The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare—The Case Against Aaron Swartz and the Need To Reform the CFAA

Sarah A. Constant*

I. INTRODUCTION

The Computer Fraud and Abuse Act (CFAA) has been subjected to numerous revisions and conflicting court interpretations since it was first adopted in 1986. The once-narrow statute has been tweaked and remodeled into an all-encompassing, broad set of provisions that gives federal prosecutors the power to charge unknowing computer users with a federal crime. Despite a few circuits issuing holdings on this broad statute and refusing to expand its reach, some prosecutors still use the CFAA to pile on charges for minor crimes such as breaching a terms of service agreement or making a fake online profile. One victim of this overreaching statute was Aaron Swartz, a hacker who was charged under

 Managing Editor, Volume 16, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2014, Tulane University Law School; B.A. *magna cum laude* 2011, The George Washington University. The author would like to thank her parents and her sister for their love, support, and encouragement. Many thanks as well to the editors and staff of Volume 16 for their hard work and dedication to the Journal.

the CFAA and later committed suicide. The law needs to be changed in order to prevent such a tragedy from occurring again.

This Comment will trace the origins of the CFAA and explore how it developed into such a broad and all-encompassing trap for computer users. I suggest that reform is necessary to prevent extreme prosecutorial discretion under an overly broad statute, and to stop unknowing computer users who breach a contract, a Web site's terms of use, from being charged with a federal crime. I will examine the use of the CFAA to prosecute Aaron Swartz and suggest ways that the statute can be amended to prevent such tragedies from recurring. Lastly, I will present some possible hurdles that need to be overcome before the statute can be amended to protect computer users like Aaron.

II. OVERVIEW OF THE COMPUTER FRAUD AND ABUSE ACT

A. The Original Act and Amendments

Along with the development of the Internet and new technologies came the need for new laws to combat emerging computer crimes.[1] Congress first reacted to this need in October 1984 by passing the Comprehensive Crime Control Act, which included the first ever federal computer crime statute.[2] Congress made it a felony to access classified information on a computer without authorization and made it a misdemeanor to access sensitive information from a financial institution or trespass into a government-operated computer.[3] Thus, instead of adding to already enacted criminal laws, Congress created an entirely new statute, 18 U.S.C. § 1030, to address federal computer crime.[4]

Congress was criticized for making the new statute overly vague and too narrow in the range of potential issues it covered.[5] The statute missed two vital infractions: "(1) the statute did not cover individuals who caused harm with authorized access; and (2) it failed to address access by proxy or a co-conspirator."[6] To fix this problem, Congress continued to investigate computer crimes to determine how to revise the

---

1. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES (2d ed. 2010).

2. *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 1976.

3. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 1, at 1.

4. *Id.*

5. *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003).

6. 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, 1549 (2012).

law.[7] Both the House of Representatives and the Senate held hearings on potential revisions to the bill that eventually concluded with the creation of the Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986 as an amendment to 18 U.S.C. § 1030.[8]

The newly amended statute added three new subsections, and it addressed federalism concerns by limiting federal jurisdiction to crimes involving federal computers or certain financial institutions, or where the crime was interstate in nature.[9] The term used by Congress was a "federal interest computer."[10] The three new prohibited criminal acts were codified at 18 U.S.C. § 1030(a)(4)-(6).[11] Section 1030(a)(4) prohibited unauthorized access with the intent to defraud, which is different from wire fraud or mail fraud by the use of a computer.[12] Section 1030(a)(5) prohibited damaging, altering, or destroying the data of another, thereby causing $1,000 or more in losses, and lastly § 1030(a)(6) made it a crime to traffic in computer passwords.[13] These three new infractions included a mens rea of "intentionally," a higher requirement than the 1984 version's "knowingly," which appeared throughout that statute.[14] The rationale behind the mens rea change was that it would protect those who accidentally stumble upon protected data or access a protected computer from being aggressively prosecuted.[15]

The act was amended three more times from 1988 to 1990 to clarify certain terms. The next notable change came in 1994 with amendments called the Computer Abuse Amendments Act of 1994.[16] These amendments expanded § 1030(a)(5) to create a misdemeanor crime for merely reckless acts.[17] This created a stricter law that criminalized unintentional damage; this was a noteworthy change from the 1984 Act, which only covered "intentionally" committed acts.[18]

Recognizing a growing problem of theft of trade secrets and the importance of trade secrets to the economic health of the country,

---

7. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 1, at 1.
8. *Id.*
9. *Id.* at 1-2.
10. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1565 (2010).
11. 18 U.S.C. § 1030(a)(4)-(6) (2012).
12. *Id.* § 1030(a)(4).
13. *Id.* § 1030(a)(5)-(6).
14. Skibell, *supra* note 5, at 913-14.
15. S. REP. NO. 99-432, at 5-6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483-84.
16. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097.
17. *Id.*
18. *Id.* § 290001(b), 108 Stat. at 2097-98.

