AARON'S LAW: BRINGING SENSIBILITY TO THE COMPUTER FRAUD AND ABUSE ACT

Mark Murfin*

I. INTRODUCTION

"Stealing is stealing, whether you use a computer command or a crowbar, and whether you take documents, data or dollars. It is equally harmful to the victim whether you sell what you have stolen or give it away."[1] With those words, U.S. Attorney for the District of Massachusetts Carmen Ortiz celebrated the indictment of twenty-four-year-old Aaron Swartz for allegedly downloading and distributing a substantial proportion of JSTOR's digitized academic journal archive.[2]

Eighteen months later, Aaron Swartz tragically committed suicide.[3] While the exact reasons for his actions will probably never be clear, his family claims that the prosecutors wanted to make an example out of Swartz, and the overzealous attack they mounted against him contributed to his depression and suicide.[4] The case against him rested on the Computer Fraud and Abuse Act of 1986 (CFAA), a law enacted well before the coming of age of the Internet and the dawn of the information age.[5] If given the maximum sentence allowed by the CFAA, Aaron Swartz would have spent thirty-five years in prison; more days than he had seen in his entire life.[6] To an Internet prodigy who made significant contributions to it by the age of fourteen,[7] this shadow of imprisonment might as well have been a death sentence.

---

* Mark Murfin is a third-year law student expecting his J.D. from Southern Illinois University School of Law in May 2014.

1. Press Release, U.S. Attorney's Office for the Dist. of Mass., Alleged Hacker Charged with Stealing over Four Million Documents from MIT Network (July 19, 2011), *available at* http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html.
2. *Id*.
3. John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y TIMES, Jan. 12, 2013, http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html.
4. Laura Smith-Spark, *Prosecutor Defends Case Against Aaron Swartz*, CNN (Jan. 18, 2013), http://www.cnn.com/2013/01/17/tech/aaron-swartz-death.
5. Grant McCool, *Computer Fraud and Abuse Act: The 1980s-Era Hacking Law Out Of Step With Today's Internet, Analysts Say*, HUFFINGTON POST (July 29, 2012), http://www.huffingtonpost.com/2012/07/29/computer-fraud-and-abuse-act_n_1716058.html.
6. Smith-Spark, *supra* note 4.
7. Todd Leopold, *How Aaron Swartz Helped Build the Internet*, CNN (Jan. 15, 2013), http://www.cnn.com/2013/01/15/tech/web/aaron-swartz-internet.

The aftermath of Aaron Swartz's suicide brought a whirlwind of media fury, and Representative Zoe Lofgren has introduced a bill to amend the CFAA. Her goal is to avoid another such tragedy by removing the tools the prosecutors used to make their case. Titled "Aaron's Law," it would completely replace the CFAA's definition of "exceeds authorized access" and require the "circumvention of technological measures designed to prevent unauthorized access" before imposing civil and criminal penalties.[8]

There are several competing interpretations of the CFAA's "authorization" provision, and there has been much discussion among legal commentators about the inadequacies of those interpretations. There have also been other proposed interpretations apart from Aaron's Law to amend the CFAA, but this is the first appearance of a bill in Congress promising real change. However, none of these approaches are adequate; a better law would address the actual harms that citizens seek to mitigate, regardless of whether that mitigation takes the form of a contract, computer code, or otherwise.

Section II of this Comment will provide an overview of the various ways in which the CFAA's authorization language is interpreted in courts today and illustrate the split between the circuits. Section III will discuss the events surrounding Aaron Swartz's suicide as the impetus for the creation of Aaron's Law as well as Aaron's Law itself. Section IV will discuss why Aaron's Law is a good step, but ultimately not enough of an improvement to the CFAA. Section V will outline a proposal targeted at fulfilling the CFAA's purpose of preventing computer crimes.

II. BACKGROUND

> See that sign up here—up here. "Defcon." That indicates our current defense condition. It should read "Defcon 5," which means peace. It's still on 4 because of that little stunt you pulled. Actually, if we hadn't caught it in time, it might have gone to Defcon 1. You know what that means, David?
>
> No. What does it mean?
>
> *World War Three*.[9]

Global thermonuclear war was the context of the 1983 movie WarGames.[10] Seemingly against all odds, a high school student found a

8. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).
9. WARGAMES (United Artists 1983).
10. *Id.*

government computer connected to the public telephone system and played a not-so-innocent simulation of nuclear war that turned out to have real-world consequences.[11] As far-fetched as it may sound, this movie was referenced on the floor of the House of Representatives as a "realistic representation of the . . . capabilities of the personal computer" and an example of the sort of computer mischief lawmakers needed to address.[12] The reference worked and the first federal computer crime laws were born: three lonely statutes in a massive crime bill known as the Comprehensive Crime Control Act.[13] As a result, when U.S. Attorney Ortiz commented that Swartz might as well have used a crowbar, she neglected to mention that the CFAA, enacted after a WarGames-induced hacking scare and possibly designed to protect vital NORAD computer resources, would punish Swartz more severely than if he had committed an assault with an actual crowbar.[14]

Congress was not finished, though, and went on to enact the CFAA to combat "a new breed of criminal: the technologically sophisticated criminal who breaks into computerized data files."[15] These "hackers" were likened to trespassers, "breaking windows" and "crawling into homes while the occupants were away."[16] As apt as Congress may have found that description, the courts had been struggling to apply traditional laws such as trespass to crimes involving computers.[17] Thus, the CFAA was also largely designed to address those apparent shortcomings that had resulted from using traditional laws like larceny, embezzlement, and conversion to punish novel crimes involving computers.[18] For instance, it hardly matters whether money is stolen by physically taking it or via an unauthorized computer transfer. The money is gone and traditional laws dealing with theft will be quite sufficient to repair the harm and punish the thief. On the other hand, an employee who uses a computer to view customers' confidential information and then gives that information to competitors has certainly committed harm, but courts have struggled to find a fiction, let alone a true reason, as to how to apply a traditional statute like theft to this situation.[19]

---

11. *Id*.
12. H.R. REP. NO. 98-894, at 10 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3694-95.
13. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563-64 (2010).
14. Declan McCullagh, *From 'WarGames' to Aaron Swartz: How U.S. Anti-Hacking Law Went Astray*, CNET (Mar. 13, 2003), http://news.cnet.com/8301-13578_3-57573985-38/from-wargames-to-aaron-swartz-how-u.s-anti-hacking-law-went-astray/.
15. 132 CONG. REC. H3275-04 (1986) (statement of Rep. Hughes).
16. *Id*.
17. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602 (2003).
18. *Id*.
19. *See id.* at 1605.

