sentences are fairly low (depending on previous criminal history), having a maximum suggested sentence of eighteen months.[135] However, the base offense level can be modified by aggravating factors.[136] These factors include: economic loss caused, number of victims, whether an e-mail was obtained through improper means, whether property was misappropriated, and a prior conviction under § 1030 involving intent to obtain personal information or the unauthorized public dissemination of personal information.[137] Due to these additional increases to the offense level, defendants rarely receive low suggested sentences under the Guidelines.[138]

---

[129] JARRETT ET AL., *supra* note 92, at 42–43.

[130] *Id.* at 43.

[131] *Id.* at 131.

[132] *See* U.S. SENTENCING GUIDELINES MANUAL ch. 5, pt. A, at 399–401 (2014) (sentencing table using the offense level for the y-axis and criminal history of the defendant for the x-axis).

[133] Fakhoury, *supra* note 116.

[134] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(a) (meaning that the absolute minimum offense level an offender under the CFAA can receive is level six; should the offender have a criminal record, the offense level would be higher).

[135] *Id.* ch. 5, pt. A, at 395.

[136] *See id.* § 2B1.1(b); *see also* Fakhoury, *supra* note 116.

[137] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b); *see also* Fakhoury, *supra* note 116.

[138] *See* Fakhoury, *supra* note 116.

ANALYSIS

"Whatever technical crimes the government claims have been committed must be weighed against the good that comes from lifting the veil on corporate and government spying and corruption. We should not punish the courageous people that exposed it."[139]

III. Discussion: Punishment Should Fit the Crime

The consequence of the current statutory scheme is threefold: (1) computer hackers, both activists and otherwise, receive harsher punishments than activists committing "parallel" crimes in the real world or even those committing physical, violent, more serious crimes;[140] (2) the current sentencing guidelines give prosecutors significant latitude in charging and sentencing similar crimes very differently;[141] and (3) long prison terms for acts meant to benefit society or individuals discourage hacktivists from committing acts of electronic civil disobedience that would otherwise contribute to progress in our digital, democratic society.[142]

A. *Current Punishments are More Severe than the Crimes*

In the federal criminal system, a defendant's sentence reflects the severity of the crime.[143] Federal sentencing guidelines are supposed to take into account empirical data and national perspectives regarding the crime when setting an appropriate punishment range.[144] Accordingly, if a crime regularly receives severe punishment, particularly in comparison to other

---

[139] Janet Reitman, *Jeremy Hammond: Rise and Fall of the Legendary Hacker*, ROLLING STONE, Dec. 7, 2012, at 36, *available at* http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207.

[140] *See, e.g.*, Clark Estes, *Executing Hackers Seems Pretty Extreme*, VICE (July 9, 2012), http://www.vice.com/read/sending-hackers-to-the-gallows-sounds-extreme (discussing the severity of hacking crimes to crimes of murder and rape); Dylan Taylor, *Hacker Who Helped Expose Steubenville Rapists Faces More Prison Time Than Perpetrators*, CISTERNYARD MEDIA (Jan. 16, 2014), http://site.cisternyard.com/2014/01/16/hacker-who-helped-expose-steubenville-rapists-faces-more-prison-time-than-perpetrators/.

[141] Earl J. Silbert, *Power Skews to the Prosecution under Federal Sentencing Guidelines*, 27 CRIM. JUST., Fall 2012, at 25, 26.

[142] *See* Scott Arciszewski, *Black and White: The Growing Schism Between Hackers and the Law*, 2600: HACKER Q., Winter 2013–2014, at 48–49.

[143] *See* U.S. SENTENCING COMM'N, AN OVERVIEW OF THE FEDERAL SENTENCING GUIDELINES 1, 3 ("The sentencing guidelines provide 43 levels of offense seriousness—the more serious the crime, the higher the offense level.") [hereinafter OVERVIEW], *available at* http://www.ussc.gov/sites/default/files/pdf/about/overview/Overview_Federal_Sentencing_Guidelines.pdf.

[144] *See* Fakhoury, *supra* note 116.

crimes, our society considers it a severe crime.[145] Computer crimes, specifically those categorized as hacking and prosecuted under the CFAA, are often punished similarly to "severe" crimes, such as breaking and entering, embezzlement, money laundering, assault, and some drug offenses.[146] This occurs even though most would agree that physical crimes, such as assault with attempt to murder, aggravated assault, and conspiracy to commit murder, are all more severe crimes than a simple computer intrusion.[147]

The first result of the current framework for prosecuting acts of hacktivism is that hacktivists (as well as those that hack for other reasons) are generally receiving sentences much more severe than is warranted for their actions.[148] Hacktivists' motivations are political or social[149]—things that are traditionally not severely punished under the law.[150] However, hacktivist activities usually *are* given hefty federal prison sentences, even under plea arrangements.[151]

---

[145] *See* OVERVIEW, *supra* note 143.

[146] *See, e.g.*, Wagenseil, *supra* note 5 ("Swartz was facing more prison time than he would have if he'd committed a serious physical crime, such as assault, burglary, grand theft larceny or involuntary manslaughter."). *Compare* U.S. SENTENCING COMM'N, *Sentence Length in Each Primary Offense Category*, *in* 2012 SOURCEBOOK OF FEDERAL SENTENCING STATISTICS tbl. 13 (2012), *available at* http://www.ussc.gov/Research_and_Statistics/Annual_Reports_and_Sourcebooks/2012/Table13.pdf [hereinafter *Sentence Length*] (showing average sentence for assault was 32 months), *with* Kyle, *Some Thoughts on the Computer Fraud and Abuse Act*, NONCURALEX.COM (Jan. 19, 2013), http://noncuratlex.com/?p=1243 (describing disparate sentencing outcomes in CFAA prosecutions). Ten percent of CFAA cases that received prison as a sentence received fifty-seven or more months in prison; five to twenty-four months was the prison term for many other cases. Kyle, *supra*.

[147] *Compare Sentence Length*, *supra* note 146 (showing average sentence for assault was thirty-two months), *with* Kyle, *supra* note 146 (noting disparate sentencing outcomes). The sentencing commission defines the assault category as including those crimes listed within the text. U.S. SENTENCING COMM'N, *Appendix A: Descriptions of Datafiles, Variables, and Endnotes*, *in* 2012 SOURCEBOOK OF FEDERAL SENTENCING STATISTICS 8 (2012), *available at* http://www.ussc.gov/Research_and_Statistics/Annual_Reports_and_Sourcebooks/2012/Appendix_A.pdf. Further, those in the industry and ordinary citizens are dismayed by the sentencing computer crimes receive; as one security analyst put it: "[w]hy the penalties are stiffer for e-crime does not make sense. These penalties are more in line with murder than theft." Wagenseil, *supra* note 5.

[148] *See* Hanni Fakhoury, *The U.S. Crackdown on Hackers is Our New War on Drugs*, WIRED (Jan. 23, 2014, 9:30AM), http://www.wired.com/opinion/2014/01/using-computer-drug-war-decade-dangerous-excessive-punishment-consequences/.

[149] *See* Peter Ludlow, *Hacktivists on Trial*, NATION (Dec. 4, 2013), http://www.thenation.com/article/177462/hacktivists-trial [hereinafter Ludlow, *Hacktivists on Trial*].

[150] *See infra* notes 206–22.

[151] *See* Smith, *supra* note 6.

