The CFAA and Aaron's Law

by James Juo

The Computer Fraud and Abuse Act (CFAA) is a computer trespass statute that has been called "one of the broadest federal criminal laws currently on the books."[1] Congress enacted the CFAA in 1984 to criminalize the hacking of computers in connection with national security, financial records, and government property.[2] But the CFAA has been expanded a number of times since then.[3] For example, in 1994 the statute was expanded to allow private entities to assert a civil cause of action and obtain compensatory damages.[4] In 1996, the CFAA was further amended to expand the class of protected computers to include any computer "used in interstate or foreign commerce or communication."[5] In the space of a dozen years, the scope of this criminal statute has gone from a limited set of protected computers to possibly every computer in the United States connected to the Internet.[6]

The CFAA prohibits "access without authorization" and "exceed[ing] authorized access" to a protected computer.[7] But the CFAA has been called "remarkably vague" on this point.[8]

The Story of Aaron Swartz

Calls to reform the CFAA have increased significantly after the tragic death of Aaron Swartz.

At age 14, Aaron was working with leading technologists to craft open standards such as the Really Simple Syndication specification for sharing information on the Internet.[9] He then helped Lawrence Lessig with Creative Commons, a company that promotes the use of simple, standardized copyright licenses that give the public permission to share and use creative works.[10] At age 19, Swartz was a founding developer of Reddit, a widely-used social news website where users can post news links and vote on them.[11] Swartz later became a political activist for Internet freedom and social justice issues, and formed the advocacy group Demand Progress.[12]

In late 2010, Swartz allegedly attempted to access and rapidly download a large number of academic articles from JSTOR (or Journal Storage), a nonprofit organization that provides a searchable database of digitized articles archived from academic journals.[13] Libraries and universities pay a subscription fee for access to JSTOR, where its Terms of Service prohibit downloading or exporting documents from JSTOR using automated computer programs.[14] JSTOR also uses technical measures to prevent such automated downloading.[15]

JSTOR declined to pursue legal action against Swartz after he turned over his hard drives which contained 4.8 million JSTOR documents.[16] But the federal government charged Swartz with violations of the CFAA.[17]

A computer expert for the defense asserts that Swartz did not "hack" the JSTOR website under any reasonable definition — Swartz did not use parameter tampering, break a CAPTCHA gate, or do anything more complicated than automate a process that downloads a file in the same manner as clicking "Save As" from a browser.[18] Whether this defense would have been successful is questionable because the CFAA prohibits more than just traditional hacking.

With criminal charges hanging over him for a year-and-a-half, Swartz was offered a plea bargain requiring a felony conviction, under which the government would recommend a six-month prison term (although his defense counsel could argue to the judge for probation instead).[19] The government would not back off its demand for jail time.[20] Faced with this dilemma, at age 26, Swartz took his own life in January 2013.[21]

Aaron's Law

In the wake of Swartz's death, there have been several proposals to amend the CFAA. In June 2013, Rep. Zoe Lofgren, D-CA, introduced a bill titled "Aaron's Law Act of 2013" to reform the CFAA.[22] The bill would eliminate the "exceeds authorized access" language from the statute and define "access without authorization" to mean obtaining information on a protected computer that the accesser lacks authorization to obtain by circumventing one or more technological measures that exclude or prevent unauthorized individuals from obtaining or altering that information.[23] "The proposed changes make clear that the CFAA does not outlaw mere violations of terms of service," but would prohibit "bypassing technological or physical measures via deception (as in the case with phishing or social engineering), and scenarios in which an authorized individual provides a means to circumvent to an unauthorized individual (i.e., sharing login credentials)."[24]

Notwithstanding the bipartisan support of Rep. Darrell Issa, R-CA, and Sen. Ron Wyden, D-OR, it may be a lengthy political journey for these legislative proposals.[25] Congress rarely scales back criminal laws," according to Tim Wu, a professor at Columbia Law School.[26] Proposals to narrow the scope of a criminal statute often also include provisions for increased penalties to avoid a soft-on-crime label.[27] "To be successful, (the effort to pass Aaron's Law) will likely take substantial time and require sustained and intense support from all of you," according to Lofgren.[28] Time will

tell whether momentum will be sustained for Aaron's Law to become law.

Endnotes:

1 Paul J. Larkin Jr., "United States v. Nosal: Rebooting the Computer Fraud and Abuse Act," 8 SETON HALL CIR. REV. 257, 261 (2012); *see also* Jennifer Granick, "Towards Learning from Losing Aaron Swartz," THE CENTER FOR INTERNET AND SOCIETY (Jan.14, 2013, 4:37 PM), https://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz. ("Another way to look at the CFAA, is that it protects the box").