The CFAA set out to solve this, doubling the prohibitions from three to six as well as adding new definitions which expanded the type and number of computers protected by the statute.[20] The protected computers seemed, at the time, to be quite narrow because they were restricted to the computers of the government itself or financial institutions or computers used to commit the offense from different states.[21] It is important to remember that in 1986, the Internet as we know it did not exist and would not exist until 1990 with the advent of the World Wide Web.[22] Thus, the reach of the original CFAA was extremely limited. The second definition was later changed in 1996 to cover computers used in interstate commerce or communication.[23] This new definition was a huge change, encompassing every computer connected to the Internet under its umbrella.[24]

The 1996 amendment to the CFAA, with its expansion of the statute's applicability, set the stage for the CFAA to make a large appearance in the courts.[25] As might be expected of any statute covering novel ground, ambiguities were found. The courts eventually split over how to define "authorization" in the context of computer access.[26] Specifically, when a person uses a computer, when does he "exceed authorized access?"

The First, Fourth, Seventh, and Ninth Circuit Courts of Appeals have all answered that question, but in different ways.[27] The interpretations fall into four categories: contract-based, agency-based, "plain meaning," and code-based. The names alone betray the difficulty courts have encountered trying to apply the vague definitions of the CFAA.

A. Contract-Based Interpretation

Under the contract-based approach, a person "exceeds authorization" when he or she violates a contract, including employment contracts, network service provider agreements, computer use policies, or any other

20. Kerr, *supra* note 13, at 1565.
21. *Id.* at 1566.
22. *Pre-W3C Web and Internet Background*, W3C, http://www.w3.org/2004/Talks/w3c10-HowItAllStarted/?n=15 (last visited Apr. 28, 2014).
23. Kerr, *supra* note 13, at 1567.
24. Every computer connected to the Internet is by definition used in interstate communication. *See id.*
25. Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 U. PITT. J. TECH. L. & POL'Y 1 (2012).
26. Orin Kerr, *Recent Developments—Both in the Courts and in Congress—on the Scope of the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (July 30, 2012), http://www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act/.
27. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

agreement as to how a person may use a computer.[28] The First Circuit Court of Appeals held in *EF Cultural Travel BV v. Explorica, Inc.* that breach of a contract would constitute exceeding access under the CFAA.[29] In *Explorica*, the defendant had created a computer program which sent 30,000 requests to the plaintiff's web server and parsed the results into a spreadsheet for the defendant's use.[30] The results consisted of the plaintiff's price structure which the defendant intended to use to compete with them.[31] The First Circuit Court found that this action likely constituted a breach of a contract between the parties that the defendant "maintain in strict confidence and not . . . disclose to any third party, either orally or in writing, any [trade or business secrets or confidential information]."[32] Furthermore, this breach would constitute "excessive access" under the CFAA.[33] Thus, the First Circuit appears to have adopted a "contract-based" approach to interpreting the authorization language of the CFAA.[34] Had Aaron Swartz been brought to trial, this is the case law which would have governed the District Court of Massachusetts' interpretation of the CFAA.[35]

The greatest fear that many commentators have expressed with the contract-based approach is that merely violating the terms of service of a website, or any other innocuous activity on the Internet, would be turned into a felony by the CFAA.[36] This fear was narrowly avoided in *United States v. Drew*, a case from the Central District of California.[37] In *Drew*, the defendant violated MySpace's terms of service by creating a profile in which she pretended to be a young boy.[38] She then used that fake account to communicate with a thirteen-year-old girl who she bullied, telling her "the world would be a better place without her"; the girl committed suicide later that day.[39] Despite the tragic facts, the *Drew* court did not accept that violating MySpace's terms of service constituted "exceed[ing] authorization" out of fear that such an interpretation would "convert a

28. Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1555 (2012).
29. *EF Cultural Travel BV*, 274 F.3d at 579.
30. *Id*.
31. *Id*.
32. *Id*. at 582.
33. *Id*.
34. *See also* United States v. Czubinksi, 106 F.3d 1069 (1st Cir. 1997) (developing the contract-based approach, but only in dicta).
35. Appeals from the U.S. District Court for the District of Massachusetts are heard by the U.S. Court of Appeals for the First Circuit.
36. Kerr, *supra* note 13, at 1578; Kerr, *supra* note 17, at 1617; Hernacki, *supra* note 28, at 1555.
37. *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
38. *Id*. at 452.
39. *Id.*

multitude of otherwise innocent Internet users into misdemeanor criminals."[40]

B. Agency-Based Interpretation

Under the agency-based interpretation, a person becomes an agent of the entity that authorizes that person's use of a computer and loses that authorization implicitly when the person acts contrary to his or her duty of loyalty under agency law.[41] The Seventh Circuit Court of Appeals adopted this approach in *International Airport Centers, LLC v. Citrin*.[42] The defendant in *Citrin* was employed by the plaintiffs in the real estate business and given a laptop to use as he collected data in the course of his work identifying potential acquisitions.[43] However, the defendant decided to quit and go into business for himself.[44] Before doing so, he deleted all the data he had collected beyond recovery.[45] The Seventh Circuit Court held that the defendant's authorization terminated the moment he decided to quit the plaintiff's employment, in violation of both his employment contract and the duty of loyalty he owed to them under agency law.[46] This violation of his duties as an agent rendered his action of deleting the files to be without authorization and thus in violation of the CFAA.[47]

