Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 24, *Issue* 4 2015 *Article* 6

VOLUME XXIV BOOK 4

Faith and Martyrdom: The Tragedy of Aaron Swartz

Austin C. Murnane*

*Fordham University School of Law

Faith and Martyrdom: The Tragedy of Aaron Swartz

Austin C. Murnane*

"[A]nd if you will not tell of his martyrdom, tell at least of his faith."
-Oscar Wilde, The Portrait of Mr. W. H. (1889)

INTRODUCTION

On January 11, 2013, Taren Stinebrickner-Kauffman found her partner, Aaron Swartz, hanging in the couple's apartment in Brooklyn, New York.[1] Swartz had committed suicide.[2] He was 26 years old.[3]

---

* J.D., 2014, Fordham University School of Law; B.S., 2006, United States Naval Academy. The Author would like to thank the *Fordham Intellectual Property, Media & Entertainment Law Journal* staff, especially Tiffany Mahmood, for their hard work and patience throughout the editorial process.

1 *See, e.g.*, 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; Michael Martinez,

At the age of 14, Swartz had coauthored the programming language specification that came to be known as Rich Site Summary (RSS) 1.0.[4] He also formed his own company, which merged with the news service Reddit, and co-founded the advocacy organization Demand Progress.[5] Despite dropping out of college after deciding that Stanford lacked the intellectual rigor he craved, he earned a position as a fellow at Harvard University's Edmond J. Safra Center for Ethics.[6] But at the time of his death, Swartz was also under federal indictment for wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer.[7]

"He was killed by the government," said Swartz's father, Robert Swartz, at Swartz's funeral.[8] This was one of many accusations leveled against the United States Attorney's Office (USAO) for the District of Massachusetts. The Massachusetts USAO had indicted Swartz for hacking into the non-profit academic journal service JSTOR using an internet connection at the Massachusetts Institute of Technology ("MIT" or "the Institute").[9] At a memorial service for Swartz in March 2013,

---

Internet Prodigy, Activist Aaron Swartz Commits Suicide, CNN (Mar. 7, 2013, 11:41 AM), http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide.

2 *See* Martinez, *supra* note 1.

3 *See* Schwartz, *supra* note 1.

4 *See id*.; *see also* Aaron Swartz, *Request for Comments No. 3870, 'application/rdf+xml' Media Type Registration,* INTERNET SOC'Y NETWORK WORKING GRP. (Sept. 2004), http://tools.ietf.org/html/rfc3870.

5 *See* Schwartz, *supra* note 1; *Aaron Swartz Biography*, HUFFINGTON POST, http://www.huffingtonpost.com/aaron-swartz (last visited Apr. 18, 2014).

6 *See* Schwartz, *supra* note 1; *RSS Creator Aaron Swartz Dead at 26*, HARVARD MAG., Jan. 14, 2013, http://harvardmagazine.com/2013/01/rss-creator-aaron-swartz-dead-at-26.

7 Superseding Indictment of Aaron Swartz at 1, United States v. Swartz, No. 11-CR-10260-NMG, 2012 WL 4341933 (D. Mass. Sept. 12, 2012) [hereinafter Superseding Indictment].

8 Sandra Guy, *Aaron Swartz Was 'Killed by Government,' Father Says at Funeral*, CHICAGO SUN-TIMES, Jan. 15, 2013, www.suntimes.com/business/17594002-420/aaron-swartz-memorialized-at-service.html.

9 Superseding Indictment, *supra* note 7, at 1.

Stinebrickner-Kauffman alleged that the prosecutors had engaged in "malfeasance."[10]

Swartz's supporters further criticized the prosecution. Professor Tim Wu of Columbia Law School described the case against Swartz as a failure of the legal system.[11] Other academics made similar accusations.[12] Swartz received posthumous awards from the American Library Association and the Internet Society.[13] Some fans took more dramatic action, targeting the prosecutors and MIT with hate mail, cyber attacks, and a hoax report of a shooting on the MIT campus.[14]

Swartz's defense attorneys, Elliot R. Peters and Daniel Purcell, wrote a letter to the Office of Professional Responsibility (OPR) at the Massachusetts USAO, accusing Swartz's prosecutors of professional misconduct.[15] Peters and Purcell alleged that prosecutors suppressed exculpatory evidence by failing to disclose information concerning the amount of time the government took to

---

[10] Taren Stinebrickner-Kauffman, *MIT Memorial Service*, TARENSK (Mar. 12, 2013), http://tarensk.tumblr.com/post/45281114505/mit-memorial-service.

[11] *See* Tim Wu, *How the Legal System Failed Aaron Swartz—And Us*, NEW YORKER, Jan. 14, 2013, http://www.newyorker.com/online/blogs/newsdesk/2013/01/everyone-interesting-is-a-felon.html.

[12] *See, e.g.*, David Amsden, *The Brilliant Life and Tragic Death of Aaron Swartz*, ROLLING STONE, Feb. 15, 2013, http://www.rollingstone.com/culture/news/the-brilliant-life-and-tragic-death-of-aaron-swartz-20130215 ("[T]he federal government had . . . been unrelenting in its quest to ensure that his punishment would be severe."); *Transcript: Lawrence Lessig on "Aaron's Laws—Law and Justice in a Digital Age*," CORRENTEWIRE (Mar. 1, 2013, 4:47 PM), http://www.correntewire.com/transcript_lawrence_lessig_on_aarons_laws_law_and_justice_in_a_digital_age [hereinafter *Lessig on Aaron's Laws*] ("Now, you don't need to believe that Aaron was right to see why what the government did here was wrong.").