For example, in late 2012 hacktivists exposed those who were actively covering up a rape in Steubenville, Ohio.[152] Anonymous member Deric Lostutter ("Lostutter"), outraged after hearing about the rape and cover up in a news article, led the operation by creating Anonymous subgroup KnightSec.[153] He posted a video on YouTube, which gained national attention and spurred other Anonymous members to take action.[154] The media attention and information gathering led not only to the prosecution and conviction of the rapists, but also the prosecution of four other school officials for assisting in the cover up.[155] The rapists received one- and two-year sentences, respectively.[156] However, Lostutter's residence was raided by the FBI after the sentencing.[157] Though not yet indicted, he is suspected of violating the CFAA, identity theft, and conspiracy.[158] Considering that someone else actively took credit for the charged crime, the FBI's action is even more stunning.[159] Lostutter could face twenty-five years in prison even though his admitted involvement is limited to being in the video posted on the team website when it was hacked and disseminating information that was given to him.[160]

Such sentences are not isolated.[161] Auernheimer was charged under the CFAA for obtaining information about iPad users from AT&T servers and

---

[152] Kushner, *supra* note 12.

[153] *Id.* The article itself would never have brought national attention to the issue, either, had it not been for another member of Anonymous posting a blog entry about the attacks, who goes by the name Grey Lady. Alex Pearlman, *Opinion: Hacking vs. Rape: Which Is A Crime More Deserving of Jail Time?*, GLOBALPOST (Mar. 18, 2013, 4:00 PM), http://www.globalpost.com/dispatches/globalpost-blogs/rights/opinion-hacking-vs-rape-which-crime-more-deserving-jail-time.

[154] Kushner, *supra* note 12.

[155] *Id.*

[156] Taylor, *supra* note 140. Part of the reason behind the apparent leniency for the rapists' sentences, however, is because they were prosecuted as minors. Justin Peters, *Stop Comparing the Steubenville Hacker to the Steubenville Rapists. It's Misleading and Wrong.*, SLATE (June 12, 2013, 5:49 PM), http://www.slate.com/blogs/crime/2013/06/12/deric_lostutter_kyanonymous_stop_comparing_the_steubenville_hacker_to_the.html.

[157] *See* Kushner, *supra* note 12; John H. Richardson, *I Am Anonymous*, ESQUIRE (Oct. 14, 2013), http://www.esquire.com/news-politics/a25210/i-am-anonymous-1113/.

[158] Tor Ekeland, *Update on Deric Lostutter's Case*, TOR EKELAND, P.C. (May 16, 2014, 10:42 PM), https://torekeland.com/blog/update-deric-lostutters-case.

[159] *See id.*; Kushner, *supra* note 12; Taylor, *supra* note 140; Michael D. McElwain, *Man Who Took Control of Fan Website Talks*, HERALD STAR (Feb. 6, 2013), http://www.heraldstaronline.com/page/content.detail/id/582917/Man-who-took-control-of-fan-website-talks.html?nav=5010.

[160] Kushner, *supra* note 12.

[161] *See* White, *supra* note 10 (explaining how the prosecutorial treatment of Swartz was not unusual).

passing it to Gawker.com.[162] Auernheimer claimed to be showing AT&T that its system was unsafe.[163] He did not actually perform a hack in the traditional sense: his charge amounts to knowing of a security flaw AT&T was responsible for creating, altering a URL, and hitting enter multiple times.[164] He did not even write the program that collected the information.[165] That his actions were not actually malicious or "penetrative" did not prevent his prosecution either.[166] Nor was his case helped by the fact that these methods are commonly used in security research.[167] Though he allegedly conspired to cause "monetary and reputational damage to AT&T,"[168] Auernheimer did not cause actual damage to any individual with the information he gathered.[169] While his motivation may be questionable (as there are other means of informing AT&T of the vulnerability), his punishment was overly severe.[170] Threatened with a long jail sentence (standard practice under the CFAA),

---

[162] James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM. (Aug. 16, 2013), http://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/.

[163] *Id.*

[164] *See* Matt Brian, *Andrew 'weev' Auernheimer Sentenced to 41 Months for Exploiting AT&T iPad Security Flaw*, VERGE (Mar. 18, 2013, 11:57 AM), http://www.theverge.com/2013/3/18/4118484/andrew-weev-auernheimer-sentenced-att-ipad-hack. Auernheimer did not have to bypass any security in order to obtain the email addresses that he leaked to Gawker: he took advantage of knowledge that AT&T displayed device IDs in plain text in URLs when iPads connected to AT&T's website. *Id.* He and a friend wrote a script that would guess IDs, and then be given emails associated with the IDs when a guess was correct (this method of guessing and checking is called "brute force"). Andy Greenberg, *Security Researchers Cry Foul Over Conviction of AT&T iPad Hacker*, FORBES (Nov. 11, 2012), http://www.forbes.com/sites/andygreenberg/2012/11/21/security-researchers-cry-foul-over-conviction-of-att-ipad-hacker/. He did not actually gain unauthorized access to the servers to obtain the emails—AT&T's servers *gave* the list in response to the program. Brian, *supra.*

[165] Adrian Chen, *The Internet's Best Terrible Person Goes to Jail: Can a Reviled Master Troll Become a Geek Hero?*, GAWKER (Nov. 27, 2012, 10:05 AM), http://gawker.com/5962159/the-internets-best-terrible-person-goes-to-jail-can-a-reviled-master-troll-become-a-geek-hero.

[166] *See* Dan Kaplan, *Fear of Prosecution Hampers Security Research*, SC MAG. (July 19, 2013), http://www.scmagazine.com//fear-of-prosecution-hampers-security-research/article/303476/1/.

[167] *See* Brief of Security Researchers as Amici Curiae Supporting Appellant at 16–21, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 13-1816) (arguing that Auernheimer is an example of a security researcher, and criminalizing his actions is contrary to public interest because it hampers security research of this kind).

[168] Superseding Indictment at 5, *Auernheimer*, 748 F.3d 525 (No. 11-470), 2012 WL 6676870.

[169] *See id.* at 5–15. The government did not even allege that Auernheimer tried to harm individuals with his actions; the most it alleged was that he emailed a reporter whose email he had gathered about the breach, and offered to detail his methods. *Id.* at 12.

[170] Hendler, *supra* note 162 ("One can argue about Auernheimer's motivation, and the blogosphere is full of discussion about whether he should be considered a whistle-blower or a criminal hacker. But either way, the severity of the punishment seems unduly harsh.").

he pled guilty and was sentenced to forty-one months in prison.[171] That same month, a child pornographer received the same punishment.[172]

When examined closely, the actions that can garner this level of punishment are even more shocking: for example, Barrett Brown ("Brown") (a former impromptu spokesperson for Anonymous) faced up to 105 years in prison for, in part, copying and pasting a link.[173] Brown was indicted for computer fraud, though not under the CFAA, in relation to the Stratfor hack conducted by Hammond.[174] However, he could have been prosecuted under the CFAA.[175] What Brown did is not generally considered hacking.[176] The information contained at the end of the link, which was the crux of the case,[177] had been compiled by Hammond.[178] Specifically, the government's case focused on files that contained Stratfor clients' credit card and account information.[179] However, this information was but a small portion of what Hammond had collected and handed over to Brown.[180] Further, Brown was not interested in the credit card

---

[171] *Id.*

[172] *Id.*

[173] *See* Ludlow, *Barrett Brown*, *supra* note 28. Charges also included obstruction of justice because he was at his mother's house when the warrant was initially served, as well as threatening a federal agent for a YouTube video he posted online in response to the actions of the particular agent. *Id.* The case began, however, due to copying and pasting the link in an IRC chat. *Id.* The charges relating to copying and pasting a link have recently been dropped. Christian Stork, *"Hyperlink" Charges Against Barrett Brown Dropped in "Victory for Press Freedom"*, INDEX ON CENSORSHIP (Mar. 11, 2014), http://www.indexoncensorship.org/2014/03/dangers-journalism-persist-prosecution-barrett-brown/. Brown has been in prison, however, since September 2012 and has six charges pending against him for which he still faces 70 years in prison. *Id.*

[174] Thompson, *supra* note 15.