C. Plain Meaning Interpretation

The plain meaning interpretation focuses on whether a person had authorized access to the computer resources that were used, and not on how those resources were subsequently used.[48] That is, courts following the plain meaning interpretation will not ask how the computer resources were subsequently used, but only whether the person using them was authorized to use them in the first place. For instance, in *Citrin*, because the defendant was authorized to access and delete the data on his laptop, his deletion of that data was thus authorized, despite the fact that his action was contrary to

40. *Id.* at 460-66.
41. Kerr, *supra* note 13, at 1584; Hernacki, *supra* note 28, at 1558.
42. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2005).
43. *Id*. at 419.
44. *Id*.
45. *Id*. Data on a computer is generally deleted by merely marking it as "free," and the next time space is needed, the space is considered for overwriting. This leaves the data intact and available to be recovered by special software. In *Citrin*, the defendant purposefully overwrote the data in addition to marking it as free, thus rendering it unrecoverable even with special software. *Id.*
46. *Id*. at 420.
47. *Id*.
48. United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

the purpose of his employer in giving him such authorization.[49] This interpretation is based on the plain meaning of the CFAA's definition of "exceeds authorized access."[50] The CFAA defines "exceeds authorization" as occurring when a person has authorization to access a computer and then uses that access to obtain or alter information in the computer that he or she is not entitled to access.[51]

The Ninth Circuit Court of Appeals developed this approach in *LVRC Holdings, LLC v. Brekka* where it explicitly rejected the Seventh Circuit's approach in *Citrin*.[52] It reaffirmed this approach in *United States v. Nosal*.[53] Mr. Nosal left his company to start a competing business.[54] After leaving, he convinced some of his former colleagues to use their access to the company's computers and give him names and contact information to use for his new business.[55] The Ninth Circuit held that the CFAA's "exceeds authorization" language "targets the unauthorized procurement or alteration of information, not its misuse or misappropriation."[56] Thus, despite their misuse of the names and contact information, Mr. Nosal's colleagues did not exceed their authorization because they were authorized to access the data.

Only a few months later, the Fourth Circuit followed suit in *WEC Carolina Energy Solutions, LLC v. Miller*.[57] Mr. Miller worked for WEC, where he had access to a broad array of confidential WEC information, such as pricing terms, technical capabilities, and other trade secrets.[58] Mr. Miller decided to go to work for a competitor, but before resigning, he copied a substantial number of WEC's confidential documents.[59] About a month later, he used those documents to give a presentation to a potential WEC customer and swayed them into going with his new company.[60] The Fourth Circuit examined both the Seventh Circuit's agency approach in *Citrin* and the Ninth Circuit's plain meaning approach in *Nosal* and sided with the latter, explicitly rejecting the Seventh Circuit's agency approach.[61] The court held that the CFAA terms "without authorization" and "exceeds

49. His employers presumably gave him authorization to delete files that were useless or outdated and expected him to use reasonable judgment.
50. *Nosal*, 676 F.3d at 856-57.
51. 18 U.S.C. § 1030(e)(6) (2012).
52. LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133-35 (9th Cir. 2009).
53. *Nosal*, 676 F.3d at 862-63.
54. *Id*. at 856.
55. *Id*.
56. *Id*. at 863.
57. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).
58. *Id*. at 202.
59. *Id*.
60. *Id*.
61. *Id*. at 203.

authorization" "apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."[62] Thus, because Mr. Miller had authorization to access the information he did at the time he did, he did so with authorization, despite his apparent later misuse of that data.

D. Code-Based Interpretation

The code-based approach has not been adopted by any court, but has its origins in a 2003 law review article by Professor Orin Kerr.[63] Under the code-based approach, a person's authorization is regulated by computer code, not contract.[64] In fact, breaching a contract may never cause a user to exceed his or her authorization.[65] To act without or beyond authorization, a person must circumvent a code-based restricted, such as a password prompt.[66] This proposal has become the most popular approach to addressing the authorization interpretation problem in the CFAA and is reflected more in the proposed Aaron's Law than any of the other approaches.[67]

III. RECENT DEVELOPMENTS

A. The Life and Death of Aaron Swartz

Aaron Swartz has only recently become the subject of popular attention, but to Internet insiders, he has been well-known for over a decade.[68] His life as an Internet prodigy began at age fourteen when he helped create the Rich Site Summary standard (RSS),[69] a syndication format used to publish frequently updated Internet works in a form that is readily useable by computer programs.[70] His work on the RSS standard led

62. *Id*. at 206.
63. Kerr, *supra* note 17, at 1649.
64. *Id*.
65. *Id*.
66. *Id*.
67. Hernacki, *supra* note 28, at 1561. *But see* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass, and Privacy*, 62 BUS. LAW. 1395 (2007) (criticizing the code-based approach and proposing an alternative interpretation).
68. Noam Scheiber, *So Open It Hurts—What the Internet did to Aaron Swartz*, NEW REPUBLIC (Feb. 25, 2013), http://www.newrepublic.com/article/112485/aaron-swartz-profile-internet-will-never-save-you.
69. Formerly known as RDF Site Summary and popularly referred to as "Really Simple Syndication." Eric Draitser, *What Makes Aaron Swartz a Hero?*, RT (Feb. 13, 2014), http://rt.com/op-edge/nsa-protests-swartz-hero-863/.
70. Schwartz, *supra* note 3.

him to meet Tim Berners-Lee, the inventor of the World Wide Web, who became impressed by Aaron, especially given his age.[71] Schwartz went on to attend Stanford University, but dropped out after his freshman year because he did not find it a "very intellectual atmosphere."[72] He essentially co-founded the popular Internet website Reddit, which was later sold to Condé Nast and made Swartz a millionaire.[73]