2 Technically speaking, the CFAA was a 1986 amendment to 18 U.S.C. § 1030, but the common convention is to refer to Section 1030 as a whole as the CFAA. Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," 94 MINN. L. REV. 1561, 1561 n.2 (2012). The original 1984 statute was called the Comprehensive Crime Control Act (CCCA). *Id*. at 1563-64.

3 *Id.* at 1566.

4 *Id*. (citing 18 U.S.C. § 1030(g)).

5 *Id*. at 1567–68 (citing 18 U.S.C. § 1030(e)(2)).

6 *Id*. at 1571 ("Perhaps the only identifiable exclusion from the scope of protected computers is a 'portable hand held calculator.'")

7 See 18 U.S.C. § 1030(a)(2); *see also* Jennifer Granick, "Thoughts on Orin Kerr's CFAA Reform Proposals: A Great Second Step," The Center for Internet and Society (Jan. 23, 2013, 9:43 PM), https://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step ("Historically, the CFAA partitioned the world of computer criminals into two camps, outsiders who 'access without authorization' and wayward insiders who abuse their position of trust to 'exceed authorized access' and obtain information they were not entitled to.")

8 "Investigating and Prosecuting 21st Century Cyber Threats: Hearing Before United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations," 113th Cong. 1 (Mar. 13, 2013) (written statement of Orin S. Kerr, Fred C. Stevenson Research Prof., George Washington Univ. Law School), *available at* http://www.volokh.com/wp-content/uploads/2013/03/KerrCFAATestimony2013.pdf.

9 Tim Carmody, "Memory to Myth: Tracing Aaron Swartz Through the 21st Century," THE VERGE (Jan. 22, 2013, 12:30 PM), http://www.theverge.com/2013/1/22/3898584/aaron-swartz-profile-memory-to-myth.

10 Lawrence Lessig, "Prosecutor as Bully," LESSIG BLOG, V2 (Jan. 12, 2013), http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully.

11 Larissa MacFarquhar, "Requiem for a Dream," THE NEW YORKER (Mar. 11, 2013), http://nyr.kr/ZUnMMv.

12 *See also* Justin Peters, "The Idealist: Aaron Swartz Wanted To Save the World. Why Couldn't He Save Himself?" SLATE (Feb. 7, 2013, 9:47 PM), http://slate.me/YevwGC.

13 Superseding Indictment at 1, *United States v. Swartz*, No. 11-cr-10260, Dkt. No. 53 (D. Mass. Sept. 12, 2012).

14 *Id*. at 2. The subscription fees are shared with the publishers who hold the original copyrights. *Id*.

15 *Id*.

16 *See* Lessig, *supra* note 10 ("JSTOR figured 'appropriate' out: They declined to pursue their own action against Aaron, and they asked the government to drop its.")

17 Press Release, United States Attorney's Office for the District of Massachusetts, "Alleged Hacker Charged with Stealing Over Four Million Documents from MIT Network" (July 19, 2011), http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html.

18 Alex Stamos, "The Truth About Aaron Swartz's 'Crime,'" UNHANDLED EXCEPTION (Jan. 12, 2013), http://unhandled.com/2013/01/12/the-truth-about-aaron-swartzs-crime/.

19 MacFarquhar, *supra* note 11; *see also* Jennifer Granick, "Towards Learning From Losing Aaron Swartz: Part 2," The Center for Internet and Society (Jan.15, 2013, 3:54 PM), https://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2 (discussing the "great practical risk" in pleading to a felony).

20 Peters, *supra* note 12; *see also* Lessig, *supra* note 2 ("[T]he question this government needs to answer is why it was so necessary that Aaron Swartz be labeled a 'felon.' For in the 18 months of negotiations, that was what he was not willing to accept.")

21 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?_r=0.

22 Proposed "Aaron's Law Act of 2013," *available at* http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20-%20lofgren%20-%20061913.pdf.

23 *Id*.

24 Section-by-Section Summary, *available at* http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20summary%20-%20lofgren%20-%20061913.pdf.

25 Tony Romm, "After Activist Aaron Swartz's Death, a Tough Slog for Aaron's Law," POLITICO (Feb. 8, 2013, 4:48 AM), http://politi.co/XVjnau.

26 Tim Wu, "Fixing the Worst Law in Technology," THE NEW YORKER NEWS DESK (Mar. 18, 2013), http://nyr.kr/YCubsS.

27 *See* Orin Kerr, "Recent Developments — Both in the Courts and in Congress — on the Scope of the Computer Fraud and Abuse Act," THE VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), 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/.

28 Romm, *supra* note 25.

James Juo is a partner at Fulwider Patton LLP, a Los Angeles law firm specializing in intellectual property including patents and trademarks. He is a registered patent attorney and holds a B.S. in electrical engineering. He previously worked as a patent examiner at the United States Patent and Trademark Office. He received his J.D. from George Washington University. He may be contacted at jjuo@fulpat.com.