[175] *See id.* ("Simply publishing publicly available information, such as phone numbers found in a Google search, would probably not be charged under the CFAA. But hacking into private computers, *or even spreading the information from a hack*, could lead to charges under the CFAA.") (emphasis added).

[176] *See* Patrick McGuire, *Why Is Barrett Brown Facing 100 Years in Prison?*, VICE (Feb. 1, 2013), http://www.vice.com/read/why-is-barrett-brown-facing-100-years-in-jail ("Barrett Brown was not a hacker. He did not infiltrate any systems, nor did he appear to know how to do anything of the sort . . . ."). Generally, hacking requires some sort of digital breaking and entering. *See* HACK, BLACK'S LAW DICTIONARY 780 (9th ed. 2009).

[177] *See* Indictment at 1, 2, 4, United States of America v. Brown (I), No. 3-12CR-413-B (N.D. Tex. 2012), *available at* http://freebarrettbrown.org/files/BB_indictment2.pdf (alleging traffic in "authentication features" due to copying a hyperlink, and that he knowingly possessed and transferred credit card information by means of the copying).

[178] *See* Ludlow, *Barrett Brown*, *supra* note 28.

[179] *See* Indictment at 1–4, *Brown (I)*, No. 3-12CR-413-B.

[180] *See* Ludlow, *Barrett Brown*, *supra* note 28. The trove of documents stolen from Stratfor included 5 million emails alone. *Id.* The government, however, alleged "in excess of 5,000"

information: he was researching the activities of surveillance companies.[181] He copied the link into a private chat room, intending to share documents with other journalists.[182] It seems clear that Brown is not a malicious hacker out to use stolen credit card information; he is a journalist.[183] However, through its insistence on his prosecution, the government demonstrated a concerning position—that it considers copying and pasting a link a computer crime.[184]

A common theme in these cases is that the government's focus appears not to be what the defendant actually did, or the harm the defendant actually caused, but the *potential* harm of their actions.[185] This is unique in criminal law—a wrongful act is ordinarily required for criminal liability.[186] Many criminal acts focus on the intent of the actor, so CFAA prosecutions are not uncommon in this respect.[187] Rather than criminalizing malicious intent in carrying out a criminal activity, the CFAA tends to criminalize concrete actions, such as accessing a computer and obtaining information.[188] Lawful acts committed with malicious intent (such as aggregating publically available data)[189] are not criminal.[190] Further, CFAA

---

credit card numbers, but only 10 specific people's information. *See* Indictment at 1, 4–5, *Brown (I)*, No. 3-12CR-413-B.

[181] *See* Ludlow, *Barrett Brown*, *supra* note 28; McGuire, *supra* note 176 (explaining Brown's previous research into surveillance companies).

[182] *See* Ludlow, *Barrett Brown*, *supra* note 28 (describing the creation of WikiPage ProjectPM, to which Brown invited investigative journalists to join to help sort through collections of documents given to Brown from hackers).

[183] *See id.* Other people *did* use the credit card information for illicit purposes; however, it does not appear that Brown had anything to do with this: he linked to the information in a private chat room, and the information had already been publically disseminated. *See* Adrian Chen, *Former Anonymous Spokesman Barrett Brown Indicted for Sharing a Link to Stolen Credit Card Data*, GAWKER (Dec. 7, 2012, 6:56 PM), http://gawker.com/5966757/former-anonymous-spokesman-barrett-brown-indicted-for-sharing-a-link-to-stolen-credit-card-information.

[184] Stork, *supra* note 173.

[185] *Compare* Superseding Indictment at 5, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 11-470), 2012 WL 6676870 (claiming an object of the charged conspiracy was for Auernheimer to make a financial and reputational benefit for himself), *with* Chen, *supra* note 165 (claiming that Auernheimer "celebrated" the success of revealing the acquired information alone in his apartment and does not receive accolades like other hackers do).

[186] *See generally* ANDREW ASHWORTH & JEREMY HORDER, PRINCIPLES OF CRIMINAL LAW 95–102 (7th ed. 2013) (discussing three situations in which no wrongful act is necessary for criminal liability: situational liability, possession, and omission).

[187] *See id.* at 95 (discussing acts that are criminalized in which the act itself is not wrongful, but the intent with which it is done makes it wrongful, such as with attempt crimes).

[188] *See* 18 U.S.C. § 1030 (2012).

[189] *See, e.g.*, Chen, *supra* note 165.

[190] *See* ASHWORTH & HORDER, *supra* note 186, at 95 (discussing acts that are criminalized in

prosecutions do not always focus on intent, just potential harm.[191] For example, former Marines who get into bar fights are not charged with murder simply because they *could* have killed their opponent.[192] However, under the CFAA hackers who leak financial information (buried within millions of other documents and sometimes not even known to the "hackers" themselves)[193] are charged because they *could have* taken advantage of the information within, not because they did.[194] Because there is a generalized fear of "hackers," a fear eagerly promoted by law and policy makers alike, they are punished for their skillset rather than their actions.[195]

More ominously, some have suggested that such prosecutions have been used specifically to target and silence activists.[196] Certainly, many of the more famous cases were targeted for overt acts of protest.[197] Brown was

---

which the act itself is not wrongful, but the intent with which it is done makes it wrongful, such as with attempt crimes).

[191] *See, e.g.*, Indictment at 3, United States v. Ackroyd, 1:12-cr-00185-LAP (S.D.N.Y. May 2, 2012), *available at* http://freejeremy.net/wp-content/uploads/2014/09/09_Superceding_Indictment.pdf (referring to defendants as an "elite group of hackers"). For computer crimes, the line between intent and capabilities can be hard to draw. *See, e.g.*, Vijayan, *supra* note 17.

[192] *See generally* GEORGE P. FLETCHER, RETHINKING CRIMINAL LAW 360 (2000) (discussing homicide jurisprudence's requirement of an act which results in the death of another for liability to be incurred).

[193] *See* Ludlow, *Barrett Brown*, *supra* note 28.

[194] *See, e.g.*, Superseding Indictment at 1, 5, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 11-470), 2012 WL 6676870 (charging Auernheimer under 18 U.S.C. § 1030(a)(7), which criminalizes extortion using a computer, rather than actually using the information he stole). The central issue in the Auernheimer case was the theft of iPad user information (the object of the conspiracy); however, the charges against Auernheimer did not relate to that theft, but rather they related to the potential use of that information. *See id.* at 5–6.