Congress passed the Economic Espionage Act of 1996 (EEA), which dramatically expanded the reach of the CFAA.[19] Prior versions of the statute were limited to unauthorized accessing of federally important information or data from financial institutions. The EEA expanded the scope of § 1030(a)(2) to cover obtaining and merely reading "any information of any kind so long as the conduct involved an interstate or foreign communication."[20] The decades-old classification of "federal interest" computers was replaced with a new category of "protected computers." This change meant that obtaining and reading information from any computer "used in or affecting interstate commerce or foreign commerce or communication," not just a computer used by a financial institution or the government, could be a violation of the CFAA.[21] Basically any computer that uses the Internet is used in interstate commerce, so this was a big departure from a "federal interest" computer, "which is one of two or more computers used in committing the offense, not all of which are located in the same State."[22]

B. The CFAA Today

Due to continued growth in technology and hacking abilities, Congress again amended the CFAA in 2008 to combat new offenders. The 2008 amendments:

(1) Removed the requirement from 18 U.S.C. § 1030(a)(2)(C) that information must be stolen through interstate or foreign communication, so the section now covers "information from any protected computer;"[23]
(2) Removed the requirement that in order to be a felony the defendant's action must result in a loss exceeding $5,000 and created a felony where the damage affects ten or more computers;[24]
(3) Expanded § 1030 (a)(7) to criminalize, in addition to threats to cause damage to a computer, threats to steal information, or threats to expose the information to public;
(4) [A]dded § 1030(h)(i)(1) which gave the court a mechanism for confiscating all property used in or derived from the violation of 1030; and

---

19. *Introduction to the Economic Espionage Act*, U.S. DEP'T JUSTICE (Aug. 7, 2013, 2:58 PM), http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01122.htm.
20. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.
21. 18 U.S.C. § 1030(e)(2)(B) (2012).
22. *Id.* § 1030(e)(2)(B).
23. *Id.* § 1030(a)(2)(C).
24. *Id.* § 1030(c)(4)(A)(VI).

> (5) Extended the definition of "protected computer" in 18 U.S.C. § 1030(e)(2) to [fully] be covered by [the] extent of Congress's commerce power by including all computers used in or affecting interstate commerce.[25]

The current version of the CFAA outlaws seven types of criminal activity: (1) obtaining national security information, (2) accessing a computer and obtaining information, (3) trespassing in a government computer, (4) accessing a computer to defraud and obtain value, (5) damaging a protected computer or the data stored within,[26] (6) trafficking in passwords, and (7) committing extortion involving computers.[27]

One of the many problems that courts have with the statute is that the CFAA fails to define certain key terms. The words "access" and "authorization" are left up to interpretation, which has resulted in uncertainty for the judiciary.[28] First, the phrase "without authorization" has caused a division of opinions in the courts. It is easy to define "without authorization" to cover the lack of authorization to access a computer; however, there are instances where someone can have access to a computer, but the courts can consider their conduct acting "without authorization."[29] Some courts have applied these terms to employees who had authorization to access a computer, but used their access in an unauthorized manner,[30] while other courts have concluded that a person who intentionally accesses a computer without authorization is necessarily a person who accesses it without any permission at all.[31]

The CFAA defines "exceeds authorized access" as "access[es] a computer with authorization and [uses] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[32] The Department of Justice instructs that "to prove someone has exceeded authorized access, prosecutors should be prepared to present evidence showing (a) how much the person's authority to obtain

---

25. *Id.* § 1030(3)(2); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 1, at 2.

26. *See* 18 U.S.C. § 1030(a)(5)(A)-(C) (including intentionally damaging by knowing transmission, recklessly damaging by intentional access, and negligently causing damage and loss by intentional access).

27. *See id.* § 1030.

28. *Id.*

29. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 1, at 6.

30. *See* United States v. John, 597 F.3d 263, 270-73 (5th Cir. 2010); Shurgard Storage Ctrs. v. Safeguard Self Storage, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

31. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (opining that authorization does not cease when the user acts contrary to the interests of the authorizing party).