[13] *See* Keith Michael Fiels, *A Memorial Resolution Honoring Aaron Swartz*, 2013 ALA MEMORIAL #5 (2013); Inductees, Internet Hall of Fame Innovator Aaron Swartz, Posthumous Recipient, THE INTERNET SOCIETY (2013), *available at* http://internethallof fame.org/inductees/aaron-swartz.

[14] *See* Derek J. Anderson, *MIT Gunman Hoax Linked to Aaron Swartz's Suicide, According to Top School Official*, BOSTON GLOBE, Feb. 27, 2013, http://www.boston .com/metrodesk/2013/02/27/mit-gunman-hoax-linked-aaron-swartz-suicide-according-top-school-official/YvOMMxJ81eAbhrz4dTfErN/story.html.

[15] Letter from Elliot R. Peters and Daniel Purcell, Counsel for Aaron Swartz, to Robin C. Ashton, Counsel, Office of Prof'l Responsibility, U.S. Dep't of Justice (Jan. 28, 2013) (on file with author) [hereinafter Peters Letter].

apply for a search warrant on one of Swartz's laptops.[16] They also accused prosecutors of abusing their discretion by offering a plea bargain of less than six months imprisonment, while charging Swartz with crimes that would likely carry seven years in prison if he were convicted.[17]

I. BLAMING THE CFAA

In addition to blaming the Massachusetts USAO, Swartz's supporters also criticized the Computer Fraud and Abuse Act (CFAA)[18]—the law articulating the computer crimes with which Swartz was charged.[19] Critics referred to the law as overbroad, vague, redundant, and an antiquated relic of the 1980s.[20] In response to Swartz's suicide, Congresswoman Zoe Lofgren and Senator Ron Wyden proposed "Aaron's Law," a bill intended to amend and reform the CFAA.[21]

The angry accusations that Swartz's family, friends, and supporters made are completely understandable given the terrible nature of their loss. However, few of these accusations reflect the reality of Swartz's case, intellectual property law, the CFAA, or the interests these laws protect. Although *United States v. Swartz*[22] provides prosecutors, defense attorneys, and intellectual property lawyers with some important lessons, it was not an unethical application of an unjust law.

The tragedy of Aaron Swartz's death should instead remind all attorneys in the criminal justice system of the serious, damaging effects that a criminal prosecution can have on a defendant's mental health. It should inspire prosecutors and defense attorneys alike to consider these health effects with great sensitivity, and

---

16 *Id*. at 1–6.

17 *Id*. at 6.

18 18 U.S.C. § 1030 (2012).

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

20 *Id*.

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

22 945 F. Supp. 2d 216 (D. Mass. 2013).

reach out when necessary to the resources that can alleviate the consequences of depression and related illness. Unfortunately, these lessons, if they have been learned at all, have been overshadowed by other reactions to Swartz's death. In the year since Swartz's suicide, there has been a regrettable lack of initiatives that might prevent the recurrence of such a terrible loss.

II. ARGUMENT/RESOLUTION: THE WRONG LESSONS

Critics of the Swartz prosecution often overlook three important aspects of the case.[23] The first is that Swartz caused real damage to information systems and risked seriously harming interests that deserve protection under the Constitution and as a matter of public policy.[24] The second is that the CFAA, despite its obvious flaws, was well-suited to prevent the serious harm Swartz almost succeeded in committing.[25] Finally, although neither MIT nor JSTOR actively participated in or encouraged the Swartz prosecution, nothing about their actions or inactions indicates that the prosecution itself was unjust.[26]

A. Swartz's Harm

Some critics of the prosecution claimed, after his suicide, that Swartz's actions did not deserve punishment because he had not caused any harm. For example, Columbia Law Professor Tim Wu, writing the day before Swartz's funeral, described Swartz's actions as follows:

> The act was harmless—not in the sense of hypothetical damages or the circular logic of deterrence theory (that's lawyerly logic), but in John Stuart Mill's sense, meaning that there was no actual physical harm, nor actual economic harm.

---

23 *See, e.g.*, Wu, *supra* note 11.
24 *See infra* notes 28–70.
25 *See infra* notes 72–132.
26 *See infra* notes 135–150.

> The leak was found and plugged; JSTOR suffered no actual economic loss.[27]

Wu and others were probably not aware at the time of the funeral of exactly what Swartz had been charged with doing—indeed, what Swartz had admitted doing. Any evaluation of the prosecutors' decisions ought to consider the extent of Swartz's actions against the MIT and JSTOR networks, the interests he threatened, and his intent.

Swartz apparently conducted three distinct series of cyber attacks[28] at MIT during the fall and winter of 2010, when he downloaded approximately 4.7 million copyright-protected academic works.[29] The word "apparently" instead of "allegedly" is used because Swartz himself admitted his responsibility for these downloads in his settlement with JSTOR.[30] At the time of the settlement negotiations, after Swartz's arrest in 2011, JSTOR knew that millions of its articles had been downloaded and was desperately trying to ensure that these copyrighted works would not be released to the public.[31] Swartz sought to alleviate JSTOR's fears by handing over hard drives containing the downloaded articles to the Massachusetts USAO, and by assuring JSTOR that

---

[27] Wu, *supra* note 11; *see also* Amsden, *supra* note 12 ("In actuality, the downloads were at the time something of an afterthought: an extension of Swartz's fascination with large data sets, his perpetual need to juggle multiple experiments at once.").