[195] *Cf. e.g.*, Vijayan, *supra* note 17 (discussing a court order to remove a software developers computer and have the contents copied, without prior warning, simply because he listed himself as a "hacker" on his personal website). The Judge wrote: "By labeling themselves this way, they have essentially announced that they have the necessary computer skills and intent to simultaneously release the code publicly and conceal their role in that act." *Id.* Intent was read into the label "hacker." *See id.*

[196] *See* Ludlow, *Barrett Brown*, *supra* note 28 ("Considering that the person who carried out the actual Stratfor hack had several priors and is facing a maximum of ten years, the inescapable conclusion is that the problem is not with the hack itself but with Brown's journalism.").

[197] *See generally We Are Legion*, *supra* note 13 (discussing Operation Payback—the DDoS of MasterCard and PayPal in response to refusing to allow funding of WikiLeaks—and Anonymous' actions against the Church of Scientology). Anonymous had always made their intentions in regard to the Church of Scientology clear: they released a video, addressed to the Church, stating its mission and goals which can be seen at Church0fScientology, *Message to Scientology*, YOUTUBE (Jan. 21, 2008), http://www.youtube.com/watch?v=JCbKv9yiLiQ; *see also*

punished for doing something in his capacity as a journalist.[198] Lostutter was working to uncover a terrible crime against a minor and provide justice where it otherwise would not have been sought.[199] Auernheimer was arguably performing a service to the thousands of iPad users whose information could have been taken advantage of by "black hats," but he chose to do so in a way that publicly embarrassed AT&T.[200] Ironically, because people like Auernheimer are being prosecuted, malicious hackers are the only ones left breaking into systems—"white hats" are being driven away because they want to follow the law and fear prosecution.[201] Part of being a security researcher is disclosing findings; therefore, those who hack as part of their job, or in order to do "good" work, are more likely to be caught and subsequently prosecuted.[202] The government should not be prosecuting those who act in the interest of others.[203] In doing so, such acts of societal betterment are being discouraged.[204] That is, after all, the purported purpose and desired effect of criminal punishment.[205]

Further, these acts have "real world" parallels—acts of civil disobedience that take place in the physical world are similar to many acts of hacktivism in the Internet realm.[206] For example, DDoS attacks (and

---

Robert Vamosi, *Anonymous Hackers Take on the Church of Scientology*, C|NET (Jan. 24, 2008, 11:35 AM), http://news.cnet.com/8301-10789_3-9857666-57.html.

[198] Ludlow, *Barrett Brown*, *supra* note 28.

[199] *See* Kushner, *supra* note 12.

[200] *See* Hendler, *supra* note 162. He argued that he was trying to show that it was not secure in their system; had he wanted to take advantage of the insecurity, he could have just done so rather than publishing the insecurity (so that it would be subsequently fixed). *See id.*; *see also* Byron Acohido, *Ethical 'White Hat' Hackers Play Vital Security Role*, USA TODAY (Nov. 11, 2013, 7:27 PM), http://www.usatoday.com/story/cybertruth/2013/11/11/ethical-hackers-play-vital-role-in-improviing-security/3497427/ ("By flushing these bugs out into public light, [white hats] compel the good guys to fix the flaws before the bad guys can discover them first, and take advantage.").

[201] *See* Kaplan, *supra* note 166. Security researcher Shane McDougall was quoted as saying: "Right now, hackers are the only ones pinging these systems because security researchers aren't." *Id.*

[202] *See* KIMBERLY GRAVES, CEH OFFICIAL CERTIFIED HACKER REVIEW GUIDE: EXAM 312–50 Ebook 16 (2007), *available at* http://amihackerproof.com/Intro%20to%20Ethical%20Hacking.pdf (explaining "ethical hacking report[s]," which should be submitted after penetration tests).

[203] *See* Kaplan, *supra* note 166.

[204] *See generally id.* (explaining how excessive CFAA prosecution is hampering security researchers).

[205] *See* OVERVIEW, *supra* note 143.

[206] *See, e.g.*, Eric Walberg, *The Graffiti Revolution: An Expression of Political Dissent at a Time of Crisis*, GLOBAL RES. (Feb. 15, 2012), http://www.globalresearch.ca/the-graffiti-revolution-an-expression-of-political-dissent-at-a-time-of-crisis/29299. Graffiti is such an example: though

virtual sit-ins[207]) are similar to sit-ins that one would encounter in the physical world.[208] Anti-war, animal rights, or workers' rights activists who block access to a location by refusing to leave and taking up space are performing the functional equivalent of blocking access to a website—people who wish to use the location cannot.[209] Physical activists receive misdemeanor charges if they are arrested at all.[210] Should they resist arrest or physically touch an officer, they could receive felony charges; however, while these crimes are not physically possible in internet crime,[211] DDoS charges are still usually felonies.[212]

---

most commonly associated with street vandals, graffiti is commonly used as a means of expressing political causes and dissent. *See id.* Website defacement, one of the more popular forms of hacktivism, is comparable to graffiti in the digital sphere. *See* RJ RUSHMORE, VIRAL ART: HOW THE INTERNET HAS SHAPED STREET ART AND GRAFFITI 337–40, *available at* http://viralart.vandalog.com/read/ (click link in table of contents titled "Defacing websites as a form of graffiti").

[207] The practical effect of the two is the same. Virtual sit-ins are similar to DDoS attacks, but they require individual users to physically load the targeted website on their individual computers, rather than use an Internet tool to simulate the same effect. *See* Samuel, *supra* note 22, at 73. Essentially, DDoS attacks produce the same results with less participants required. *See id.*

[208] *See* Stefan Wray, On Electronic Civil Disobedience, Mar. 20–22, 1998, *available at* http://www.thing.net/~rdom/ecd/oecd.html (paper presented to the 1998 Socialist Scholars Conference).

> Just as the Vietnam War and the Gulf War brought thousands into the streets to disrupt the flow of normal business and governance—acting upon the physical infrastructure—future interventionist wars will be protested by the clogging or actual rupture of fiber optic cables and ISDN lines - acting upon the electronic and communications infrastructure.

Id. But see Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed By Denial-Of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 245–46 (2011) ("The relative or actual anonymity that participants enjoy in large-scale DoS attacks depersonalizes their message, requires much less commitment, and thus evidences much less conviction than a public act of disobedience in which an individual must take responsibility for her actions and face possible criminal punishment.").

[209] *Compare* BLACK'S LAW DICTIONARY 1599 (10th ed. 2014) ("sit-in"), *with* BLACK'S LAW DICTIONARY 529 (10th ed. 2014) ("Denial-of-service-attack": "A malicious strike against a computer, website, network, server, or database designed to render it inaccessible, usu. *by overwhelming it with activity* or by forcing it to malfunction.") (emphasis added).

[210] *See* NATIONAL LAWYERS GUILD LOS ANGELES, QUESTIONS AND ANSWERS ABOUT CIVIL DISOBEDIENCE AND THE LEGAL PROCESS 1, *available at* http://nlg-la.org/sites/default/files/cd_questions.pdf ("Protestors are usually charged with infractions (crimes not punishable by jail time) or misdemeanors (crimes punishable by a year in jail or less).").

[211] *See id.* at 1, 3–4.