Swartz's legal troubles began in 2008 when he went to the Seventh Circuit Court of Appeals library in Chicago and installed a PERL script[74] that took advantage of the Government Printing Office's experiment giving away free access to PACER at select libraries.[75] The PERL script requested a PACER document every three seconds and uploaded the document to a server Swartz had prepared.[76] The script ran from September 4 to September 20, and a total of twenty million pages were downloaded.[77] At that point, the IT department at PACER noticed that somebody was downloading *everything* and shut down the free trial.[78] PACER then reported to the Federal Bureau of Investigations that it had been compromised, and the FBI subsequently began investigating Swartz.[79] They did not contact him until the following April, but he refused to meet with them. They closed the case not long after.[80]

The PACER documents are, of course, public records and free of copyright, but PACER normally charges $0.08 per page.[81] If the documents had been requested without the free access at the Seventh Circuit library, they would have cost approximately $1.5 million.[82] Aaron Swartz donated all the documents he downloaded to public.resource.org, an organization dedicated to making government databases available to the public for free.[83]

---

71. Scheiber, *supra* note 68.
72. Aaron Sekhri, *Aaron Swartz, Prodigy and Drop-out, Takes Own Life*, STANFORD DAILY, Jan. 13, 2013, http://www.stanforddaily.com/2013/01/13/aaron-swartz-prodigy-and-drop-out-takes-own-life/.
73. Scheiber, *supra* note 68. Swartz founded a company that later merged with Reddit; however, he single-handedly wrote the code that ran Reddit, replacing older code. Glen Fleishman, *Setting the Record Straight on Aaron Swartz's Contributions*, BOING BOING (Jan. 17, 2013), http://boingboing.net/2013/01/17/aaron.html.
74. PERL is a programming language. A PERL script is a computer program.
75. Ryan Singel, *FBI Investigated Coder for Liberating Paywalled Court Records*, WIRED (Oct. 5, 2009), http://www.wired.com/threatlevel/2009/10/swartz-fbi/.
76. *Id*. For the curious, the server was hosted on Amazon EC2.
77. *Id*.
78. *Id*.
79. *Id*.
80. *Id*.
81. *Id*.
82. *Id*.
83. *Id*.

Swartz did not stop there, though, and in 2010 he bought a laptop and took it to the Massachusetts Institute of Technology (MIT) where he logged on to MIT's infamously open network and left it hidden under some cardboard boxes in an unlocked server closet.[84] He installed a Python script that used the MIT network's free access to JSTOR, a scholarly article database, to once again download documents en masse.[85] MIT and JSTOR soon noticed this activity on their network and twice blocked Swartz's laptop.[86] The first time JSTOR blocked the laptop's IP address, preventing only Swartz's laptop from accessing JSTOR.[87] Swartz simply got another IP address to get around this trivial block.[88] Next, JSTOR blocked an entire range of IP addresses, effectively blocking all of MIT from accessing JSTOR for three days.[89] That prompted MIT into action, blocking the laptop's MAC address; but less than a week later, Swartz slightly altered that address as well and kept going.[90]

MIT eventually located the laptop, but left it hidden.[91] They set up a hidden camera to see who would come back for the laptop.[92] The camera picked him up on January 4, 2011, and his description was noted.[93] On January 6 he returned, and this time police were called. They eventually found him outside the building and apprehended him after a chase on foot.[94]

Aaron Swartz was charged with wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer.[95] The maximum penalty he would have faced under these charges was a fine of $1 million and thirty-five years in prison.[96] However, after over a year of negotiations, prosecutors appeared

84. Scheiber, *supra* note 68.
85. Connor Kirschbaum, *Swartz Indicted for JSTOR Theft*, TECH (Aug. 3, 2011), http://tech.mit.edu/V131/N30/swartz.html. Python is a programming language. A Python script is a computer program. PYTHON, https://www.python.org/ (last visited Apr. 28, 2014).
86. *Id*.
87. *Id*. An IP address is an ephemeral four byte number that uniquely identifies a computer on the Internet, but is subject to frequent change. *RFC 760 DoD Standard: Internet Protocol*, IETF TOOLS, http://tools.ietf.org/html/rfc760#section-3.1 (last visited Apr. 28, 2014).
88. *Id*.
89. *Id*.
90. *Id*. A MAC address is a six byte number that is generally tied to the actual network hardware of a computer. *Id.* It can be changed, but almost never is without a specific technical reason. *Id.*
91. *Id*.
92. *Id*.
93. *Id*.
94. *Id*.
95. Press Release, U.S. Attorney's Office for the Dist. of Mass., *supra* note 1.
96. *Id*.

to have settled on recommending six months in jail as the appropriate penalty.[97]

Nevertheless, on January 11, 2013, Aaron Swartz was found dead in his New York City apartment, the result of an apparent suicide by hanging.[98] He left no note or other indication explaining his reasons, and those reasons may never be known.[99] His family has spoken out and claimed that prosecutorial overreach was at least partly to blame.[100] The prosecutors dispute this claim, but it has nevertheless enraged some parts of the Internet and called for immediate change to the CFAA to eliminate any possibility of another tragedy like Aaron Swartz's happening again.[101]

B. Aaron's Law

On January 16, 2013, Representative Zoe Lofgren posted a draft of a bill she named "Aaron's Law" on Reddit.[102] It is fitting that the bill she proposed in Swartz's name would first be seen on the website Swartz helped to build. Using Reddit as a way to facilitate discussion with the Internet community, Representative Lofgren refined her bill with the Internet's feedback in mind.[103]

Only four double-spaced pages with large font, the changes outlined in Aaron's Law are deceptively simple. At first glance, it merely strikes a few words here and adds some new ones there. The repercussions are many, though, and in addition to perhaps ruling out the possibility of another Swartz-esque scenario playing out, the amendment might also cure the split among the circuits.