32. 18 U.S.C. § 1030(e)(6).

or alter information on the computer was limited, rather than absolute, and (b) how the person exceeded those limitations in obtaining or altering information."[33]

III. RECENT COURT DECISIONS INTERPRETING THE CFAA

A. Defining "Authorization"

Courts are divided on interpretations of the term "authorization" under the CFAA. Some circuits have interpreted the CFAA broadly to cover violations of corporate computer use restrictions or violations of the duty of loyalty.[34] These courts are of the opinion that misuse or misappropriation of information means the user did not have authorized access.[35] Interpreting the CFAA narrowly, other circuits have chosen only to target the unauthorized procurement of information, not its misuse.[36]

The United States Court of Appeals for the Fifth Circuit in *United States v. John* examined whether someone who was authorized to access a computer exceeded their authorized access under the CFAA.[37] Here, an employee at a financial institution accessed account information and passed it on to others who incurred fraudulent charges.[38] The question was whether "authorized access" may include limits placed on the use of information obtained by permitted access to the computer system.[39] The court ruled that the defendant exceeded authorization when she accessed information in order to use it in a fraudulent scheme, which she knew or should have known was beyond her authorized access.[40]

The United States Court of Appeals for the Seventh Circuit has also defined the limits of authorization, finding that an employee's violation of his employment agreement terminated his authorization to use his company laptop.[41] The court used agency principles and held that the defendant breached his duty of loyalty to the employer by deleting evidence that he had started a competing company in violation of his

---

33. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 1, at 8.

34. *See* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

35. *Rodriguez*, 627 F.3d at 1258; *Citrin*, 440 F.3d at 418.

36. *See* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 39 F. Supp. 2d 479, 499 (D. Md. 2005).

37. 597 F.3d 263, 270-73 (5th Cir. 2010).

38. *Id.* at 269.

39. *Id.* at 271.

40. *Id.* at 272-73.

41. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 418 (7th Cir. 2006).

employment contract.[42] Once the defendant had breached his duty of loyalty, he no longer had the authority to access the information.[43]

The United States Court of Appeals for the Ninth Circuit has held the opposing view in two recent cases, holding that once a user has authorization, they cannot be charged for accessing "without authorization" merely because their actions went beyond the scope intended by the provider. In *LVRC Holdings LLC v. Brekka*, the court held that the employee, who e-mailed himself confidential information for the purpose of using it to compete with his employer after termination, had the authorization to access the computer merely because his job required him to use it.[44] The court explained that "without authorization" means "without permission," reasoning that expanding the definition further would be crossing into the territory of "exceeds authorized access" under the CFAA. The court upheld this view again in *United States v. Nosal*.[45] In *Nosal*, a former employee was prosecuted for persuading current employees to access the company's database, in violation of computer-use policies, in order to benefit his competing company.[46] Here, the Ninth Circuit, sitting en banc, held that "exceeds authorized access" is limited to *access* restrictions, not *use* restrictions, under the CFAA.[47]

B. Terms of Service Violations

Due to the failure of the legislature and the courts to clearly explain the phrases "access a computer without authorization" and "exceed authorization," the government has had a generous amount of leeway to be creative in bringing charges.[48] Prosecutors have gone so far as to argue that a violation of a Web site's terms of service is a criminal violation under the CFAA.[49] This is a dangerous leap that gives the

---

42. *Id.* at 420.
43. *Id.*
44. 581 F.3d 1127, 1132-33 (9th Cir. 2009).
45. 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, No. 10-10038, 2012 WL 1176119, at *7 (9th Cir. Apr. 10, 2012).
46. *Id.* at 782.
47. United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).
48. *See* 18 U.S.C § 1030 (2012); Marcia Hoffman & Rainey Reitman, *Rebooting Computer Crime Law Part 1: No Prison Time for Violating Terms of Service*, DEEPLINKS BLOG (Feb. 4, 2013), https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service.
49. *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

government too much power to prosecute mere contract violations under a federal criminal statute.[50]

A Web site's terms of service are a legal contract between the Web site and the user.[51] The courts will recognize a Web site's terms of service as a legally binding contract and will enforce the terms that can limit a Web site owner's legal liability.[52] Most users do not read a Web site's terms of service before accepting them, so they are unaware of the legal rights they are giving up and bestowing.[53] This creates a problem if prosecutors want to bring criminal charges under the CFAA for terms of service violations.

The issue of whether an intentional breach of a Web site's user agreement is enough to be a violation of the CFAA was recently examined in *United States v. Drew*.[54] In this case, Lori Drew was charged with violating § 1030(a)(2)(C) and § 1030(c)(2)(B)(iii), "which prohibit accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involved an interstate foreign communication and the offense is committed in furtherance of a crime or tortious act."[55] Drew had made a fictitious profile on MySpace.com, posing as a sixteen-year-old boy named Josh Evans;[56] posted a photo of the boy without his knowledge; and begun to send Megan Meier, her daughter's classmate, flirtatious messages from the fictitious account.[57] Making a fake profile was a direct violation of MySpace's terms of service.[58] On October 16, 2006, Drew had "Josh" tell Megan that he no longer liked her and that the "world would be a better place without her in it."[59] Later that same day, Megan committed suicide.[60]

The court examined Drew's violation of the terms of service under the CFAA and determined, "[T]here is nothing in the way that the undefined words 'authorization' and 'authorized' are used in the CFAA

---

50. *Computer Fraud and Abuse Act (CFAA)—Internet Law Treatise*, ELEC. FRONTIER FOUND. (Jan. 24, 2013), https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA).