[212] *See* JARRETT ET AL., *supra* note 92, at 47–49 (listing DDoS as an example of what can be prosecuted under § 1030(a)(5), as well as the various ways this section can be proven as a

Additionally, website defacement is a popular tactic used by hacktivists to distribute a message or make a point to the website's owner.[213] This action is also prosecuted under the CFAA.[214] Website defacement usually requires intrusion into a server or computer without permission or outside of the parameters set by the owners of the computer.[215] However, this is usually incidental to the hacktivists' goals.[216] Regardless, CFAA prosecutions result in hefty sentences: In 1999 Eric Burns ("Burns") received over a year in prison, three years probation, and over $35,000 in fines in a *plea deal* for defacing the White House website.[217] The CFAA has only strengthened and expanded since 1999.[218] Burns' actions are the digital equivalent of graffiti or replacing the contents of a display case.[219] In comparison, a man who actually attempted to graffiti the White House by rigging his car to drive through a barricade received thirty-five months and had to pay $5,345 in restitution.[220] The restitution is the only portion of his sentence related to the actual property damage—the

---

felony violation); Press Release, Fed. Bureau of Investigation, Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks (July 19, 2011), *available at* http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (explaining charges to those who participated in PayPal DDoS: "The charge of intentional damage to a protected computer carries a maximum penalty of 10 years in prison and a $250,000 fine. Each count of conspiracy carries a maximum penalty of five years in prison and a $250,000 fine.").

[213] Hampson, *supra* note 14, at 519–20.

[214] *See* JARRETT ET AL., *supra* note 92, at 38–39 (explaining that website defacement meets the damages element of § 1030(a)(5)).

[215] *See* Klang, *supra* note 70.

[216] *See id.* at 76–77.

> [W]hile the act of hacking, or the gaining of illegal access, is in many cases both illegal and not uncontroversial it is usually the means, and not the goal, of an act of civil disobedience. This is not to say that those who carry out online civil disobedience are not considered to be hackers, by themselves or others, but rather that the act of hacking is only part of the act of disobedience since it is a necessary component of webpage defacement.

Id. (internal citations omitted).

[217] MICHAEL NEWTON, THE ENCYCLOPEDIA OF HIGH-TECH CRIME AND CRIME-FIGHTING 127 (2004).

[218] *See generally* Skibell, *supra* note 86 (outlining the history of the CFAA and its various amendments which have increased its scope and strength).

[219] *See* KENNETH EINAR HIMMA, INTERNET SECURITY: HACKING, COUNTERHACKING, AND SOCIETY 90 (2007) (referring to website defacement as "e-graffiti").

[220] Press Release, The United States Attorney's Office, District of Columbia, Ohio Man Sentenced to 35 Months in Prison for June 2013 Incident at White House Complex (Jan. 10, 2014), *available at* http://www.justice.gov/usao/dc/news/2014/jan/14-005.html.

rest is related to breaking through the barricade and endangering officers' lives.[221] Because hacking takes place on a computer the people who hack are charged as felons, receiving years in prison and thousands of dollars in fines.[222]

The precedent set by prosecuting hacktivists under the CFAA is that civil disobedience in the digital frontier will not be tolerated.[223] Additionally, precedent considers computer crime more severe than crimes traditionally seen as the worst in society, such as rape: "So you get 25 years in prison for forcibly entering your way into a computer, but one year in prison for forcibly entering your way into a female. That's the message that we're sending with the Computer Fraud and Abuse Act."[224] Though acts of civil disobedience generally are not legal, they are also generally not felonies.[225] The critical difference is how one chooses to engage with democracy; civil disobedience of a different skill set is punished in an extremely severe manner.[226] In fact, the CFAA combined with the Guidelines expressly allow for more punishment *because* those who commit computer crimes use "sophisticated means" to do so.[227] As such, not only are hacktivists punished for their actual crime, but also for engaging in democracy through use of their specific skillset.[228]

---

[221] *See id.*

[222] *Compare* 18 U.S.C. § 1030(a)(5), (b)–(c) (2012) (possibility of a federal felony charge, should aggravating factors be present), *with* MASS. GEN. LAWS ch. 266, § 126A (2014) (maximum punishment is three years in prison and $1500 in fines), *and* N.Y. PENAL LAW § 145.60 (McKinney, McKinney's Penal Law through L.2014, chapters 1 to 398) (graffiti is a class A misdemeanor).

[223] Ludlow, *Hacktivists on Trial*, *supra* note 149 ("Taken together, the lesson appears to be that computer hacking for social causes and computer hacking aimed at exposing the secrets of governing elites will not be tolerated.").

[224] Sanya Dosani, *Are Computer Laws Too Tough On 'Hacktivists'?*, AL JAZEERA AM. (Oct. 22, 2013), http://america.aljazeera.com/watch/shows/america-tonight/america-tonight-blog/2013/10/22/are-computer-lawstootoughonhacktivists.html.

[225] *See supra* text accompanying notes 210, 220–21.

[226] *See generally supra* Part III.A.

[227] *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9) (2014) (allowing for an increase in offense level of two if "sophisticated means" were used to commit the crime); *see also* Fakhoury, *supra* note 116 (explaining that merely running a script is sufficient to meet this "sophisticated means" standard, as it was in Auernheimer's case, and it may have been in Swartz's case, though it never got to sentencing).

[228] *See* Fakhoury, *supra* note 116.

B. *Discouraging Electronic Civil Disobedience*

Presently, many "famous" forms of hacking that are prosecuted are expressly undertaken to promote political or social causes.[229] Anonymous, in particular, is known for its political statements and democratic or meritocratic agenda: "We stand for freedom. We stand for freedom of speech. The power of the people, the ability for them to protest against their government, to right wrongs. No censorship, especially online, but also in real life."[230] However, due to excessive prosecution, and the very active role the FBI and other investigative units are playing in trying to find Anonymous members and other hacktivists,[231] such forms of electronic civil disobedience are discouraged, even those with express political and social motivations.[232]

Civil disobedience has historically been used as a means to move the United States forward when the traditional political process was too slow or plagued by the same social ills and prejudices as the general populace.[233] As such, though illegal by nature, it has an honored place in our society.[234] Taking into account the progress of America and the increasing digitization of the American way of life (which was itself part of the push behind

---

[229] *See generally We Are Legion, supra* note 13. Such famous cases that are in the social consciousness are Operation Payback (the DDoS of PayPal and MasterCard), Swartz, Hammond, Julian Assange, and other operations of Anonymous such as outing the Steubenville rapists or organizing the blockade against the Westboro Baptist Church. *See, e.g., id.*; Smith, *supra* note 6.

[230] *We Are Legion, supra* note 13 (quoting an Anonymous member at a protest).

[231] *See, e.g.*, Robert S. Mueller, III, Director, Federal Bureau of Investigation, Remarks at the International Conference on Cyber Security 2013: The Future of Cyber Security from the FBI's Perspective (Aug. 8, 20130), *available at* http://www.fbi.gov/news/speeches/the-future-of-cyber-security-from-the-fbis-perspective; Robert S. Mueller, III, Director, Federal Bureau of Investigation, Remarks at the RSA Cyber Security Conference: Working Together to Defeat Cyber Threats (Feb. 28, 2013), *available at* http://www.fbi.gov/news/speeches/working-together-to-defeat-cyber-threats.

[232] *See We Are Legion, supra* note 13. For example, a high ranking member of Anonymous, Anonyops, stated: "I would love to live in a country where the government fears its citizens and not the other way around. Right now, *plenty of Anonymous actors are in hiding because of fear of reprisals by the government.*" *Id.* (emphasis added).

[233] *See* Tammy A. Tierney, Comment, *Civil Disobedience As The Lesser Evil*, 59 U. COLO. L. REV. 961, 967–68 (1988).