---

97. Sam Gustin, *Aaron Swartz, Tech Prodigy and Internet Activist, Is Dead at 26*, TIME (Jan. 13, 2013), http://business.time.com/2013/01/13/tech-prodigy-and-internet-activist-aaron-swartz-commits-suicide/.

98. *Id*.

99. Sam Gustin, *Aaron Swartz's Suicide Prompts MIT Soul-Searching*, TIME (Jan. 14, 2013), http://business.time.com/2013/01/14/mit-orders-review-of-aaron-swartz-suicide-as-soul-searching-begins/.

100. Aaron Ricadela & Dan Hart, *Web Activist's Family Blames MIT, Prosecutors in Death*, BLOOMBERG (Jan. 13, 2013), http://www.bloomberg.com/news/2013-01-12/aaron-swartz-programmer-turned-activist-dies-at-26-nyt-says.html.

101. Marisa Gerber, *'Anonymous' Hacks Government Site to Protest Hacktivist's Death*, L.A. TIMES, Jan. 26, 2013, http://articles.latimes.com/2013/jan/26/nation/la-na-nn-anonymous-hackers-swartz-20130126. Brian Resnick, *How a Martyr Makes a Law*, NAT'L J. (Feb. 6, 2013), http://www.nationaljournal.com/tech/how-a-martyr-makes-a-law-20130206.

102. Zoe Lofgren, *I'm Rep Zoe Lofgren & I'm introducing "Aaron's Law" to Change the Computer Fraud and Abuse Act (CFAA)*, REDDIT (Jan. 16, 2013), http://www.reddit.com/r/technology/comments/16njr9/im_rep_zoe_lofgren_im_introducing_aarons_law_to/.

103. Zoe Lofgren, *I'm Rep Zoe Lofgren, Here is a Modified Draft Version of Aaron's Law Reflecting the Internet's Input*, REDDIT (Feb. 1, 2013), http://www.reddit.com/r/IAmA/comments/17pisv/im_rep_zoe_lofgren_here_is_a_modified_draft/.

Aaron's Law makes a sweeping change to the CFAA by changing the principle of "access."[104] The CFAA, as it currently stands, uses the principle that when a person accesses a computer, his or her access will be considered as in one of three states: within authorized access, exceeding authorized access, or without authorized access.[105] Aaron's Law removes any mention of "exceeding authorized access" and changes the scheme to a dichotomy where a person accessing a computer is either accessing the computer with or without authorization.[106] The person must be accessing the computer without any authorization—at all, under the letter of the amendment—to trigger the CFAA penalties.[107] It goes on to redefine "access without authorization" as obtaining or altering information on a computer, without the authorization to do so, coupled with the circumvention of a technological measure aimed at preventing that information from being obtained or altered.[108] The amendment also specifically excludes violations of agreements, contractual or otherwise, from being considered access without authorization.[109] This amendment represents a move toward a code-based approach in defining what access is illegal under the CFAA. The title of the section of the bill laying out these changes reinforces this idea, as it reads: "Clarifying that violations of 18 U.S.C. 1030 are limited to circumvention of technological barriers in order to gain unauthorized access."[110]

The explicit change in Aaron's Law to a code-based definition of access is unprecedented, but the desire to exempt the mere violation of a website's terms of service as exceeding authorization and thus incurring criminal punishment is not.[111] In the fall of 2011, Senators Al Franken and Chuck Grassley added language preventing agreement violations from being considered unauthorized or excessive access to the Personal Data Privacy and Security Act of 2011, but that bill was never passed.[112]

104. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).
105. 18 U.S.C. § 1030 (2012).
106. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).
107. *Id*. § 2.
108. *Id*. § 2(a).
109. *Id*. § 2.
110. *Id*.
111. Marcia Hofmann, *Senate Committee Agrees That Violating Terms of Service Shouldn't Be a Crime*, ELEC. FRONTIER FOUND. (Sept. 23, 2011), https://www.eff.org/deeplinks/2011/09/senate-committee-agrees-violating-terms-service-shouldnt.
112. S. 1151, 112th Cong. (1st Sess. 2011).

IV. ANALYSIS

With such a diverse array of interpretations in use among the circuits, clarification of the CFAA is clearly needed and Representative Lofgren's bill might be the solution. Aaron's Law is one of the so called "memorial" laws, named after someone who has suffered some treatment that legislators believe should not have happened. Such laws are notorious for being popular but ultimately bad laws because they are drafted in the heat of the moment. The aptly named "Aaron's Law" is the latest attempt to fix the CFAA, promising to bring clarity and uniformity to the CFAA's ambiguous wording. However, while it is an improvement, it ultimately falls short of being the computer crime law this nation deserves.

A. The Programmer's "Words" Are More Valued Than The Lawyer's Words

On February 19, 2013, Professor Lawrence Lessig gave a talk at Harvard University entitled "Aaron's Laws—Law and Justice in the Digital Age."[113] In that talk, he reasoned that because Aaron's Law requires authorization to be in the form of technological measures, a vastly higher value is placed on the speech of a programmer than on a lawyer.[114] "Disagree with the coder and you go to jail. Disagree with the lawyer and you're just laughed at."[115]

The approach in Aaron's Law parallels the path taken by the Fourth and Ninth Circuits in that the owner of a computer may no longer give out fine-grained authorization, allowing only certain types of alterations or access to data for certain reasons. It is all or nothing: either users can access the computer or users cannot access the computer. Any purpose users employ that computer for is irrelevant. Aaron's Law allows the computer owner to police access with technological measures, but this is insufficient because it is impossible to express a wide range of necessary restrictions in computer-manageable form.