51. Jill Hubbard, *Website Legal Issues: Why Your Terms of Use May Be Critical*, IP LAW FOR STARTUPS (May 26, 2011), http://www.iplawforstartups.com/website-legal-issues-why-your-terms-of-use-may-be-critical/.

52. *Id.*

53. *See id.*

54. 259 F.R.D. 449 (C.D. Cal. 2009).

55. *Id.* at 452.

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

(or from the CFAA's legislative history) which indicates that Congress intended for them to have specialized meanings."[61] Therefore, the court concluded that an "intentional breach of the MSTOS [MySpace Terms of Service] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute."[62] However, the court went on to say that the pivotal issue was whether basing a § 1030(a)(2)(C) violation upon the conscious violation of a Web site's terms of service is permitted under the void-for-vagueness doctrine.[63] The court concluded that the statute, applied in this way, is void for vagueness because of the absence of minimal guidelines to guide law enforcement and the lack of actual notice to the user that there are potential criminal penalties for breaching the contract.[64] The CFAA does not state or even suggest that it has criminalized breaches of contract in the context of a Web site's terms of service.[65] As a result, the court granted the defendant's motion for judgment of acquittal.[66]

In *Nosal*, Judge Alex Kozinski of the Ninth Circuit addressed the problem of allowing prosecutors to use the CFAA to make anyone a federal criminal who violates a Web site's terms of service.[67] He said, "Under the Government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."[68] The Electronic Frontier Foundation later echoed this concern, listing on their Web site the following activities that would be criminalized under the government's interpretation of the CFAA: "lying about your age on Facebook," "letting a friend log into your Pandora account," "posting impolite comments on the New York Time's website," and "sending a sexy message on eHarmony."[69] The decision in *Nosal* resulted in a split with three other circuits, raising the possibility that the issue will one day reach the United States Supreme Court.[70]

---

61. *Id.* at 461.
62. *Id.*
63. *Id.* at 464.
64. *Id.*
65. *Id.*
66. *Id.* at 468.
67. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).
68. *Id.* at 862.
69. Hoffman & Reitman, *supra* note 48.
70. Debra Cassens Weiss, *9th Circuit Narrows Computer Fraud Law, Protecting Lying Homely People and Web-Surfing Workers*, ABA J. (Apr. 11, 2012), http://www.abajournal.com/news/article/9th_circuit_narrows_computer_fraud_law_protecting_lying_homely_people_and_w/.

IV. THE CASE AGAINST AARON SWARTZ

Aaron Swartz was a prodigy and an activist who contributed to many technological projects throughout his short life.[71] He committed suicide in early 2013 while he was facing serious criminal charges in federal court.[72] However, Aaron's legacy, the work he did, and the cause he fought for still live on. At the young age of fourteen, Aaron was part of the team that created RSS, or Rich Site Summary, the Web-content syndication protocol that is used by millions of Web sites.[73] He was also an early employee of Reddit, a social news site, and he founded the reformist activist group DemandProgess.[74]

Aaron firmly believed in freedom of information and was widely praised for his efforts to make online information free for all users.[75] In 2008, he wrote a manifesto entitled the "Guerilla Open Access Manifesto."[76] The manifesto said that it was a "moral imperative" to allow open sharing of information and spoke harshly against the "privatization of knowledge."[77] Aaron wrote: "We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive."[78] He believed that academic journals had privatized knowledge and that corporations who were "blinded by greed" were preventing others from accessing educational information.[79] This manifesto was later used by the Justice Department in Aaron's criminal proceedings to demonstrate that he had "malicious intent in downloading documents on a massive scale."[80]

Aaron's first run-in with the law happened in 2008 with the PACER effort.[81] Public Access to Court Electronic Records (PACER) is the

---

71. Patrick Lambert, *The Case Against Aaron Swartz: Why We Should Be Concerned*, TECHREPUBLIC (Jan. 29, 2013, 6:00 AM), http://www.techrepublic.com/blog/security/the-case-against-aaron-swartz-why-we-should-be-concerned/8980.

72. *Id.*

73. Nancy Sims, *Library Licensing and Criminal Law: The Aaron Swartz Case*, 72 C&RL NEWS 534, 534-37 (2011), *available at* http://crln.acrl.org/content/72/9/534.full.pdf+html.