[234] *See id.* at 968 ("As history demonstrates, Americans have come to believe that civil disobedience is an important part of their political culture."); *see also* Matthew Lippman, *Civil Resistance: The Dictates of Conscience and International Law Versus The American Judiciary*, 6 FLA. J. INT'L L. 5, 7–8 (1990) ("[T]he assertion of individual conscience against governmental strictures is a persistent theme in United States history. One manifestation of the primacy of individual conscience is the tradition of non-violent civil disobedience to governmental authority.").

passing the CFAA),[235] it only makes sense that civil disobedience shifted into the forums where the rest of our everyday lives moved.[236] Such technological progress in civil disobedience has happened before—distributing information via mail or telephone, organizing more effectively over social media, and even hacking in the earlier days of the Internet.[237] This is particularly unsurprising given that the effectiveness of traditional means of protest has recently come into question.[238]

By discouraging protest where it is most effective and heard (*i.e.*, where the majority of American life is now conducted),[239] the government is hindering social change and, perhaps most importantly, a cornerstone of democracy—citizen protest.[240] Discouraging such acts erodes the very foundations of democracy.[241] There has been a space for these types of actions in the past; this space should continue to permit acts of civil disobedience, regardless of the medium.[242]

---

[235] *See* H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694.

[236] *See* Züger, *supra* note 17 ("Albeit civil disobedience is a dedicated term, it is today being revisited – its forms are being adapted to new technical possibilities and to the environment of the information age.").

[237] *See, e.g.*, Joshua Brunstein, *Drones for Hire*, N.Y. TIMES (Feb. 17, 2012), http://www.nytimes.com/video/technology/100000001364648/drones-for-hire.html (discussing various uses for drones, including "drone activism" to film protest encounters with police); Gloria Feldt, *Margaret Sanger's Obscenity*, N.Y. TIMES (Oct. 15, 2006), http://www.nytimes.com/2006/10/15/opinion/nyregionopinions/15CIfeldt.html (detailing Sanger's use of the mail to disseminate information about birth control in violation of the Comstock Act); McCormick, *supra* note 25 (noting the second major computer worm ever released, the "'WANK'" worm, was an anti-nuclear protest, displaying the message "'WORMS AGAINST NUCLEAR KILLERS'" on the target's computer); Howard et al., *supra* note 52, at 2 (finding "[s]ocial media played a central role in shaping political debates in the Arab Spring").

[238] Philip Wight, *Has Civil Disobedience Become Too Predictable?*, WAGING NONVIOLENCE (Nov. 5, 2013), http://wagingnonviolence.org/feature/civil-disobedience-become-predictable/.

[239] *See, e.g.*, U.S. CENSUS BUREAU, E-STATS 1–2 (2011), *available at* http://www.census.gov/econ/estats/2011/2011reportfinal.pdf (showing that e-commerce is a large portion of U.S. business).

[240] *Cf.* Tierney, *supra* note 233 (explaining uses of civil disobedience to effect large scale social change in American history).

[241] *See* WILLIAM SMITH, CIVIL DISOBEDIENCE AND DELIBERATIVE DEMOCRACY 137–39 (2013) (explaining that civil disobedience is a democratic practice: "The theory, if sound, suggests that civil disobedience should be regarded as an important, albeit somewhat transgressive, guardian of deliberative democracy"); *see, e.g.*, U.S. CONST. amend. I (guaranteeing the freedom of peaceful assemblage to the people).

[242] *See* Tierney, *supra* note 233.

Electronic civil disobedience has a place in our digital world and can produce real results that benefit society.[243] This is true particularly in a democratic society, where freedom of speech and individual participation in government are encouraged.[244] The CFAA is discouraging acts of electronic civil disobedience, and as a result "white-hat" hackers—those that would use their abilities to help rather than harm—are pulling back from participation to avoid criminal liability.[245] These hackers are warning each other not to help due to fears of prosecution: "There is a lesson to be learned from all of this [prosecutions of the writer and others], and this is what I would like to emphasize: *Do not be a good guy.* It never pays off."[246] The writer continues: "don't help companies, don't help schools, don't help the government. . . . You can't trust anyone."[247]

Even worse, activists are taking extreme measures to avoid or escape prosecution: it is commonly believed, and has been asserted by his family, that Swartz took his own life in response to the stress of the charges and sentence he faced.[248] This type of activism will decline if we expressly tell those engaging in online activism that what they are doing is a severe crime and will result in the same fate as Hammond, Brown, or perhaps even Swartz.[249] America has a long history of civil disobedience, beginning with its founding.[250] It does not bode well for the future of our country, as we move into a digital age, to strike fear into the hearts of those who seek to make political and social progress; when political and social progress are stunted, so is the country.[251]

C. *Malleable Sentencing Structure Results in Excessive Punishment Inconsistently Applied*

The third problem with current hacktivism prosecution is that the sentencing structure gives prosecutors an incredible amount of power over

---

[243] *See supra* Part I.B.

[244] *See, e.g.*, U.S. CONST. amend. I, XV, XX.

[245] *See, e.g.*, Kaplan, *supra* note 166 (explaining that security researchers, a form of white-hat hackers, are afraid to continue their research in particular circumstances due to fear of prosecution).

[246] Arciszewski, *supra* note 142.

[247] *Id.*

[248] *See* Owen Thomas, *Family of Aaron Swartz Blames MIT, Prosecutors for His Death*, BUS. INSIDER (Jan. 12, 2013, 6:21 PM), http://www.businessinsider.com/statement-family-aaron-swartz-2013-1.

[249] *See supra* notes 231–232 and accompanying text.

[250] *See* Tierney, *supra* note 233; Kayla Star & Bonnie Blackberry, *The Role of Civil Disobedience in Democracy*, CIV. LIBERTIES MONITORING PROJECT (1998), *available at* http://www.civilliberties.org/htdocs/sum98role.html.

[251] *Cf.* Tierney, *supra* note 233.

the ultimate outcome of the case.[252] This results in excessive and inconsistent punishment because similar crimes are charged differently depending on the prosecutor, the offender, and whether or not a particular defendant would make a good example.[253] This inconsistency makes it difficult to predict the outcome of any given case, and therefore makes it difficult for an actor to know whether their actions fall within the boundaries of felony or misdemeanor CFAA conduct.[254]

The Guidelines have, since their inception, placed more of the sentencing decision in the hands of prosecutors.[255] This occurs because of how prosecutors charge particular crimes: both the "nature of the crime" and the nature of the criminal affect federal sentencing; prosecutors only need to change the "nature of the crime" to increase to offense level.[256] With respect to the CFAA, this occurs in two ways: prosecutors charge misdemeanor crimes as felonies by piling on aggravating factors under the provisions of the CFAA and take advantage of the Guidelines which allow for increasing a defendant's offense level for similar reasons.[257] While it may seem that only particularly heinous acts of hacking would potentially be charged as felonies, the aggravating factors of the CFAA are not particularly difficult to meet.[258]

For example, under § 1030(a)(2), an aggravating factor is if the information obtained (obtained, under the statute, could mean simply viewing the information) exceeds $5,000 in value.[259] While at first blush this may appear to be a bright line rule, the damages amount is actually an incredibly malleable standard: in calculating the value of the information obtained prosecutors can include research and development costs, manufacturing costs, the property's value on the black market, or what the company itself paid for the property.[260] Prosecutors can use any

---

[252] *See* Fakhoury, *supra* note 116.