[28] "Cyber attack" is a term with various definitions. The Bureau of Justice Statistics defines the term as "crimes in which the computer system is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage." *Cybercrime*, BUREAU OF JUSTICE STATISTICS (2005), *available at* http://www.bjs.gov/index.cfm?ty=tp&tid=41. The U.S. National Research Council defines cyber-attacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009). Swartz's actions met both definitions.

[29] *See* HAROLD ABELSON ET AL., TO THE PRESIDENT: MIT AND THE PROSECUTION OF AARON SWARTZ 19–25 (2013) [hereinafter MIT REPORT], *available at* http://swartz-report.mit.edu/docs/report-to-the-president.pdf.

[30] Press Release, JSTOR, Misuse Incident and Criminal Case (July 19, 2011) [hereinafter JSTOR Press Release], *available at* http://about.jstor.org/news/jstor-statement-misuse-incident-and-criminal-case; MIT REPORT, *supra* note 29, at 41.

[31] MIT REPORT, *supra* note 29, at 41.

no other copies existed, because he had downloaded all of the files himself and kept them in his exclusive possession.[32]

Assuming that Swartz's assurances to JSTOR were true, it was he who conducted the first cyber attack on JSTOR on or about September 25, 2010.[33] He entered MIT's campus, where he had never been a student, faculty member, or employee,[34] and connected his computer to the Institute's network.[35] This first action was unremarkable, because MIT at that time maintained an open network that allowed any member of the public to enter the campus, connect to the internet via the Institute's provider, and take advantage of the information resources, including JSTOR, for which the Institute had contracted access.[36] The extent of the public's access to resources like JSTOR was limited, in accordance with contracts that MIT had signed with these content providers.[37] Users could only access a limited number of articles for limited uses—until Aaron Swartz disabled a safeguard in the network.[38]

Specifically, Swartz inserted a line of code, also known as a "flag," that modified the access protocol for JSTOR.[39] The initial access protocol had required that any user requesting to download a JSTOR file from the MIT network would have to manually confirm that user's acceptance of JSTOR's terms of use prior to each download.[40] Simply put, users had to click a box to indicate their agreement prior to each download.[41] JSTOR's terms of service prohibited users from automatically downloading articles

---

32 JSTOR Press Release, *supra* note 30; MIT REPORT, *supra* note 29, at 42.

33 JSTOR Press Release, *supra* note 30; MIT REPORT, *supra* note 29, at 42.

34 *See* Superseding Indictment, *supra* note 7, at 2; MIT REPORT, *supra* note 29, at 52 (The MIT Review Panel noted that, if Aaron Swartz had been formally associated with MIT, the Institute might have been able to lobby against a federal criminal prosecution by informing the USAO that it would handle the matter internally using the Institute's disciplinary system.).

35 *See* MIT REPORT *supra* note 29, at 52; Superseding Indictment, *supra* note 7, at 4.

36 *See* MIT REPORT, *supra* note 29, at 27.

37 *See* Superseding Indictment, *supra* note 7, at 4.

38 *See* MIT REPORT, *supra* note 29, at 16.

39 *See id.*

40 *See id.*

41 *See id.*

in bulk.[42] MIT's terms of service explicitly notified users that misuse of its network or those of content partners like JSTOR could lead to state or federal prosecution.[43] This "click" requirement effectively notified users of the legal limits for downloading and using JSTOR's articles, and prevented those users from quickly downloading a large number of articles.[44]

After neutralizing this safeguard, Swartz's computer was able to run a program that rapidly downloaded thousands of articles.[45] Swartz downloaded so many articles so quickly that his requests overloaded a server at JSTOR.[46] When JSTOR's engineers realized what was going on, they stopped their server from transferring files to the Internet Protocol (IP) address, or the physical terminal at MIT, where Swartz had connected his computer to the network.[47] JSTOR also sent Swartz a message indicating that his downloads exceeded JSTOR's terms of use.[48]

Undeterred, Swartz switched to a different IP address and continued downloading files.[49] Over eleven hours, he managed to

---

42 *Terms and Conditions of Use*, JSTOR, http://www.jstor.org/page/info/about/policies/terms.jsp (last visited Apr. 18, 2014); *see also* Superseding Indictment, *supra* note 7, at 2.

43 *MITnet Rules of Use*, MIT, http://ist.mit.edu/network/rules (last visited Apr. 18, 2014); *see also* Superseding Indictment, *supra* note 7, at 2.

44 *See* MIT REPORT, *supra* note 29, at 16 n.2.

45 *See id.* at 16; *JSTOR Evidence in United States vs. Aaron Swartz*, Summary of Events, JSTOR (July 30, 2013), http://docs.jstor.org/summary.html [hereinafter *JSTOR Summary*].

46 *See* MIT REPORT, *supra* note 29, at 16; Email from [redacted sender] to [redacted recipient] (Sept. 26, 2010, 11:01 AM), *available at* http://docs.jstor.org/files/J00028_09-26-2010.PDF ("We are going to block them at the network level this is too much activity for the system.").

47 *See* MIT REPORT, *supra* note 29, at 16; Email from [redacted sender] to [redacted recipient] (Sept. 25, 2010 8:59 PM), *available at* http://docs.jstor.org/files/J00003_09-25-2010.PDF ("[I.P. address] 18.55.6.215 is toast.").

48 *See* MIT REPORT, *supra* note 29, at 16; Email from [redacted sender] to [redacted recipient] (Sept. 25, 2010 10:04 PM), *available at* http://docs.jstor.org/files/J00022_09-25-2010.PDF ("[T]he bad guys aren't getting PDFs anymore. Just 'go away' messages.").