74. *Id.*

75. Gerry Smith, *Were the Charges Against Internet Activist Aaron Swartz Too Severe?*, HUFFINGTON POST (Jan. 13, 2012, 11:02 AM), http://www.huffingtonpost.com/2013/01/13/aaron-swartz-death-_n_2468879.html.

76. 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.

77. *Id.*

78. *Id.*

79. *See id.*

80. *Id.*

81. Lambert, *supra* note 71.

computer system that holds all federal court documents, which are available to access after paying a fee.[82] Because these are public documents, Aaron felt that they should be free to access.[83] Aaron purchased access to the system and released for free 18 million documents (20% of the database).[84] The FBI investigated, but charges were never brought because Aaron did not actually break a law.[85]

However, the next time Aaron decided to carry out a massive download, he did not get away unscathed. In July 2011, Aaron was indicted on federal charges of computer fraud and unlawfully obtaining information from a protected computer by illegally accessing JSTOR, a subscription-only service that provides access to academic articles.[86] The indictment alleged that "between September 24, 2010 and January 6, 2011, [Aaron] contrived to: (a) break into a restricted wiring closet at MIT [the Massachusetts Institute of Technology,] (b) access MIT's network without authorization," (c) connect to JSTOR through MIT's network, (d) download a large amount of JSTOR's archive onto his computers and hard drives, (e) avoid MIT's and JSTOR's efforts to stop him, and (f) elude detection and identification.[87] In the end, Aaron had managed to download around 4.8 million articles and faced thirteen felony counts that carry penalties of up to thirty-five years in prison and $1 million in fines.[88]

A. How Did Aaron Carry Out His Crime?

First, Aaron purchased a new Acer laptop and connected it to MIT's computer network using the fictitious name "Gary Host."[89] He also made a throwaway e-mail address, addressghost@mailinator.com.[90] Then Aaron began to rapidly download volumes from JSTOR using a software program called "Keepgrabbing.py" that automated the downloading and sidestepped any efforts by JSTOR to stop it.[91] JSTOR took actions to

---

82. PACER, http://www.pacer.com (last visited Sept. 24, 2013).
83. Lambert, *supra* note 71.
84. *Id.*
85. *Id.*
86. *See* Swartz Indictment, United States v. Aaron Swartz, Crim. No. 11-cr-10260 (D. Mass. July 14, 2011), http://www.documentcloud.org/documents/217117-united-states-of-america-v-aaron-swartz.
87. *Id.* at 3.
88. *See* 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?ref=technology.
89. Swartz Indictment, *supra* note 86, at 4.
90. *Id.*
91. *Id.* at 9.

stop Aaron's computer by blocking his Internet protocol (IP) address.[92] Every computer connected to the Internet is assigned an IP address so that the Internet traffic sent from and to that computer can be directed to the proper destination.[93] So when JSTOR blocked his original IP address, Aaron simply obtained a new one and continued to download articles.[94]

JSTOR then contacted MIT, which decided to prevent the Acer laptop from being assigned an IP address on its network by blocking its MAC address.[95] A MAC address is a unique number assigned to a computer, often assigned by the manufacturer and generally remaining constant on the machine.[96] However, a user with the knowledge to do so can change the MAC address on their computer; so, on October 2, 2010, Aaron connected to MIT's network using another MAC address.[97] Over the next few weeks, Aaron returned a few times to the MIT closet where he was stationed and changed his MAC address yet again.[98]

In the end, Aaron had stolen 4.8 million articles, of which approximately 1.7 million had been made available by independent publishers for purchase on JSTOR.[99] Aaron did not hack into the network to download these articles, and he did not crack any passwords to get into JSTOR's system. All Aaron did was figure out how JSTOR filed certain articles he wanted and write a script that would gather those articles and copy them onto his hard drive.[100]

B. Did the Punishment Fit the Crime?

Even though Aaron turned over all of the hard drives with the 4.8 million documents, and JSTOR and MIT refused to pursue the case and press civil charges—JSTOR even opened its archives and made 1200 journals free for reading after the incident, showing that they were not against Aaron[101]—the United States Attorney's office pressed on.[102] U.S. Attorney Carmen M. Ortiz said, "[S]tealing is stealing, whether you use a computer command or a crowbar, and whether you take documents, data

92. *Id.* at 5.
93. *Id.*
94. *Id.*
95. *Id.* at 6.
96. *Id.*
97. *Id.*
98. *Id.* at 6-9.
99. *Id.* at 9.
100. Lawrence Lessig, *A Law for Aaron Swartz*, NAT'L J. (Jan. 17, 2013, 10:31 AM), http://www.nationaljournal.com/domesticpolicy/a-law-for-aaron-swartz-20130117.
101. Schwartz, *supra* note 88.
102. *Id.*

or dollars."[103] She referred to stealing even though Aaron was indicted on fraud charges.[104]

