Andrew Brinker

Professor Boland

English 240

10 April 2013

Aaron's Law and Personal Liberties in the Modern Age

Abstract

The Computer Fraud and Abuse Act of 1984 has struggled to keep pace with technology, giving broad powers to corporations to write federal law. In *US v. Aaron Swartz* an activist was faced with 35 years in prison under the CFAA for downloading too many academic articles. He killed himself. Now a bill dubbed "Aaron's Law" will amend the CFAA, limit these powers, and protect people's right to use technology. In this paper I discuss this bill, the CFAA, and personal liberties in the modern age.

Introduction

The Computer Fraud and Abuse Act of 1984 (18 USC § 1030) instituted a collection of reforms intended to criminalize certain computer-related activities, defining as a federal crime any action which exceeded "authorized access" on a "protected computer". The internet became publicly available with the decommissioning of NSFNET in 1995, and in the years since then the CFAA has been modified and applied by US courts to cases involving the internet.

In US v. Aaron Swartz, Mr. Swartz was prosecuted by the US Attorney's Office for violations of several CFAA clauses, specifically those relating to exceeding authorized access. In this case, Mr. Swartz accessed an MIT network switch from a closet at MIT, where Swartz was a research fellow. From that closet he downloaded a large number of articles from the journal

repository JSTOR, avoiding attempts by the MIT system administrators to block his connection. He was apprehended and charged with fifteen felonies and misdemeanors, thirteen of which were violations of the CFAA (Superceding Indictment).

On January 11th, after learning that the US Attorney's Office would not accept a plea agreement in his case, Mr. Swartz killed himself.

In the time since Swartz's suicide, proposals have been discussed that would reform the CFAA to limit the abilities of corporations to define “authorized access”, to protect the rights and abilities of security researchers, news organizations, and entrepreneurs, and to bring the CFAA's punishments in line with the severity of the crimes being punished. One such proposal is a bill dubbed “Aaron's Law”, proposed by Representative Zoe Lofgren of California, that would amend the CFAA to decriminalize the violation of a website's fine print usage agreement (Lofgren).

In this paper I discuss the legal history of the Computer Fraud and Abuse Act, the potential effects of Aaron's Law, and the legislation’s path to passage.

Background

The CFAA defines a “protected computer” as any computer used for a financial institution, the United States government, or “interstate or foreign commerce or communication”. At the time of the bill's passage, before the advent of widespread internet availability, this meant computers owned and operated by the government, banks, and large businesses. With the arrival of the internet, which allows connection of a user's computer to a page of code hosted on another computer, the issue of whether unauthorized access of a website constituted a violation of the CFAA became pertinent. In *U.S. v. Drew, 259 F.R.D. 449 (2009)* federal prosecutors argued that

such access did constitute a violation, as it met the three standards put forth by the CFAA, namely that (1) the defendant accessed the computer intentionally either without authorization or exceeding authorization; (2) the access of the computer involved interstate or foreign commerce or communication; (3) the defendant obtained, during this access, information from the computer involved in interstate or foreign commerce or communication. In this case the judge agreed that standards (2) and (3) were met, but questioned whether the violation of the terms of service of a website (in this case http://www.myspace.com) constituted intentionally accessing a protected computer either beyond or without authorization. He found that if such a violation did meet standard (1), then any violation of the terms of service of a website could meet that standard, thus rendering the statute overboard and invalidating it on grounds of vagueness. However, he did not state that a violation of the terms of service of a website did not meet standard (1), instead merely stating that without the users of said site being adequately informed of the contents of the agreement and made adequately aware of the consequences of a violation of that agreement, the issue of whether a breach of authorized access would be intentional was too vague. This left the issue at hand incompletely addressed.

In *SCEA v. Hotz*, Sony Computer Entertainment of America sued programmer George Hotz for violation of the end-user license agreement of his PlayStation 3, citing section (a)(2)(c) of the Computer Fraud and Abuse Act, which states that any individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains… information from a protected computer" shall be punished with "a fine under this title or imprisonment for not more than ten years" (S, Ben).

In this case, Mr. Hotz, a security researcher, was sued by Sony for his successful

jailbreaking of their PlayStation 3 product. “Jailbreaking”, also known as “privilege escalation” is defined as “modify[ing] the firmware of an electronic device, especially a mobile phone, in order to remove restrictions that prevent it from running unofficial software” (Jailbreak). In the case of Mr. Hotz, he was the first known individual to successfully gain system-level access to a PlayStation 3 and therefore have full privileges to modify the system as desired. After discovery of the method used to obtain this access Mr. Hotz published directions on his personal website, allowing others to give themselves the same level of access he had obtained.