49 *See* MIT REPORT, *supra* note 29, at 16; Superseding Indictment, *supra* note 7, at 5; Email from [redacted sender] to [redacted recipient] (Sept. 26, 2010, 1:16 PM), *available at* http://docs.jstor.org/files/J00032_09-26-2010.PDF ("Unfortunately, it didn't take long for them to switch to another address this time.").

download 450,000 JSTOR articles from 560 academic journals.[50] JSTOR only managed to stop him by denying access to the entire Class C network,[51] which consisted of all of the IP addresses in the building where Swartz had connected his computer.[52]

Apparently to hide his identity, Swartz had modified his laptop's media access client (MAC) address to read "ghost laptop," and registered for access to the MIT network under the false name "Gary Host," which prevented MIT from determining who had hacked their system.[53] However, MIT's department of Information Systems and Technology (IS&T) was able to determine that the laptop was not registered to an MIT student, faculty member, or employee.[54] JSTOR's service remained disabled at the building Swartz used until MIT's librarians assured JSTOR that the offending user had apparently been a guest of the Institute and was unlikely to return.[55]

Less than two weeks later, Swartz connected to the MIT network again and used a new technique to robotically harvest JSTOR's files.[56] After downloading each article, Swartz's computer, which also had a disguised user name and MAC address, was now programmed to rapidly download an article, delete the "cookie" (record of Swartz's connection to JSTOR), disconnect from JSTOR, and then reconnect to download another article.[57] Swartz also made it appear to JSTOR as if thousands of

---

50 *See* MIT REPORT, *supra* note 29, at 16.

51 "Class C addresses," IBM.COM, *available at* http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=%2Fcom.ibm.aix.commadmn%2Fdoc%2Fcommadmndita%2Faddresses_classc.htm (describing a Class C network as being large enough to support 256 local host addresses).

52 *See* MIT REPORT, *supra* note 29, at 17; Email from [redacted sender] to [redacted recipient] (Sept. 26, 2010, 5:58 PM), *available at* http://docs.jstor.org/files/J00033_09-26-2010.PDF ("[A]dded the class c net below to the block and we've been in the clear for two hours now.").

53 *See* MIT REPORT, *supra* note 29, at 18 n.8; Superseding Indictment, *supra* note 7, at 4.

54 *See* Superseding Indictment, *supra* note 7, at 6.

55 *See* MIT REPORT, *supra* note 29, at 17; Email from [redacted sender] to [redacted recipient] (Sept. 29, 2010, 4:03 PM), *available at* http://docs.jstor.org/files/J00038_09-29-2010.PDF.

56 *See* MIT REPORT, *supra* note 29, at 18; *JSTOR Summary*, *supra* note 45.

57 *See* MIT REPORT, *supra* note 29, at 18 n.9.

computers across MIT's campus were rapidly downloading articles.[58] These rapid downloads caused a "cascade of failures that brought down multiple JSTOR servers. Half the servers in one data center failed, and JSTOR engineers feared that the entire service might go down worldwide."[59] To stop the attack, the non-profit's engineers shut down JSTOR access to every IP address on MIT's campus—an unprecedented step for JSTOR's security team.[60] Thanks to JSTOR's prompt action, Swartz was only able to download about 8,000 articles.[61] Meanwhile, no one on the Institute's campus was able to access JSTOR for three days, and the Director of the MIT Libraries had to inform the Institute's leaders that the reason for the shut down was "a cyber-attack of the JSTOR database."[62]

A few weeks afterward, in late November, Swartz entered MIT once again and went into an academic building in the center of the campus.[63] This time he went into the basement and opened a closet containing the building's network switches.[64] The locking mechanism on the closet was later found to be broken.[65] Swartz used a cable to connect his own laptop to the Institute's network using one of these network switches, and hid the laptop under a cardboard box on the floor.[66] By connecting to a network switch in the basement, instead of a computer terminal elsewhere in the building, Swartz managed to use MIT's internet connection

---

58 *See id.* at 18.

59 *Id.*; Email from [redacted sender] to [redacted recipient] (Oct. 9, 2010, 6:14 PM), *available at* http://docs.jstor.org/files/J00052_10-09-2010.PDF ("About half the servers in [redacted] are now broken.").

60 *See* MIT Report, *supra* note 29, at 18; Email from [redacted sender] to [redacted recipient] (Oct. 9, 2010, 10:31 PM), *available at* http://docs.jstor.org/files/J00054_10-09-2010.PDF.

61 *See* MIT REPORT, *supra* note 29, at 18.

62 *See id.*

63 *See id.* at 19–25; Superseding Indictment, *supra* note 7, at 8.

64 *See* MIT REPORT, *supra* note 29, at 19–25; Superseding Indictment, *supra* note 7, at 8.

65 *See* MIT REPORT, *supra* note 29, at 19–25; Superseding Indictment, *supra* note 7, at 8.

66 *See* MIT REPORT, *supra* note 29, at 19–25; Superseding Indictment, *supra* note 7, at 8.

without registering as a user at all.[67] He could therefore use MIT's network to access the internet (and JSTOR) without any supervision by MIT's information technology administrators.[68] His computer remained there for at least a month, during which time he employed a new series of hacks to download approximately 4.3 million articles from JSTOR without detection.[69] In the aftermath of this attack, MIT implemented a new access protocol, which prevented any of the Institute's visitors from accessing JSTOR, except from certain monitored computers in the MIT libraries.[70]

B. The Interests Swartz Threatened, and How the CFAA Defends Them

In his article for *The New Yorker*, Professor Wu wrote, "Like a pie in the face, Swartz's act was annoying to its victim, but of no lasting consequence."[71] JSTOR's actions and statements at the time of the attacks contradict this assertion. In September 2010, JSTOR shut down access to one of MIT's buildings in response to the 450,000-article theft.[72] At that time, JSTOR notified MIT that Swartz's activity "clearly indicat[ed] robotic harvesting of PDFs [articles] which violates our Terms & Conditions of Use."[73] In October, JSTOR denied its service to MIT's entire campus in response to the multiple server crash that occurred during the 8,000-article theft.[74] JSTOR informed MIT that the downloaded articles were "not limited to a specific discipline, but were sequential across JSTOR's entire database [which indicated] 'a concerted effort [was] being made to download the entirety of the JSTOR archive."[75] Finally, when it detected the 4.3 million-

---

67 *See* MIT REPORT, *supra* note 29, at 19–25; Superseding Indictment, *supra* note 7, at 4.