Prosecutors charged Aaron with wire fraud and computer fraud under the CFAA, and he faced thirty-five years in prison for his crimes.[105] He was offered a plea bargain early in the case that would have given him a three-month sentence in exchange for a guilty plea, but Aaron would not take it.[106] Here, the prosecution did not waiver and used the terms of use that MIT created for its users and those that JSTOR created and MIT accepted as the basis for criminal prosecutions.[107] Breaching terms of service on a Web site usually results in being banned from the site, not jail time.[108] This is why prosecutors focused on the fact that Aaron used fake names and IP addresses to hide his identity in order to add wire and computer fraud charges.[109]

Changing a MAC address is a very trivial task. TechRepublic's Patrick Lambert explains, "Many adapters offer the option right on their configuration screen, and in Windows you simply have to click a few buttons to access it."[110] The same is true for changing an IP address; anyone can configure their adaptor to use any address they want as long as the router accepts it.[111] "So," says Lambert, "the idea that changing your MAC or IP address equals to computer or wire fraud is very scary, since those are not authentication mechanisms; there is no security behind them."[112] This is why names, passwords, digital signatures, and public key cryptography are often used for authentication.[113]

There was a lot of backlash against U.S. Attorney Ortiz for bringing charges with such harsh penalties against Aaron—there was even an online petition with 35,000 signatures asking President Obama to remove her from office[114]—but the Department of Justice believes the federal prosecutors acted reasonably.[115] The DOJ says the prosecutors were motivated by the desire to deter others from committing similar

---

103. *Id.*
104. *See id.*; Swartz Indictment, *supra* note 86.
105. Schwartz, *supra* note 88.
106. Reilly, *supra* note 76.
107. Sims, *supra* note 73.
108. Lambert, *supra* note 71.
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*
114. Declan McCullagh, *Prosecutor in Aaron Schwartz 'Hacking' Case Comes Under Fire*, CNET (Jan. 15, 2013, 11:59 PM), http://news.cnet.com/8301-13578_3-57564212-38/prosecutor-in-aaron-swartz-hacking-case-comes-under-fire/.
115. *See* Reilly, *supra* note 76.

offenses.[116] Prosecutors said that Swartz's "Manifesto" made it clear that he intended to share the articles with the public at large.[117] However, not everyone agrees that the prosecutors acted reasonably. House Oversight Committee Chairman Darrell Issa (R-Calif.) launched an investigation into Aaron's prosecution,[118] and Representative Jared Polis (D-Colo.) said: "The charges were ridiculous and trumped-up. It's absurd that he was made a scapegoat."[119]

V. PROPOSED CHANGES TO THE CFAA

Aaron's untimely death was the spark that started the fire of a much needed movement toward, and discussion about, making changes to the CFAA. Four days after Aaron's death, Representative Zoe Lofgren (D-Calif.) announced on Reddit (a Web site cofounded by Aaron) that she would propose a number of changes to the CFAA.[120] Representative Lofgren said, "As we mourn Aaron Swartz's death, many of us are deeply troubled as we learn more about the government's actions against him,"[121] and there is "no way to reverse the tragedy of Aaron's death, but we can work to prevent a repeat of the abuses of power he experienced."[122]

Representative Lofgrens's first draft, which was released on January 15 on Reddit, amended the statute so that a contractual violation would not be a crime under the CFAA.[123] It was a step in the right direction, but many familiar with the CFAA thought that this amendment was not enough. Tor Ekeland, a lawyer for convicted hacker Andrew Auernheimer, said, "Amending the definition of unauthorized access to exclude [terms of service] violations is just putting a band aid on a gaping, gushing wound."[124]

After receiving feedback from Reddit followers and other organizations, Representative Lofgren released a revised draft on January

---

116. *Id.*

117. *Id.*

118. McCullagh, *supra* note 114.

119. *Id.*

120. *Congresswoman Introduces 'Aaron's Law' To Honor Swartz*, RT (Jan. 16, 2013, 9:15 PM), http://rt.com/usa/swartz-cfaa-aaron-law-148/.

121. *Id.*

122. *Id.*

123. *See* ZoeLofgren, *Hi I'm Rep Zoe Lofgren & I'm Introducing "Aaron's Law" Change the Computer Fraud and Abuse Act (CFAA)*, REDDIT (Jan. 15, 2013), http://www.reddit.com/r/technology/comments/16njr9/im_rep_zoe_lofgren_im_introducing_aarons_law_to/.

124. Andy Greenberg, *'Aaron's Law' Suggests Reforms to Computer Fraud Act (But Not Enough To Have Protected Aaron Swartz)*, FORBES (Jan. 16, 2013, 8:58 PM), http://www.forbes.com/sites/andygreenberg/2013/01/16/aarons-law-suggests-reforms-to-hacking-acts-but-not-enough-to-have-protected-aaron-swartz/.