Sony sued Mr. Hotz and others associated with him, claiming that his act of gaining root access on a PlayStation 3 constituted a violation of the CFAA clause prohibiting accessing a protected computer beyond or without authorization (Sony Computer Entertainment). In this case, Sony argued that the PlayStation 3 met the standards needed for a protected computer because it was sold across state lines and facilitated interstate and foreign commerce and communication, allowing users both to purchase content from remote servers and to communicate with other players worldwide. The PlayStation 3's end-user license agreement (EULA) stated: “SCE [(Sony Computer Entertainment)] does not grant any license to System Software obtained by users in any manner other than through SCE's authorized distribution methods” (System Software License Agreement). This made the accessing and modification of system software a violation of the EULA, as the user did not have any license or easement to allow access to such software.

The issue at hand with the CFAA claims in *SCEA v. Hotz* was whether violating the EULA of a PlayStation 3 constituted a crime. Many organizations and activists published articles in support of Mr. Hotz, and challenged Sony's legal reasoning in their claim against him. As

stated by the Electronic Frontier Foundation, a non-profit that provides legal support in cases relating to personal liberties and technology, “Sony is sending another dangerous message: that it has rights in the computer it sells you even after you buy it, and therefore can decide whether your tinkering with that computer is legal or not” (McSherry, Hoffman).

In this case, Mr. Hotz settled out of court with Sony (Gilbert). The settlement, which included a legally binding agreement not to use Sony products, also included a requirement that Hotz take no part in further research into security vulnerabilities in Sony products, placing him under a gag order for any and all information related to Sony. This gag order, which is in effect whether that information is obtained legally or illegally, was disconcerting to the EFF, who stated “Hotz has agreed to do more than simply avoid hacking any Sony products; he has agreed not to even link to anyone else’s research on Sony products, or to share any Sony confidential information he might receive, even if he obtains it legally. In other words, Hotz is now under a gag order” (McSherry, Corynne). Because the case was settled out of court, and because of the gag order placed on Mr. Hotz, the issue of whether his violation of the PS3's EULA constituted a criminal violation of the CFAA went unanswered. However, it did raise an important issue. Namely that even the ability of companies like Sony to threaten criminal penalties for violating the limits they place on their products seriously stifles the efforts of security researchers like Mr. Hotz. It also left several legal questions unanswered, including (1) what limitations, if any, exist on a company's ability to limit use of their product; (2) what makes the repurposing of a computer a more serious crime than the repurposing of another object; (3) what standards should be put in place to define what can or can't be included within a terms of service agreement; (4) at what point is a terms of service agreement considered to be overreaching and thus invalid? All of

these unanswered questions left open the possibility of a case like that of Aaron Swartz.

Aaron Swartz was a writer, programmer, and activist. At the age of fifteen he was a contributor to the Rich Site Summary ("RSS") specification, which allowed for the syndication of content from the website so it could be accessed without accessing the site directly. (Swartz, Aaron "Aaron Swartz"). He also was one of two creators of the Markdown markup language, used for writing documents that could be easily translated into HTML ("HyperText Markup Language"), the major language for defining the structure of a webpage. He also authored the web.py framework, and became an early and important staff member of the popular internet site Reddit. After Reddit was purchased by Wired Magazine, a subsidiary of Conde Nast, Swartz founded Watchdog.net, and soon after Demand Progress, both of which are internet organizations focused on activism related to technology and personal liberties.

In late 2010 to early 2011, Aaron Swartz was a research fellow at the Massachusetts Institute of Technology. While at the university, he used MIT's internet network to access the journal repository JSTOR, downloading a large number of articles (Jay). On at least one of these occasions he accessed the network through a network switch in a closet, and throughout his access he avoided attempts by the university to block his connection using a method known as MAC address spoofing. Mr. Swartz's actions were done with the intention of making all articles downloaded from JSTOR available free to the public. As stated by Swartz in his "Guerrilla Open Access Manifesto": "The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers" (Swartz, Aaron "Full Text"). The act was

therefore an act of political activism, and political speech.