Specifically, consider the Internet phenomenon of blogging. In many cases, the most successful blogs are multi-author, where many authors all contribute articles to the same blog. It is necessary for each of those authors to have access to the blog to create their articles. They are given access so that they may add relevant content to the blog to keep its readers informed and entertained. Under Aaron's Law, any such author would be

113. Lawrence Lessig, *Aaron's Laws—Law and Justice in the Digital Age*, YOUTUBE (Feb. 20, 2013), http://www.youtube.com/watch?v=9HAw1i4gOU4.

114. *Id*.

115. *Id*.

free to deface the website however he wanted and be untouched by CFAA penalties because he was given access to that website and it was only the programming that could control his authorization, not any contract. The malevolent author might delete the blog's content or add new, obscene content. Such actions are not what was intended of the owner, and under the CFAA, as it now stands, it would be illegal under the agency-based and possibly contract-based interpretations. Aaron's Law would allow such actions to go unpunished, leaving the blog owner with only potentially expensive and impractical civil remedies. Effectively, the blog owner is left without the means to limit the authorization he gives to that author. He must rely on trust, not the law.

Compare that situation to something more physical. Suppose a computer technician is given access to a computer in a medical setting. He is given access to make repairs to that computer and thus has the ability to run it and test it. Under Aaron's Law, because he had access, he would be free to do whatever he wished on the computer, including browse private patient information. In this scenario, he would be unstopped by technological restrictions because there would be none in order to facilitate his service.

In both of these scenarios, the aggrieved parties may employ civil actions, such as breach of contract and copyright violation, for remedies. These sorts of remedies may serve to deter such conduct, but in many cases, such as those involving contracts, deterrence is not a principle considered in the remedy. Although the CFAA was enacted with the goal of extending new remedies to people affected by computer misuse that did not have remedies under existing civil law, the criminal penalties were enacted solely to deter computer misuse.[116] This deterrence aspect of the CFAA is one of its fundamental problems because it so broadly covers many innocent Internet activities. Aaron's Law "fixes" that by ripping a huge chunk from the scope of conduct covered by the CFAA; that is, any conduct not violating a technological measure designed to police use. In fact, the last statute enacted covering such a broad range of computer crimes was the CFAA itself. The same broad range of problems facing the CFAA can thus be expected to come up in a post-Aaron's Law world.

116. Kerr, s*upra*, note 17.

B. Aaron's Law Does Not Fix the Fundamental Flaws of the Computer Fraud and Abuse Act

The CFAA has been criticized over and over again in legal scholarship.[117] The primary criticism leveled against it is overbreadth.[118] Aaron's Law will roll back the statute's coverage, and for that alone it is a step in the right direction. A better statute, though, would be one that does not rely on the crude language of the CFAA.

For instance, consider the computer technician servicing a computer in a physician's office. Under the CFAA as it stands, he might face charges of exceeding his authorization or perhaps acting without it. These charges would be useless additions to the HIPAA charges he would already be facing for accessing private electronic patient data. For many crimes punishable under the CFAA as it stands, there are additional charges already out there that speak more closely to the actual crime committed. This situation occurs over and over again with a myriad set of possible computer misconduct.

The difficult question comes when conduct which is popularly viewed as misconduct by ordinary persons is, upon closer examination, actually beneficial conduct that ought to be encouraged. Consider the case of Andrew Auernheimer, recently sentenced to forty-one months for violating the CFAA.[119] The government contends he stole 114,000 email addresses of new iPad owners from AT&T's servers.[120] The facts of that case illustrate perfectly how the CFAA, despite its supposed purpose, is not designed nor equipped to deal with the Internet. AT&T set up web servers which connected iPad identification numbers (IDs) with the user's email addresses.[121] When the URL associated with an iPad ID was requested, the AT&T server would return the email address.[122] There was no password requested and the only form of verification required was that the browser

---

117. *See* Kerr, *supra* note 13; Kerr, *supra* note 17; Hernacki, *supra* note 28; Goldman, *supra* note 25; David Rosen, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access,"* 27 B. TECH. L. J. 737 (2012).

118. *See* Kerr, *supra* note 13, at 1572.

119. Orin Kerr, United States v. Auernheimer, *and Why I Am Representing Auernheimer Pro Bono on Appeal Before the Third Circuit*, VOLOKH CONSPIRACY (Mar. 21, 2013, 6:13 PM), http://www.volokh.com/2013/03/21/united-states-v-auernheimer-and-why-i-am-representing-auernheimer-pro-bono-on-appeal-before-the-third-circuit/.

120. *Id*.

121. United States v. Auernheimer, No. 11-cr-470(SDW), 2012 WL 5389142 (D.N.J. Oct. 26, 2012).

122. *Id*. Internet browsers commonly identify themselves by sending user agent strings to the server. This helps websites identify characteristics about their audience such as browser version, operating system, etc. and assists them in tailoring their website to the requirements of the systems their visitors use. User agent strings are configurable in almost every browser though and there is nothing illegal about changing them.

pass a user agent string identifying it as an iPad.[123] Perhaps AT&T believed it could rely on the cryptic iPad IDs to provide security through obscurity, but they still effectively published the email/ID pairs on the World Wide Web, without restriction. What Auernheimer did was merely notice that AT&T did this, and then write a program to repeatedly send requests to the publicly available URLs with slightly different parameters.

That this behavior, simply sending a request to a server and having it respond over the Internet, could possibly be illegal defies all logic. Some have called what Auernhemier did "hacking." Computer hacking, though, is just the use of technical knowledge to manipulate computers to enable them to be used to reach the user's desired end. Put another way, this is exactly what lawyers do: use technical legal knowledge to manipulate the words of a law in a way that enables that law to be used to reach the lawyer's desired end. Whether you are manipulating the bytes in a user agent string, or manipulating the meaning of "exceeds authorization," the only difference is the domain of knowledge being employed. If recognizing that a server, publicly available on the Internet and responding to requests, will return responses that can in any way be illegal, then surely recognizing that the wording "exceeds authorization" could mean throwing Aaron Swartz in prison for thirty-five years should also be illegal.