30.[125] The bill, called "Aaron's law," would limit the scope of the CFAA and exclude crimes that are nothing more than a breach of a contract, such as a terms of service agreement.[126] It also specifies that efforts to prevent personal identification of a computer user (i.e., changing a MAC address) are not a violation of the CFAA.[127] Representative Lofgren says that these changes, though minor, could make a huge difference in how prosecutors use the CFAA and could help avoid another tragedy.[128] However, some say that Representative Lofgren's attempt is still not enough to make sure that what happened to Aaron will not happen again.[129]

The Electronic Frontier Foundation (EFF), a nonprofit that fights for digital rights, released a memo with suggestions for updating the CFAA on their Web site in reaction to Representative Lofgren's first proposed amendment, in addition to some new ideas that could be added to the amendment in the near future.[130] The EFF would like to ensure that when a user breaks a contract, such as a terms of service agreement, the government cannot charge them under the CFAA.[131] This change would just be reinforcing circuit court decisions that were made in the United States Courts of Appeals for the Fourth and Ninth Circuits, but that did not reach where Aaron was charged, in the First Circuit.[132] The EFF also made two proposals in its memo that were not included in Representative Lofgren's "Aaron's Law." First, they suggested clarifying the term "unauthorized access" and getting rid of the term "exceeds authorized access,"[133] arguing that there needs to be a definition that encompasses all of the conduct that is considered "unauthorized."[134] Their proposed amendment is as follows:

---

125. Zach Walton, *Rep. Zoe Lofgren Publishes Revised Aaron's Law After Receiving Input from Reddit*, WEBPRONEWS (Feb. 1, 2013), http://www.webpronews.com/rep-zoe-lofgren-publishes-revised-aarons-law-after-receiving-input-from-reddit-2013-02.

126. Rep. Zoe Lofgren, *Aaron's Law Discussion Draft*, WIRED (Jan. 30, 2013), http://www.wired.com/images_blogs/threatlevel/2013/02/Aarons-Law_revised-draft.pdf.

127. *Id.*

128. *Congresswoman Introduces 'Aaron's Law' To Honor Swartz*, *supra* note 120.

129. *Id.*

130. Cindy Cohn, Mark Jaycox & Marcia Hofmann, *EFF's Initial Improvements to Aaron's Law for Computer Crime Reform*, ELEC. FRONTIER FOUND. (Jan. 17, 2013), https://www.eff.org/deeplinks/2013/01/effs-initial-improvements-aarons-law-computer-crime-reform.

131. *Id.*

132. *Id.*; *see* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

133. Cindy Cohn & Marcia Hofmann, *Part 2: EFF's Additional Improvements to Aaron's Law*, ELEC. FRONTIER FOUND. (Jan. 23, 2013), https://www.eff.org/deeplinks/2013/01/part-2-effs-additional-improvements-aarons-law.

134. *Id.*

> The term "access without authorization" means to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to access the computer, file, or data, but does not include circumventing a technological measure that does not effectively control access to a computer, file, or data.[135]

Next, the EFF proposed major changes to the penalties in the CFAA. They would like to remove 18 U.S.C. § 1030 (a)(3) and (a)(4) because they are repetitious of other parts of the law, and this gives prosecutors power to add more charges for the same behavior.[136] They also would like to remove the provision of the CFAA that allows for civil causes of action, because the claims are often redundant of other causes of action, and removing them could prevent civil court cases from creating precedent for CFAA criminal cases.[137]

Marcia Hofmann, the attorney with the EFF who wrote these suggestions, also said, "[A]ny reform to the CFAA should also address the difference between data theft for profit versus a more benign hack like [Aaron's] that had no such motive."[138] Aaron was charged with a felony because he stole information worth more than $5,000; however, he never intended to sell the documents and make a profit.[139] Hoffman said: "He wasn't stealing this information to sell trade secrets or sell credit histories. This was an act of civil disobedience,"[140] and there "needs to be a safety valve in the law that at least recognizes that."[141]

VI. POTENTIAL HURDLES IN THE WAY OF REFORM

Despite the momentum for reform following Aaron's death, there is still a long road ahead for Representative Lofgren and her suggested amendments.[142] The White House and the DOJ have both been silent on the issue.[143] Supporters of Aaron's law tried to appeal to the Obama Administration through an online petition entitled, "We the People," but

---

135. *Explanation of Effects of Aaron's Law with EFF Proposed Amendments to "Access Without Authorization,"* ELEC. FRONTIER FOUND. (Jan. 23, 2013), https://www.eff.org/document/eff-explanation-access-amendments.