68 *See* MIT REPORT, *supra* note 29, at 19–25; Superseding Indictment, *supra* note 7, at 4.

69 *See* MIT REPORT, *supra* note 29, at 19–25, 41; *JSTOR Summary*, *supra* note 45.

70 MIT REPORT, *supra* note 29, at 27.

71 Wu, *supra* note 11.

72 *See* MIT REPORT, *supra* note 29, at 17; *JSTOR Summary*, *supra* note 45.

73 *See* MIT REPORT, *supra* note 29, at 17; *JSTOR Summary*, *supra* note 45.

74 *See* MIT REPORT, *supra* note 29, at 18; *JSTOR Summary*, *supra* note 45.

75 *See* MIT REPORT, *supra* note 29, at 18; *JSTOR Summary*, *supra* note 45.

download attack in December, which brought Swartz's overall theft to approximately eighty percent of JSTOR's entire archive, the non-profit requested that MIT make "every effort . . . to identify the individuals responsible and to ensure that the content taken in this incident and those previously mentioned is secured and deleted."[76] JSTOR described Swartz's downloads as "extreme unauthorized activity . . . malicious and intentional."[77]

JSTOR's interest in preventing the release of the articles with which it was entrusted might seem self-explanatory. However, the repeated assertions, by critics of the prosecution, that Swartz's actions involved "no harm" indicate a need to emphasize the interests at stake. The articles in JSTOR's archive are the intellectual property of their authors and publishers.[78] JSTOR itself is a non-profit institution.[79] It makes digital copies of articles from thousands of academic journals, and provides those articles in a catalogued, searchable format to subscribers, mostly academic institutions, for a fee.[80] Some institutions receive free or discounted access.[81] Schools pay for access to JSTOR's digital copies of articles so that they do not have to acquire, store, or digitize documents themselves.[82]

As an ethical matter, this means that the information in its archive is not JSTOR's product. JSTOR does not produce anything. Instead, JSTOR provides a service: digitizing information and providing a searchable, accessible source for those seeking access to it. JSTOR provides this service, in its words, to "[support] scholarly work and access to knowledge around the world."[83] The non-profit pays content providers for access to their

---

76 *See* MIT REPORT, *supra* note 29, at 19–20, 31–32.

77 *See id.* at 20.

78 *See* 17 U.S.C. § 106 (2012) ("the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords"); *New to JSTOR? Learn More About Us*, JSTOR, http://about.jstor.org/10things (last visited Apr. 18, 2014) [hereinafter *JSTOR About Us*].

79 *See* Schwartz, *supra* note 1; *JSTOR About Us*, *supra* note 78.

80 *See* Schwartz, *supra* note 1; Superseding Indictment, *supra* note 7, at 1.

81 *See* Schwartz, *supra* note 1; Superseding Indictment, *supra* note 7, at 1.

82 *See* Schwartz, *supra* note 1; *JSTOR About Us*, *supra* note 78.

83 JSTOR Press Release, *supra* note 27.

intellectual property, and makes these valuable documents available to "[f]aculty, teachers, and students at more than 7,000 institutions in 153 countries."[84] JSTOR's leaders emphasized in the non-profit's press release that as "responsible stewards" of their content providers' works, it is their responsibility to prevent unauthorized use.[85]

It ought to be self-evident that if all of JSTOR's articles were released online, the non-profit could no longer provide its service. That is probably what Aaron Swartz was trying to accomplish. In 2008, Swartz published[86] a document entitled, "Guerilla Open Access Manifesto," in which he stated that those with access to information databases have a moral duty to break copyright laws by "trading passwords with colleagues" and "filling download requests for friends."[87] He praised those who "have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers . . . ."[88] Swartz criticized the notion that such activity is "stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew."[89] He described the copyright laws, which prevent these actions, as "unjust" and backed by politicians who have been "bought off" by corporations who in turn are "blinded by greed."[90] He declared that the time had come to engage in "civil disobedience" against the copyright laws.

---

84 *Id.*

85 *Id.*

86 In the aftermath of his suicide, at least one of Swartz's friends disputed his responsibility for the manifesto. Quinn Norton told the MIT Review Panel that she had edited the document and that she was not sure who had written the text that they were trying to use to prove his intent, as it had been authored by four people. Quinn Norton, *Life Inside the Aaron Swartz Investigation*, ATLANTIC, Mar. 3, 2013, http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartzinvestigation/273654. The 580-word manifesto contains a brief byline, which reads in its entirety: "Aaron Swartz, July 2008, Eremo, Italy." Aaron Swartz, *Guerilla Open Access Manifesto*, INTERNET ARCHIVE (July 2008), http://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt.