Because of these events, Mr. Swartz was arrested by MIT police and a member of the Secret Service, and charged with breaking and entering with intention to commit a felony (MIT Crime Club). Proceedings on these charges went on for several months until his case was handed over to the US Attorney's Office, who dropped the original charges and charged him with fifteen violations of federal statutes, specifically those related to the CFAA and the Digital Millennium Copyright Act. During the criminal proceedings, JSTOR stated they had no intention of pursuing civil charges against Mr. Swartz (JSTOR Statement).

Between the fifteen charges, Mr. Swartz faced up to thirty-five years in prison. According to statements made by Andy Good, Swartz's initial attorney in this case, Swartz was a suicide risk, and the US Attorney's Office was made aware of this. It is stated by Good that the US Attorney's Office offered to have Swartz locked in a holding cell so long as he was a risk to himself, but this offer was refused (Cullen).

Soon after this incident, on January 11th, 2013, Mr. Swartz committed suicide. The US Attorney's Office then dropped the charges against Mr. Swartz, stating that they never “intended to seek maximum penalties under the law” (Smith-Spark).

In the wake of his suicide, many legal experts, activists, and civil liberties advocates began to question the US Attorney's actions in this case. It also led many to question the charges that had been brought against him. One of the charges, which carried a potential sentence of ten years in prison, was that he had knowingly violated JSTOR's terms of service agreement, and therefore illegally accessed a protected computer in violation of the CFAA.

Aaron's Law was proposed soon after Aaron Swartz's suicide, with the intention of

modifying the CFAA to decriminalize the violation of a website's terms of service agreement. The law has gone through several drafts, with input from organizations like the Electronic Frontier Foundation, and is currently being finalized for introduction into the US House of Representatives.

Discussion

The largest issue with the Computer Fraud and Abuse Act is the over-broad definition of "protected computer". By defining as a protected computer any and all machines involved in finance, government operations, or foreign and interstate commerce or communication, the law makes nearly all computers protected. This effect is something that may not have been anticipated or intended by Congress when passing the law, as the internet was not yet available to the public, and would not become so for another eleven years (the law was passed in 1984 and the internet gained widespread availability in 1995). Before the advent of the internet many computers were not able to engage in interstate or foreign commerce or communication, and thus did not qualify as protected computers. However, post-internet almost all computers can engage in interstate or foreign commerce or communication; visiting a website often involves a connection across a state or national border; using a service like Skype involves communicating using servers that may be in another state or country; and so on and so forth. The end result of this fact is that nearly every internet-connected computer meets the CFAA's standards of "protected computer".

When nearly any computer can be considered a protected computer under the CFAA, the actions of many individuals can be considered criminal. Consider, for example, a security researcher who is investigating a method for gaining system level access on a smartphone. Under

the CFAA and associated case law if the smartphone has the ability to engage in computation and logic operations it qualifies as a computer, and if it is used for interstate or foreign commerce or communication (which, being a phone, it almost certainly is) it is a protected computer. So, the actions of the security researcher, even if they are done with no intention of exploitation for monetary gain, merely for an academic understanding of the vulnerabilities of the phone's particular system architecture, may qualify as a criminal violation of the CFAA's clauses banning an individual from exceeding authorized access on a protected computer.

Imagine then that the security researcher, concerned about the legal implications of his actions under the CFAA, decides not to investigate this particular phone, and so fails to discover a vulnerability he would have otherwise discovered. Then, some time later, a malicious hacker, not concerned with the implications of the CFAA, discovers that vulnerability and exploits it for monetary gain. Because the researcher did not discover the vulnerability, no papers have been published on it, thus slowing the response of software developers who must now determine how the attack was done and seal the security hole. Had the attack vector been discovered by a researcher instead of a malicious hacker, it could have been reported to the appropriate developers and corrected before being exploited in the wild. In this case, the end result of the CFAA's clauses is a decrease in computer security and a serious limitation for security researchers.

Consider another case: a programmer is developing a program to let you view the content from your favorite social networking sites in one place, so that instead of having to login to each individually you can log into one place and get the content you want. If any of the websites' terms of service agreements have a clause prohibiting the redisplaying of content, this program

would be in violation of the CFAA. The social networks could then sue the programmer, or worse, pursue him with criminal charges of knowingly exceeding authorized access on a protected computer (after all, his program used the Application Programming Interface (API) of the services to access remote servers and gain information from them). His innovative and potentially very useful service would then be shut down, innovation stifled by the statutes of the CFAA.