[253] *Computer Fraud and Abuse Act (CFAA) Reform*, TECH FREEDOM (July 19, 2013), http://techfreedom.org/post/58451738234/computer-fraud-and-abuse-act-cfaa-reform (stating that the CFAA "[r]elies on inconsistent and politically-motivated prosecutorial discretion" in case selection and prosecution, that prosecutors have "too much room to pick and choose defendants based on their visibility (or other political motivations)" and that it "fails to place clear limits on a prosecutor's ability to seek an increase in the severity of punishment," which results "in inconsistent and unpredictable sentencing").

[254] *Id.*

[255] Silbert, *supra* note 141.

[256] *See generally* discussion *supra* Part II.B.

[257] *See generally* discussion *supra* Part II.B.

[258] *See* Fakhoury, *supra* note 116 (describing the calculation of "financial loss" under the sentencing guidelines, and how this standard is susceptible to manipulation).

[259] 18 U.S.C. § 1030(c)(2)(B)(iii) (2012).

[260] JARRETT ET AL., *supra* note 92, at 20; CLIFFORD, *supra* note 102, at 193.

"reasonable" method to calculate damages, which in practice means almost any tangentially related method.[261] Under subsection (a)(5), the damaged computer does not even have to be the computer accessed by the defendant.[262] Simply making a computer temporarily unavailable constitutes damage—a DDoS attack by definition causes damage.[263] Theft of trade secrets can be "damage" under the CFAA, despite being its own, separate, prosecutable offense.[264] Additionally, whether the perpetrator accessed the information in furtherance of *any* criminal or tortious act is also an aggravating factor allowing the charge to become a felony.[265] Prosecutors are even encouraged to look into state common law tort claims, such as invasion of privacy, to find such a tortious act in order to charge the felony.[266]

Further, § 1030(c)(2)(C) provides that if a violation of § 1030(a)(2) occurs after a previous conviction under subsections (a)(2), (a)(3), or (a)(6) (or an attempt to commit either), it may be a felony.[267] Counter intuitively, however, previous convictions do not have to come *before* the present indictment: should a defendant be charged under more than one provision of the CFAA in one indictment, and convicted under more than one provision in a single proceeding, the contemporaneous conviction counts as a "previous conviction."[268] This means a first time offender can be charged with a felony simply because the prosecutor is able to charge his conduct under more than one provision of the CFAA.[269] This is exceedingly likely considering multiple sections of the CFAA are duplicative.[270] For example, § 1030(a)(3) is a misdemeanor, but § 1030(a)(2) is applicable in many cases in which this provision would apply, and would actually be

---

[261] JARRETT ET AL., *supra* note 92, at 43 (explaining various loss calculations that courts have upheld and instructing: "Prosecutors should think creatively about what sorts of harms in a particular situation meet this definition and work with victims to measure and document all of these losses").

[262] *Id.* at 38.

[263] *Id.* at 39.

[264] *Id.* at 41.

[265] 18 U.S.C. § 1030(c)(2)(B)(ii) (2012).

[266] *See* JARRETT ET AL., *supra* note 92, at 27.

[267] § 1030(c)(2)(C) (providing for punishment up to ten years).

[268] *See* Cindy Cohn, Hanni Fakhoury & Marcia Hofmann, *Rebooting Computer Crime Part 3: The Punishment Should Fit the Crime*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 2013), https://www.eff.org/deeplinks/2013/02/rebooting-computer-crime-part-3-punishment-should-fit-crime.

[269] *See id.*

[270] *See id.* (suggesting these provisions be struck from the present law, as they allow for this "double-counting" of a single offense).

the preferred prosecutorial tool because it can be charged as a felony with aggravating factors.[271]

PROPOSAL

IV. Consider Hacker Intent, Delete Duplicity, and Charge More Misdemeanors

In the wake of Swartz's suicide, several proposals have been made to amend, repeal, or otherwise revise the CFAA.[272] The majority of these proposals aim to reduce liability under the CFAA.[273] However, a number of them actually aim to strengthen the Act and *increase* statutory maximums.[274] Though simply increasing statutory maximums may not drastically affect prosecutions,[275] another proposal to make any violation of subsection (a)(2) into a felony, rather than a misdemeanor, could.[276] Such a change would increase prosecutions under that provision, as felonies are more likely to be charged by federal prosecutors than misdemeanors, and likely criminalize more conduct.[277] Congress is proposing this change, as it has in the past, with no evidence that it is necessary.[278] This is not the direction we should take: creating more crimes with longer sentences will just exacerbate current problems within the CFAA.[279] Despite this, draft legislation increasing the power of the CFAA, rather than reducing its bite, has been more popular with Congress and "big data" companies.[280]

The most commonly known proposal to reduce the computer crimes the CFAA covers is known as "Aaron's Law."[281] Its primary concerns are clarifying the meaning of "access without authorization," eliminating redundancy (which allows duplicitous charging), and making penalties proportional to the charged crimes.[282] In order to reduce redundancy within the law, this draft legislation would remove § 1030(a)(4) from the

---

[271] *See* JARRETT ET AL., *supra* note 92, at 20.

[272] *See, e.g.*, Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/.

[273] *See* Toren, *supra* note 88.

[274] *Id.*

[275] *Id.*

[276] *Id.*

[277] *Id.*

[278] *Id.*

[279] *See generally supra* Part III.

[280] *See* Toren, *supra* note 88; Wu, *supra* note 76.

[281] *See* Toren, *supra* note 88.

[282] Aaron's Law, H.R. 2454, 113th Cong. §§ 2–4 (1st Sess. 2013).

CFAA entirely.[283] Additionally, Aaron's Law seeks to modify the penalty enhancement (from a misdemeanor to a felony) for violations of subsection (c)(2), so that prosecutors would not be able to seek the enhancement if the violation was committed in furtherance of another tortious act.[284] This would further prevent the duplicitous charging problem.[285] Aaron's Law also seeks to clarify the "conviction for another offense" language concerning penalty enhancement so that the offense actually has to be *subsequent*; in other words, a crime charged at the same time cannot be "subsequent."[286]

This is an excellent start, achieved through listening to the input of regular Internet users.[287] However, Aaron's Law still does not solve some of the problems presented by the CFAA, such as ignoring the intent of a defendant in committing the act.[288] In order to account for acts of civil disobedience that occur in the digital realm, the law should take into account the hacker's intent in committing the act.[289] Currently, the CFAA does not require that a hacker intend to cause damage to impose penalties.[290] In addition to the reforms above, the law should consider whether the hacker was engaged in electronic civil disobedience when committing the act (or otherwise did not intend harm in the traditional sense, such as an accidental overreach or security research).[291] This would allow hacktivists an opportunity to express their views in court and to have the court consider those motivations in sentencing.[292] Additionally, security researchers would no longer need to fear prosecution for finding and

---

[283] *Id.* § 3.

[284] *See id.* § 4.

[285] *Id.*

[286] *Id.*

[287] *See* Lofgren & Wyden, *supra* note 272. Legislators solicited the opinion of the public on the Internet while drafting this legislation. *Id.*

[288] *See* Aaron's Law, H.R. 2454, 113th Cong. (1st Sess. 2013) (proposing amendments to 18 U.S.C. § 1030 but none of the listed modifications refer to intent).

[289] *Cf.* Trevor Timm, *Reform the CFAA: Don't Let it Stop The Next Steve Jobs, Bill Gates, Mark Zuckerberg, or Steve Wozniak*, ELECTRONIC FRONTIER FOUND. (Mar. 7, 2013), https://www.eff.org/deeplinks/2013/03/innovators ("[T]he law needs to recognize the difference between commercial criminals and those who are merely "testing the boundaries" or engaging in youthful indiscretions.").