87 Swartz, *supra* note 86.

88 *Id.*

89 *Id.*

90 *Id.*

> We need to take information, wherever it is stored, make our copies and share them with the world . . . We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for Guerilla Open Access. With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge—we'll make it a thing of the past.[91]

In 2008, Swartz took advantage of a trial period during which the United States courts temporarily allowed free access to the Public Access to Court Electronic Records (PACER) archive, which contains documents filed in federal courts.[92] Normally PACER charges users a small fee per page, which finances the collection, scanning, and uploading of records to the PACER archive, as well as PACER's catalogue and search functions.[93] In 2008, however, the federal courts made PACER available for free to public libraries.[94] Swartz took this opportunity to write a program that began downloading all of the documents in the PACER archive.[95] Doing so, he managed to acquire almost 20 million pages of records, or twenty percent of PACER's documents, before the courts shut down the libraries' free access in order to stop the bulk downloads.[96] Swartz donated all of these records to an open government initiative called public.resource.org.[97] Since the court documents were in the public domain and not protected by copyright, the government determined that Swartz had not broken any law.[98]

One Swartz supporter, whom the MIT Review Panel decided to identify publicly as only "a leader in the global movement for open

---

91 *Id.*

92 Schwartz, *supra* note 1.

93 *How Much Does PACER Cost?*, PACER, http://www.pacer.gov (last visited Apr. 18, 2014).

94 *See* Schwartz, *supra* note 1; MIT REPORT, *supra* note 29, at 32.

95 *See* Schwartz, *supra* note 1; MIT REPORT, *supra* note 29, at 32.

96 Schwartz, *supra* note 1.

97 *See* MIT REPORT, *supra* note 29, at 32.

98 *See id*.

access to scientific publications," wrote an email to the President of MIT, which indicated that Swartz intended to release JSTOR's documents to the public, just as he had done with the PACER documents.[99] In an apparent attempt to excuse Swartz's actions, the leader, who confessed a limited knowledge of the American justice system, told MIT's President that: "Aaron Swartz had attended a meeting that included a discussion of how much it would cost to get JSTOR to open up its archive for the public and how that exceeded the funds available to the group at the meeting."[100] The leader also wrote of his fear that their conversation at that meeting played a role in Aaron Swartz's unfortunate decision to conduct the hack.[101]

Other friends and supporters of Swartz suggested that he might not have actually intended to release the JSTOR archive to the public. Carl Malamud, the open-government advocate to whom Swartz had donated the PACER documents, wrote that he did not think Swartz would release the downloaded documents "without a great deal of post-download analysis."[102] At least one supporter has suggested that Swartz might have downloaded JSTOR's articles only to collect data *about* the articles, that is, to determine the influence of "big money" in scientific research, or how many publicly funded scientific studies were being sold or licensed for fees by their authors and publishers.[103] Swartz had previously assisted a law student in conducting a similar study of law journal articles.[104] JSTOR, however, pointed out that it has made data about its articles and their funding available to the public since 2008 for exactly this purpose, and that it actively participates in data-driven studies of its publications:

---

99 *Id.* at 71–72.

100 *Id.*

101 *Id.*

102 Carl Malamud, On Crime and Access to Knowledge para. 18 (Mar. 30, 2013) (unpublished essay), https://public.resource.org/crime/pamphlet.pdf.

103 *See Lessig on Aaron's Laws*, *supra* note 12; *see also* Norton, *supra* note 86.

104 *See* MIT REPORT, *supra* note 29, at 33 n.18 and accompanying text; *see also* Shireen A. Barday, *Punitive Damages, Remunerated Research, and the Legal Profession*, 61 STAN. L. REV. 711, 713 (2008) (explaining how the author used "Python source code extracting all entries (441,170) contained in the Westlaw "Journals and Law Reviews" database, including full-text articles").

> [W]e support and encourage the legitimate use of large sets of content from JSTOR for research purposes. We regularly provide scholars with access to content for this purpose. Our Data for Research site (http://dfr.jstor.org) was established expressly to support text mining and other projects, and our Advanced Technologies Group is an eager collaborator with researchers in the academic community.[105]

Swartz would not have needed to attack MIT's and JSTOR's network to get the kind of information he acquired for the legal journal study.

It is hard to argue that Aaron Swartz had an innocent reason for disabling MIT's network security protocols and connecting a computer hidden in a basement to the Institute's network switch. It is even harder to make that argument when one notes how close he came to downloading the entirety of the JSTOR archive.[106] Swartz's actions, in fact, fall squarely within the purview of the Computer Fraud and Abuse Act (CFAA), which clearly prohibits modifying a computer network in order to exceed authorized use.[107] Swartz repeatedly modified MIT's network security protocols, and used the network without authorization by plugging directly into the network switch.[108] He did so in order to defeat the safeguards that would have prevented him from downloading millions of articles, which he probably intended to share freely with the rest of the world.[109] The potential consequences of his goal ought to be readily apparent from the actual consequences. Whenever Aaron Swartz began robotically harvesting files from a document provider, be it PACER or JSTOR, that provider shut down its service in order to safeguard its ability to operate.[110] This

---

105 JSTOR Press Release, *supra* note 30.

106 *See* MIT REPORT, *supra* note 29, at 32.

107 *See* 18 U.S.C. § 1030(a)(4) (2012).

108 *See* MIT REPORT, *supra* note 29, at 19–25.

109 *See id*. at 16–19.

110 *See* MIT REPORT, *supra* note 29, at 18; *see also* Email from [redacted sender] to [redacted recipient] (Oct. 9, 2010, 10:31 PM), *available at* http://docs.jstor.org/files/J00054_10-09-2010.PDF.

illustrates the divergence between what he claimed he was doing and what he was actually doing: instead of making all information free to the public, he was making it impossible to distribute any information to the public in a sustainable way.