Similar laws, for example the Digital Millennium Copyright Act, have clauses that allow for certain fair-use cases related to the accessing of certain computers (Digital Millennium Copyright Act). For example, under the DMCA, anti-circumvention provisions in software are not permitted if they would block an individual from building an interoperable program. The DMCA recognizes that such anti-circumvention provisions are an anti-competitive practice, and therefore does not allow them.

However, the CFAA does not have any similar provisions limiting the ability of corporations to define how their devices are used. In the case of *SCEA v. Hotz*, Sony had no real limitations in what they could define as “authorized access”, and the actions of the security researcher George Hotz were thus criminal because they consisted of gaining system access on a device manufactured by Sony that Sony had placed limits on. Without limits on the ability of corporations to control use of their devices post-sale, corporations are given broad powers to abuse the legal system to gag security researchers from publishing about problems with their systems (like the case of Mr. Hotz) and to stop individuals from using the hardware they have purchased, thus requiring them to, for example, purchase software from the Sony provided store instead of purchasing elsewhere and installing directly. These are anti-competitive practices that

should be limited under the CFAA, but currently aren't.

The end effect for consumers is that they are in essence renting, not purchasing, the electronic devices they pay for. If you buy a PlayStation 3 but are not allowed to modify it, can you truly be said to own it? Furthermore, because of the limits on security researchers, consumers are made less safe. Researchers can't research security holes on devices if the company doesn't want them to, and so these security holes are more likely to be discovered by malicious hackers who will exploit them for monetary gain. Finally, because of the way it stifles innovations, consumers are kept from enjoying potentially wonderful products at the bleeding edge of technology.

It is unacceptable for companies to wield the power they currently wield under the CFAA. Aaron's Law, with its modification of the CFAA to decriminalize violations of a terms of service agreement, helps protect all individuals who use and create technology, and helps foster innovation in an important and quickly growing marketplace.

The issue now is how to get Aaron's Law passed. It is a difficult prospect. At the same time as some lawmakers are trying to get a final draft of Aaron's Law written so it can be voted on, others are pushing a series of reforms designed to strengthen and harshen the limits and penalties of the CFAA. To combat this, organizations like the EFF, Demand Progress, Fight for the Future, BoingBoing, FreePress, and Reddit are organizing an internet protest against expansion of the CFAA (Demand Justice). These efforts are designed to spread publish awareness about the issue of the CFAA, and to encourage voters to contact their representatives and voice their support of Aaron's Law, and their opposition to the potential CFAA expansion.

These tactics, of a simultaneous public awareness campaign and public political

lobbying, are the best options right now to help get Aaron's Law passed. Given that there are lawmakers pushing for expansion to the CFAA, it will be difficult to get Aaron's Law passed without strong public support. Such support is possible though.

When SOPA was coming up for a vote in 2012, hundreds of websites blacked themselves out in protest, and the public awareness campaign helped sway political will and stop SOPA from passing. An event of similar magnitude may be necessary for the issue of CFAA reform, and such an event is possible.

Conclusion

Aaron's Law represents a much-needed reform to the Computer Fraud and Abuse Act of 1984. It will help protected consumers, security researchers, and anyone else who uses modern technology. The legal history of the CFAA, particularly related to terms of service agreements, has inadequately addressed the issue, and the current situation is untenable. The passage of Aaron's Law is needed to clarify the law, and limit the ability of corporations to write federal law. The path to passage for Aaron's Law is difficult, and currently faces a collective of lawmakers who want to strengthen the CFAA, not weaken it as Aaron's Law does. In order to pass Aaron's Law, a large public awareness and advocacy campaign is needed, potentially on the same order of magnitude as the campaign organized against SOPA last year. Such a campaign will take a large amount of effort, but it is possible that within the next year Aaron's Law or a similar reform will be passed. The CFAA cannot stand as it is, and change can happen soon.

Works Cited

"18 USC § 1030 - Fraud and Related Activity in Connection with Computers." *Cornel University Law School Legal Information Institute*. Cornel University Law School, n.d. Web. 09

Apr. 2013.

"Superceding Indictment, United States of America v. Aaron Swartz." *Archive.org*. Archive.org, n.d. Web. 9 Apr. 2013. <http://ia700504.us.archive.org/29/items/gov.uscourts.mad.137971/gov.uscourts.mad.137971.53.0.pdf>.