136. Cohn, Jaycox & Hoffman, *supra* note 130; *see also* 18 U.S.C. § 1030 (2012).

137. Cohn, Jaycox & Hoffman, *supra* note 130.

138. Greenberg, *supra* note 124.

139. *Id.*

140. *Id.*

141. *Id.*

142. Tony Romm, *After Activist Aaron Swartz's Death, a Tough Slog for Aaron's Law*, POLITICO (Feb. 8, 2013), http://www.politico.com/story/2013/02/activist-aaron-swartz-death-aarons-law-87332.html.

143. *Id.*

the White House has yet to respond.[144] However, appealing to the President may not be very helpful in this situation.[145] Presidents change periodically, and so do their positions.[146] Most noteworthy is the fact that the Obama Administration tried to expand the CFAA as a part of its 2011 proposal on cybersecurity reform.[147]

The DOJ, too, wants to expand the CFAA and increase some penalties under the law. In 2011, DOJ lawyers told Capitol Hill that they "didn't support any revision to the law that would have clarified what constitutes unauthorized access."[148] This is the part of the law that allows the government to prosecute those individuals who merely violate a Web site's terms of service agreement.[149] In Congress, the bill has a number of influential backers, but in the House and in the Senate, members are more preoccupied with immigration reform and gun control.[150]

However, in the House, Representative Issa, Chairman of the House Oversight and Government Reform Committee, and ranking minority leader Elijah Cummings (D-Md.) recently sent a letter to the DOJ inquiring about the charges against Aaron.[151] They specified in their letter, "It appears that prosecutors increased the felony counts by providing specific dates for each action, turning each marked date into its own felony charge, and significantly increasing [Aaron's] maximum criminal exposure to up to 50 years imprisonment and $1 million in fines."[152] The lawmakers are worried about the zealous prosecutions under the CFAA.[153] However, lawmakers in general refrain from acting in a way that may cause them to be accused of being soft on crime.[154] Also, lawmakers' propensity for vagueness in laws may be warranted because "it gives the people who carry out enforcement and make regulations the ability to adjust to changing circumstances."[155] Except, in the case of the

---

144. *Id.*

145. Dan Gillmor, *Is the Computer Fraud and Abuse Act the 'Worst Law in Technology'?*, GUARDIAN (Mar. 20, 2013, 11:17 AM), http://www.guardian.co.uk/commentisfree/2013/mar/20/computer-fraud-abuse-act-law-technology.

146. *Id.*

147. Romm, *supra* note 142.

148. *Id.*

149. *Id.*

150. *Aaron's Law Faces UpHill Battle*, BRIEF (Feb. 14, 2013), http://thebrief.io/news/aarons-law-faces-uphill-battle.

151. Kim Zetter, '*Aaron's Law' Proposes Reining in Federal Anti-Hacking Statute*, WIRED (Feb. 1, 2013, 5:51 PM), http://www.wired.com/threatlevel/2013/02/aarons-law-amending-the-cfaa/.

152. *Id.*

153. *Id.*

154. Gillmor, *supra* note 145.

155. *Id.*

CFAA, where there is obvious abuse by the DOJ, there needs to be specific reform that clarifies the law.[156] Representative Lofgren has not formally introduced her amendments in Congress yet, but when she does, there will hopefully be much support from her colleagues.[157]

VII. CONCLUSION

Since the CFAA's inception in 1986, Congress has amended it multiple times to make it the ultimate catchall for computer infractions. This broad statute gives prosecutors the power to pile charges onto unsuspecting Internet and computer users. The law needs to be amended with more specific provisions so that there is not another tragedy like Aaron's. The words "access" and "authorization" left undefined have resulted in an overreaching statute that needs to be limited.[158] Aaron was a victim of a broad statute, extreme prosecutorial discretion, and the prosecutors' desire to make an example of him for all hackers.[159] Representative Lofgren's "Aaron's Law" is a step in the right direction, but there needs to be more support in the government in order for any real change to occur.[160] The Fourth and the Ninth Circuits have already decided to limit the scope of the CFAA in those jurisdictions.[161] Maybe one day soon, the Supreme Court will take up this issue and decide to limit the scope of the CFAA nationally. Right now, it is a waiting game to see who acts first, Congress or the courts, but, regardless, there must be change soon, or else another innocent, young computer user may be at risk of facing severe criminal charges.

---

156. *Id.*
157. Romm, *supra* note 142.
158. *See* 18 U.S.C. § 1030 (2012).
159. Reilly, *supra* note 76.
160. *Congresswoman Introduces "Aaron's Law" To Honor Swartz*, *supra* note 120.
161. *See* WEC Carolina Energy Solutions LLC v. Willie Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).