When Swartz attempted to robotically harvest the entire PACER archive on behalf of public.resource.org, Carl Malamud envisioned that his organization might place all of the courts' documents on an "independent server, one that would offer the same material but be better organized, easier to search and free, anytime and anywhere."[111] No such archive exists, not least because neither Malamud nor Swartz had the employees or infrastructure to do what PACER and JSTOR do.

The services that Swartz attacked do not create or even own content—they distribute content to the public.[112] That distribution involves collecting, scanning, digitizing, cataloguing, and preparing millions of articles to be searched, accessed, and downloaded.[113] Those processes cannot happen without time, effort, and money. PACER and JSTOR found a way to collect money—not to make a profit, but to enable the processes that distribute content. Aaron Swartz almost stopped them.

Critics of the CFAA have argued that the law, which was originally passed in 1986, does not reflect the reality of modern computer usage.[114] The most common concern is the law's language prohibiting any use of a computer that "exceeds authorized access."[115] This has raised fears about the law's scope, and whether it might criminalize minor or trivial violations of software terms of use, which most computer users disregard without reading.[116] Scholars have suggested that it might even be construed to criminalize as felons those employees who use their

---

111 Amsden, *supra* note 12.

112 *See JSTOR About Us*, *supra* note 78.

113 *See id.*

114 *See* Wu, *supra* note 11, at 2.

115 18 U.S.C. § 1030 (2012).

116 *See* Kelsey T. Patterson, *Narrowing it down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 513 (2013); *see also* Lothar Determann, *Internet Freedom and Computer Abuse*, 35 HASTINGS COMM. & ENT. L.J. 429, 430 (2013).

work computers to "frolic" on the Internet.[117] The United States Court of Appeals for the Ninth Circuit used similar reasoning in 2011 when it affirmed a district court ruling dismissing a CFAA charge in *United States v. Nosal*.[118]

Professor Wu cited the Ninth Circuit's *Nosal* decision when he wrote that the government's "legal authority" in the Swartz case was "shaky."[119] Even if *Nosal* were binding precedent in the District of Massachusetts—which it is not—the case is distinguishable from Swartz. *Nosal* involved a defendant who conspired with employees of an executive-recruiting company to steal files from the company.[120] At the defendant's urging, those employees accessed their company's network in a normal, authorized manner, but did so in order to improperly transfer confidential files to the defendant.[121] Chief Judge Kozinski, writing for the majority, affirmed the dismissal of the CFAA-related counts of the *Nosal* indictment, holding that the CFAA cannot apply to "everyone who uses a computer in violation of computer use restrictions," because such an application "may well include everyone who uses a computer."[122] *Nosal* is distinguishable from *Swartz* for several reasons, not least because the former did not involve anything that could be characterized as a cyber attack.[123] Unlike Aaron Swartz, none of the employees modified or defeated their company's network security protocols.[124] They did not disable a network's safeguards, nor did they surreptitiously seize control of someone else's computer network in order to use that network in a manner for which it was not intended.[125] Most obviously, they did not create dummy accounts, connect unauthorized computers to network switches

---

117 *See* Patterson, *supra* note 116, at 513.

118 United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012).

119 Wu, *supra* note 11.

120 *Nosal*, 676 F.3d at 856.

121 *Id.*

122 *Id.* at 857.

123 *Compare Nosal*, 676 F.3d at 856, *with* Superseding Indictment, *supra* note 7, at 3–9.

124 *See* MIT REPORT, *supra* note 29, at 16–22; Superseding Indictment, *supra* note 7, at 4–8.

125 *See* MIT REPORT, *supra* note 29, at 16–22; Superseding Indictment, *supra* note 7, at 4–8.

hidden in closets, or crash servers.[126] They did not attack their company's network. They just stole files from work—a theft that the Court of Appeals acknowledged was a chargeable crime under other laws.[127]

The CFAA has its faults, including vague language that could expose a network user to a severe penalty for minor violations if courts or prosecutors interpret the law too broadly. However, when Swartz disabled network security protocols and trespassed on MIT property to connect his computer to their network switch, he was not like any employee who "frolics" on the internet at work. He used MIT's and JSTOR's computers against the will of both non-profit entities, despite the objections of both, and repeatedly overpowered their efforts to resist his penetration and control of their systems. This was not analogous to using a nickname on Facebook. He damaged information systems in order to steal millions of copyrighted works. No revision of the CFAA would excuse this conduct. The United States Constitution itself requires the federal government to "secur[e] for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[128] Aaron Swartz quite self-consciously attempted to deprive content producers of that exclusive right.

If he had accepted the government's guilty plea offer, and served a few months in prison, it stands to reason that Swartz would have emerged with an even greater reputation as a fighter for open access. Perhaps he would have used his notoriety to advocate for the amendment of the CFAA, so that defendants charged with relatively minor computer crimes—crimes more minor than his own—would not face the possibility of years in prison. Instead, it was his death that inspired the bill known as "Aaron's Law" to amend the CFAA.[129] As of this writing, the bill is before the House Committee on the Judiciary.[130] If it passes,

---

126 *See* MIT REPORT, *supra* note 29, at 16–22; Superseding Indictment, *supra* note 7, at 4–8.

127 *Nosal*, 676 F.3d at 863–64.

128 U.S. CONST. art. I, § 8, cl. 8.

129 *See* Lofgren & Wyden, *supra* note 19.

130 *See H.R. 2454: Aaron's Law Act of 2013*, GOVTRACK, https://www.govtrack.us/congress/bills/113/hr2454 (last visited Apr. 18, 2014).