[290] *See* Trevor A. Thompson, Comment, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537, 562–63 (2009).

[291] *See generally* Part III.B.

[292] *Contra* Kopstein, *supra* note 1 (explaining that even if the judge in Hammond's case had been sympathetic to his dissent, she could not have given a lenient sentence due to the "base offense level" calculations).

reporting dangerous security holes to relevant authorities and the public.[293] In this way, looking at the intent of the actor adequately balances the needs of society: on the one hand, punishing transgressive acts that cause harm to others, but on the other, not overly discouraging a time-honored form of political participation solely because of the forum in which it takes place.[294]

However, Congress has previously reduced the mens rea necessary to be convicted under the CFAA,[295] and considering the hacker's intent has been a controversial suggestion.[296] Inquiry into criminal intent is nothing new, and therefore is unlikely to impose a significantly heavier burden on judicial actors than other crimes.[297] For example, the common crime of possession with the intent to distribute narcotics requires a showing of intent.[298] The intent, absent a confession, is proven circumstantially using the quantity of the substance recovered, packaging, and other paraphernalia.[299] Similarly, in a CFAA case the Government can introduce evidence of chatlogs, past similar criminal acts, and the type of equipment found at the defendants address.[300] In opposition, the defendant can introduce evidence that the act is part of a larger political or social protest, the announcement of the act ahead of time, and that they did not profit from their act.[301] In this way, the defendant's intent (to cause harm, make money, or promote a particular cause) can be taken into account without forcing courts to ignore it.[302]

---

[293] *See* Tom Brewster, *US Cybercrime Laws Being Used to Target Security Researchers*, GUARDIAN (May 29, 2014, 11:09AM), http://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers.

[294] *Cf. supra* notes 233–234 and accompanying text.

[295] Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 290–94 (1997).

[296] *See, e.g.*, Robert B. Milligan & Grace Chuchla, *Significant Amendments Proposed to the Computer Fraud and Abuse Act to Limit Its Use to Traditional Hacking Scenarios*, LEXOLOGY (Jun. 26, 2013), http://www.lexology.com/library/detail.aspx?g=6257c52f-2cc4-4f18-968d-8d23cd6a9ddb (explaining that security companies have come out against Aaron's Law in part because of the language "*knowingly* circumventing technological or physical measures") (emphasis added).

[297] *See infra* notes 298–302 and accompanying text.

[298] *See* Anna Lindemann, *Peddling or Possession? Proving Intent to Distribute Versus Personal Use*, LIVESAY & MYERS (Mar. 4, 2013), http://www.livesaymyers.com/proving-intent-to-distribute-versus-personal-use-virginia/.

[299] *Id.*

[300] *See, e.g.*, Sentencing Hearing Transcript at 40–45, United States v. Hammond, No. 12 CR 185 (LAP) 2013 WL 637007 (S.D.N.Y. Feb. 21, 2013), *available at* freejeremy.net/wp-content/uploads/2014/09/Hammond_sentencing_transcript.pdf.

[301] *See, e.g., id.* at 14–40.

[302] *See* Kopstein, *supra* note 1.

Additionally, measures contained in Aaron's Law do not entirely eliminate duplicitous charges—subsection (a)(3) is also a redundancy of (a)(2).[303] Subsection (a)(2) is sufficiently broad to cover these crimes.[304] Therefore, *both* subsections (a)(3) and (a)(4) should be removed to prevent stacking charges.[305] Finally, barring extreme circumstances (such as large monetary loss fairly calculated or furthering an actual felony), first-time offenses under the CFAA should be misdemeanors.[306] This would better track physical-world civil disobedience penalties,[307] while still recognizing that hacking *is* a computer crime, regardless of a noble motive.[308]

An additional remedy, though less obvious, is the severance of civil liability through the CFAA.[309] Under the CFAA, a person can be civilly liable for the same actions that create *felony* criminal liability.[310] However, because both criminal and civil liability exist under the same provisions, criminal liability has been impacted by civil interpretations of the Act.[311] It has been suggested that much of the broad overreach under the CFAA's provisions is caused by interpretations of the Act in the civil context rather than broad criminal liability.[312]

> Even if [Judge] Preska had been sympathetic to Hammond or to his cause, it would have been difficult for her to hand down a particularly lenient sentence. The Supreme Court has instructed judges to ignore sentencing guidelines at their own peril, and the Computer Fraud and Abuse Act . . . engenders restrictive sentencing guidelines.

Id.

[303] *See* Cindy Cohn & Marcia Hofmann, *Part 2: EFF's Additional Improvements to Aaron's Law*, ELECTRONIC FRONTIER FOUND. (Jan. 23, 2013), https://www.eff.org/deeplinks/2013/01/part-2-effs-additional-improvements-aarons-law; Aaron's Law, H.R. 2454, 113th Cong. (1st Sess. 2013).

[304] *Compare* 18 U.S.C. § 1030(a)(3), *with* 18 U.S.C. § 1030(a)(2).

[305] *See* Cohn & Hofmann, *supra* note 303.

[306] *See id.*

[307] *See supra* notes 206–222 and accompanying text.

[308] *See* Cohn, Fakhoury, & Hofmann, *supra* note 268.

[309] *See, e.g., EFF CFAA Revisions – Penalties and Access*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/document/eff-cfaa-revisions-penalties-and-access (last visited Apr. 14, 2015) (changing subsection (f) of the CFAA to impose no civil liability, as civil liability is duplicative of other civil claims).

[310] Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 93–94 (2014).

[311] *See, e.g.*, JARRETT ET AL., *supra* note 92, at 5–12 (using civil cases to assist in explaining the definition of "Without Authorization" or "Exceeds Authorized Access," definitions key to several provisions of the CFAA).

[312] *See* Cohn, Fakhoury, & Hofmann, *supra* note 268 (information is located in a footnote).

CONCLUSION

Hacktivism is the next generation of civil disobedience, moving a time-honored tradition of our individual participation in government into the digital sphere. It has proven effective in a variety of contexts throughout the world, sometimes more effective than traditional means of protest. However, the United States is, in some cases, punishing these civil dissidents more severely than those who commit severe physical crimes. In order to preserve this means of political participation, the CFAA needs to be reformed.

Currently, the sentences that hacktivists receive do not fit the crimes they have committed. Hacktivism is assuredly less of a crime than child pornography or assault, both of which have received similar, or at times less onerous, sentences. Further, the federal sentencing guidelines, combined with the CFAA's statutory maximums and aggravating factors allowing misdemeanors to be charged as felonies, allow for relatively simple conduct to be compounded into decades of prison time. The CFAA also has a number of duplicitous provisions which allow for the stacking of charges. This means some provisions are charged as felonies where they would otherwise be charged as misdemeanors, based on the conduct of the hacker.

In the end, this discourages electronic civil disobedience. In a country with a tradition of social change through political activism, this result should be concerning. To prevent this, the CFAA should be reformed in the following ways: the intent of hackers should be accounted for so that the court can consider whether the acts were for personal gain or social betterment; duplicitous provisions should be removed; and first time offenses under the CFAA's provisions should be misdemeanors. In this way, hacktivism would be treated more like traditional civil disobedience, and hacktivists would not be punished for using a different skill set to protest.

* * * *