The Internet works because all computers use the same technology standards. These standards are like the contracts of the computer world. If you give a computer data in a standard format and way, that computer will act in some predictable way according to the particular standard. Programmers sometimes neglect to account for people breaking the standards, which leads to "hacking." Just like legal contracts, breaking computer standards should not be punished.

Additionally, what Auernheimer did is exactly what every other security researcher on the planet does every day. The researchers explore computers to see what sort of new and interesting things they will do when given unusual information. It is this sort of activity alone that moves the security of our nation's infrastructure forward. Auernheimer is perhaps not the most likeable security research because of his less than reputable antics, and that may have been part of why he was convicted.[124] However, whatever harm he might have done, and whatever harm is actually done by malicious hacking, pales in comparison to the value added to the ecosystem of computer security by such hacking. It is primarily through the activities of ethical "hackers," whether for criminal purposes or commercial research,

123. *Id.*; Ryan Tate, *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*, GAWKER (June 9, 2010), http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed.

124. Andrew Couts, *Andrew Auernheimer is Not Aaron Swartz*, DIGITAL TRENDS (Mar. 21, 2013), http://www.digitaltrends.com/opinion/andrew-auernheimer-weev-is-not-aaron-swartz/.

that our software is made more secure. Thus, our power plants are made more secure and our hospitals are better able to protect private patient information. Each new "hole" found in software and disclosed to the world is one less vulnerability sold on the black market and used to exploit everyday citizens.

In short, the growing number and ridiculousness of prosecutions under the CFAA has proven, and will continue to prove, a hindrance to the goal it purports to advance: preventing harmful computer misuse.

C. "Circumvention of a Technological Measure" Is Not A Meaningful Standard

Aaron's Law hinges on whether a person circumvents a technological measure before making that activity illegal. Does sending an iPad user agent string to a server when not on an iPad constitute circumventing the technological measure employed by the AT&T server? If a website owner puts up a button on his website that says "Click if you are Jack Johnson" and some random Internet user presses it, has the user just circumvented the technological measure of that button?

Aaron's Law probably envisions the circumvention of password prompts as what it really means by "technological measures." The principle behind passwords is merely to ask a user for something only he or she should know, and if he or she actually knows it, then the server will assume the person is the associated user. Thus, passwords are, in essence, just obscure collections of characters. Not all passwords are tied to an individual, though: some passwords are distributed to groups to give the entire group access to some resource. One example is a home or business wireless Internet password. Everyone needing access to the wireless Internet in that location will enter the same password and be granted access to the wireless Internet resource. If the case of Auernheimer is considered in light of Aaron's Law and we assume that his conduct is the type of misuse we want to punish, the question of whether the user agent string may be considered alike to a group password, and thus a technological measure designed to restrict access, arises. Access to the resources managed by AT&T's servers were offered only if a certain user agent string were present, similar to how a generic server offers access to its managed resources only if a specific password is offered.

However, interpreting a user agent string in this way must be analyzed in light of the purpose of a user agent string as outlined in section 14.43 of

the HTTP 1.1 standard in RFC2616.[125] The standard makes it clear that the user agent string is for "statistical purposes, the tracing of protocol violations, and automated recognition of user agents for the sake of tailoring responses to avoid particular user agent limitations."[126] When the protocol drafters wrote that the user agent could be used to tailor responses to avoid limitations of particular users, did they intend that the user agent might be used in the same way as a password? To tailor content to a particular user might mean to send the user on a desktop computer a high resolution image whereas to a mobile phone user with less processing power and bandwidth it might send a lower resolution image. It might be reasonable to construe "tailoring content" as policing the content by treating the user agent string as a password, but the drafters of the HTTP standard treated authorizing users in section 11 of the standard.[127]

In light of the consideration of both of these topics in separate sections, it is clear that the HTTP 1.1 standard drafters did not intend for user agents to be treated as passwords or used for code-based restrictions. Thus, although AT&T employed the HTTP 1.1 protocol and used the user agent string to identify users, that should not be considered a technological restriction of access given the actual technical methods employed.

Furthermore, even though the distinction above is somewhat murky, Aaron's Law expressly does not include "efforts to prevent personal identification of a computer user, or identification of a user's hardware device or software, through a user's real name, personally identifiable information, or software program or hardware device identifier(s)" as violations of code-based restrictions.[128] Thus, given that AT&T employed a feature of the HTTP 1.1 standard designed to identify a user by that user's hardware and software, to be used in connection with that user's iPad ID, in order to personally identify that user through his or her email address, Andrew Auernheimer's conduct would not have violated Aaron's Law. What this means is that despite the fact that AT&T attempted to secure access to the resources managed by its servers by using a code-based restriction, under Aaron's Law, their efforts would not legally qualify as a technological measure designed to police access.

125. *RFC2616 HTTP 1.1, 14.43 User-Agent*, W3, http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html (last visited Apr. 28, 2014).

126. *Id.*

127. *RFC2616 HTTP 1.1, 11 Authorization*, W3, http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html (last visited Apr. 28, 2014).

128. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

D. Public Support

Aaron Swartz's death has prompted considerable public debate and news coverage.[129] The vast majority of this coverage has been positive toward Aaron's Law, with nearly uniform decrial of the CFAA as it stands.[130]

In general, people are concerned with the apparent arbitrariness about the CFAA and the ability to drum up a vast array of charges covering even seemingly innocent activity.[131] This arbitrariness is the focus of many commentators' charges of vagueness and overbreadth.[132] In that light, people's preference for the seemingly more concrete boundaries provided by the code-based authorization concept adopted in Aaron's law makes sense. Instead of facing the worrying prospect of relying on a prosecutor's almost arbitrary decision on whether to prosecute, people would instead have a bright line test by which to determine whether their conduct was illegal or not.