Lofgren, Zoe. "I'm Rep Zoe Lofgren & I'm Introducing "Aaron's Law" to Change the Computer Fraud and Abuse Act (CFAA)." *I'm Rep Zoe Lofgren & I'm Introducing "Aaron's Law" to Change the Computer Fraud and Abuse Act (CFAA) :*. Reddit, 15 Jan. 2013. Web. 09 Apr. 2013. <http://www.reddit.com/r/technology/comments/16njr9/im_rep_zoe_lofgren_im_introducing_aarons_law_to/>.

"US v. Drew." *Scribd*. Scribd, 29 July 2011. Web. 9 Apr. 2013. <http://www.scribd.com/doc/61217247/US-v-Drew-aug-29-2009#fullscreen>.

S, Ben. "Yale Law & Technology." *Yale Law Technology*. Yale Law Technology, 1 Mar. 2011. Web. 09 Apr. 2013. <http://www.yalelawtech.org/trusted-computing-drm/46-dc-ea-d3-17-fe-45-d8-09-23-eb-97-e4-95-64-10-d4-cd-b2-c2/>.

"Jailbreak." *Wiktionary*. Wiktionary, n.d. Web. 09 Apr. 2013. <https://en.wiktionary.org/wiki/jailbreak>.

"SYSTEM SOFTWARE LICENSE AGREEMENT (Version 1.4) FOR THE PlayStation®3 SYSTEM." *SYSTEM SOFTWARE LICENSE AGREEMENT (Version 1.4) FOR THE PlayStation®3 SYSTEM*. Sony Computer Entertainment, 10 Dec. 2009. Web. 09 Apr. 2013.

Sony Computer Entertainment America. "Complaint." *Scribd*. Scribd, 1 Dec. 2011. Web. 09 Apr. 2013. <http://www.scribd.com/doc/46739943/Complaint>.

McSherry, Corynne, and Marcia Hoffman. "Sony v. Hotz: Sony Sends A Dangerous Message to Researchers -- and Its Customers | Electronic Frontier Foundation." *Electronic Frontier Foundation*. Electronic Frontier Foundation, 19 Jan. 2011. Web. 09 Apr. 2013.

Gilbert, Ben. "Sony and PlayStation 3 Jailbreaker George Hotz Settle out of Court." *Joystiq*. Joystiq, 11 Apr. 2011. Web. 09 Apr. 2013.

McSherry, Corynne. "Sony v. Hotz Ends With a Whimper, I Mean a Gag Order | Electronic Frontier Foundation." *Electronic Frontier Foundation*. Electronic Frontier Foundation, 12 Apr. 2011. Web. 09 Apr. 2013.

Swartz, Aaron. "Aaron Swartz." *Aaron Swartz*. Aaron Swartz, n.d. Web. 09 Apr. 2013.

Jay, Lindsay. "Feds: Harvard Fellow Hacked Millions of Papers." *Yahoo! News*. Yahoo!, 19 July 2011. Web. 09 Apr. 2013.

Swartz, Aaron. "Full Text of "Guerrilla Open Access Manifesto"" *Full Text of "Guerilla Open Access Manifesto"* Archive.org, July 2008. Web. 09 Apr. 2013.

"MIT Crime Club Report, December 15th to January 20th." *MIT Crime Club*. MIT Crime Club, n.d. Web. 9 Apr. 2013. <http://mitcrimeclub.org/11pologDec15Jan20.pdf>.

"JSTOR Statement: Misuse Incident and Criminal Case." *JSTOR*. JSTOR, 2011. Web. 09 Apr. 2013.

Cullen, Kevin. "On Humanity, a Big Failure in Aaron Swartz Case." *BostonGlobe.com*. The Boston Globe, 15 Jan. 2013. Web. 09 Apr. 2013.

Smith-Spark, Laura, and Marina Carver. "Prosecutor Defends Case against Aaron Swartz." *CNN*. Cable News Network, 18 Jan. 2013. Web. 09 Apr. 2013.

"Digital Millennium Copyright Act of 1998." *Copyright.gov*. Copyright.gov, n.d. Web. 9 Apr.

2013.

"Demand Justice for Aaron Swartz." *Fix the CFAA*. Fix the CFAA, n.d. Web. 09 Apr. 2013.