A minority of people are concerned with the limitations of code-based governance of authorization.[133] One particular rejection of code-based authorization reasons that it is inconsistent with trespass law.[134] Specifically, a person who has the consent of the owner of land to use a specific part of that land may not use that consent as a defense to the tort of trespass if they venture onto more land than the owner consented to, even if it is not fenced.[135] Unlike land, however, computers require technical knowledge to operate and maintain. Landowners are not required to have any knowledge about their land other than the extent required to own and operate it. Computer owners, on the other hand, require technical knowledge to own and operate their computers and technical knowledge is especially required to grant others access to them. The illicit accessors themselves must be far more technically knowledgeable than their trespassing counterparts because trespass requires only some sort of transportation, but hacking requires intimate knowledge of computer

129. A search for "Aaron Swartz" on Google News between January 12, 2013 and April 12, 2013 returns three thousand articles. This averages to over thirty-four news articles per day over this ninety-one day period; or one new article every forty-one minutes. This covers only online articles and not TV, newspaper, magazine, or social media discussion.

130. *See* Ryan Grim, *CFAA: Internet Activists Win First-Round Victory In Fight Over Anti-Hacking Law*, HUFFINGTON POST (Apr. 12, 2013), http://www.huffingtonpost.com/2013/04/12/cfaa-internet-activists_n_3068978.html.

131. *Id*.

132. *See* Kerr, *supra* note 13; Hernacki, *supra* note 28.

133. *See* Lessig, *supra* note 113; Hernacki, *supra* note 28, at 29.

134. Hernacki, *supra* note 28, at 29.

135. *Id*.

systems.[136] Furthermore, the decision of which party to punish does not clearly fall onto the unauthorized accessor. In the context of electronic patient information, the maintainers of the records themselves are responsible for the security of their systems and face civil and criminal penalties for inadequate safeguards.[137] This is equivalent to reversing the trespass law above and saying that inadequately fencing one's land would give the trespasser a claim against the owner!

Policing computer misuse is a difficult task for a central government to perform and is best accomplished by allowing computer owners to police their own computers, aided by their software vendors. Time and experience will strengthen computer security naturally and in a way that the public can stomach. If nothing else is clear from the public debate surrounding Aaron's Law, the people clearly want the CFAA's breadth reigned in and the Internet to be allowed to breathe freely, regardless of any hiccups along the way.[138]

V. PROPOSAL

So far, this Comment has detailed the fact that the CFAA does not prevent or deter computer misuse and actually is more likely to punish innocent use of the Internet. Additionally, Aaron's Law, while good law in the sense that it reigns in a terrible one, is wholly inadequate to address the problem of computer misuse. Even its sponsor, Representative Lofgren, admits this much.[139]

The first question which must be asked is: What problem are we facing? In some ways, the problem is similar to that which faced the original drafters of the CFAA: computer hackers causing real financial trouble. Today, however, the problems have taken on the larger scale of international cyber warfare.[140] At the same time, a sprawling domestic industry of computer security research has taken root.[141]

Additionally, in the time since the CFAA was passed, our understanding of computers and computer issues has risen almost as astronomically as computers have proliferated. Legislators have decades of

136. To trespass, one merely needs legs. To hack, one needs to understand all the concepts involved in what they are hacking.

137. 42 U.S.C. § 1320d-6 (2012).

138. *See* Grim, *supra* note 130.

139. Lofgren, *supra* note 103.

140. Kevin Voigt, *Chinese Cyber Attacks on West are Widespread, Experts Say*, CNN (Feb. 1, 2013), http://www.cnn.com/2013/02/01/tech/china-cyber-attacks.

141. *See* DEFCON, https://www.defcon.org/ (last visited Mar. 31, 2014). DefCon is an annual conference for computer security research where computer security is actively discussed by as many as ten thousand "good" and "bad" hackers.

history and experience to call upon when drafting computer legislation. Congress no longer needs to rely on broad language to cover up its poor grasp of computer concepts. Congress has already proven that it can attack computer-specific problems with HIPAA, establishing severe penalties for mishandling electronic patient information.[142] As decried as HIPAA might be, it represents a step in the right direction; that is, enacting legislation not with broad and over-inclusive language that sweeps up ordinary citizens in its giant path, but with narrow and laser-focused precision on the actual issues that affect society as a whole. Such narrow statutes covering actual malicious deeds, not innocent or even questionable, but exploratory Internet behavior, are the future of computer and Internet legislation.

One possible downside of this approach is that the ever-quickening pace of technological advancement will make such narrow statutes obsolete as time moves on, whereas a broader statute might be able to cope with those changes. Nevertheless, the broad language of the CFAA has been roundly derided, and a change is sorely needed. There is a medium between narrow language and broad language that allows statutes to stand the test of time. This medium may be seen in timeless concepts like trespass, theft, and battery. Actual harm results from the commission of any of those misdeeds, and the harm is almost invariably punishable under the narrowly-tailored, yet broad coverage of each. If nothing else, this Comment urges the adoption of statutes that will be as timeless as these principles, which are ingrained in almost every citizen and commonly recognized as a part of justice.

VI. CONCLUSION

The death of Aaron Swartz has ignited a long-overdue public debate on the CFAA. The proposal of Aaron's Law by Representative Zoe Lofgren would improve the CFAA, but only because it essentially neuters its rapidly growing criminal application to ordinary and innocent Internet conduct. Aaron's Law, considered by itself, probably makes the situation worse by adding in a cryptic requirement for technological measures that must now be considered with the still-overbroad authorization language.

If Congress and the nation are serious about reforming the CFAA, it must craft a new statute that deters specific misuse scenarios while fostering the technical exploration of computers and computer security that is necessary to fight the emerging information war. Our children should grow up encouraged to play with the Internet and learn how to harness its power with the technical knowledge that will serve them well in the future.

142. 42 U.S.C. § 1320d-6 (2012).

The government should not continue its self-defeating crackdown on the same people who are finding and reporting the very vulnerabilities in our nation's software that foreign hackers use to steal our intellectual property.