Aaron's Law would strike the potentially problematic language, "exceeds authorized access" from the CFAA, and clarify that the crime of "access without authorization" means an act:

> (A) to obtain information on a protected computer;
> (B) that the accesser lacks authorization to obtain; and
> (C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information.[131]

In their press release announcing the bill, Aaron's Law drafters Representative Zoe Lofgren and Senator Ron Wyden were careful not to claim that such revisions to the CFAA would prevent prosecution of acts like Swartz's sustained attacks on MIT and JSTOR.[132] Swartz, of course, circumvented, manipulated, and disabled a number of physical and technological safeguards in order to obtain copyrighted intellectual property against JSTOR's and MIT's expressed objections and despite their concerted efforts to stop him.[133] Aaron's Law would not legalize such activity.

C. Neither MIT's Neutrality Nor JSTOR's Later Opposition Rendered Prosecution Unjust

Several critics of the prosecution have pointed out that JSTOR and MIT, the alleged victims of Swartz's crimes, declined to press charges against him.[134] Such criticism overlooks the vigor with which JSTOR asserted and defended its own intellectual property rights, resisted his attacks on its network, demanded that he be identified and stopped, and condemned his actions until the moment JSTOR received its property back along with assurances that he would no longer harm JSTOR's interests.[135] It also overlooks the possibility that the threat of a criminal penalty

---

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

132 *See* Lofgren & Wyden, *supra* note 19.

133 *See supra* notes 34–70 and accompanying text.

134 *See* Wu, *supra* note 11 ("Among the most frustrating components of the ordeal was the fact that JSTOR, ostensibly the most overtly wronged party, had declined to press charges against Swartz after he returned the downloaded documents.").

135 *See* JSTOR Press Release, *supra* note 30.

allowed JSTOR to demand the return of its property from Swartz, or, conversely, that Swartz withheld JSTOR's property until his lawyers extracted from the non-profit a promise that it would not seek his prosecution.[136]

All of this runs counter to the idea that JSTOR actually believed Aaron Swartz had done nothing wrong. Indeed, JSTOR's increasingly agitated complaints throughout the months of Swartz's cyber attacks belie the notion. In September 2010, JSTOR asserted that Swartz's first attacks "clearly" violated its terms of use.[137] A JSTOR administrator described the attack as an "extreme case," using a download pattern that was "terribly efficient, but not terribly subtle," and necessitating the largest service blockage (denying service to entire Class C range) that the administrator had ever seen in his tenure.[138]

In October 2010, JSTOR concluded that the server-crashing attacks were a "concerted effort" to download its entire archive.[139] In December 2010, JSTOR described the multi-million-download attacks as "malicious and intentional."[140] Another JSTOR administrator suggested on December 26 that if JSTOR and MIT could not stop the attacks, they might have to call the FBI.[141] In June of 2011, when JSTOR informed MIT that Swartz had handed over the downloaded files to the Boston USAO, it described the files as "stolen records."[142]

As for MIT, the Institute maintained a stance of "neutrality" throughout the prosecution, and even after Swartz's death reiterated its compelling reasons for not opposing the prosecution:

> Aaron Swartz had used MIT's premises and network to allegedly commit crimes, he had adversely affected MIT's relationship with JSTOR,

---

136 *See* MIT REPORT, *supra* note 29, at 41.

137 *Id.* at 17.

138 Email from [redacted sender] to [redacted recipient] (Sept. 29, 2010, 5:13 PM), *available at* http://docs.jstor.org/files/J00040_09-29-2010.PDF.

139 MIT REPORT, *supra* note 29, at 18.

140 *Id.* at 20.

141 *See* Email from [redacted sender] to [redacted recipient] (Dec. 26, 2011, 11:41 PM), *available at* http://docs.jstor.org/files/J00217_12-26-2010.PDF.

142 MIT REPORT, *supra* note 29, at 57.

> and he had seriously inconvenienced MIT's Libraries, MIT researchers, and students seeking to use JSTOR, and MIT's IS&T personnel who repeatedly tried to stop his misuse of MIT's network. MIT felt no sense of obligation toward someone who had abused the open access privileges it had provided for the convenience of guests, even if that abuse was carried out in the name of open access.[143]

MIT's Review Panel further observed that opposing the prosecution might indicate to the public that the Institute was not serious about contracts with licensors or the integrity of its network.[144]

But setting all of that aside for a moment, and assuming *arguendo* that JSTOR or MIT had expressed a completely genuine desire that Swartz not be punished, such a desire would not necessarily compel the government to drop the charges. In the first place, these parties' supposed absolution could not encompass the feelings of every single academic, author, and publisher who entrusted them with their intellectual property. Indeed, neither JSTOR nor MIT are the owners or publishers of the intellectual property that Swartz stole.[145] Furthermore, when authorities encounter remarkably forgiving-crime victims, these victims' desire to turn the other cheek, and who conscientiously object to the imposition of criminal penalties, does not stand in the way of the government enforcing its laws.[146] In the case of intellectual property, prosecutors have a clear constitutional and statutory duty to prevent theft.[147]

AUSA Heymann, the lead prosecutor, indicated to MIT's Office of General Counsel that he had considered JSTOR's and

---

143 *Id.* at 55.

144 *Id.* at 85.

145 *See JSTOR About Us*, *supra* note 78.

146 *See* Angela Corsilles, *No-Drop Policies in the Prosecution of Domestic Violence Cases: Guarantee to Action or Dangerous Solution?*, 63 FORDHAM L. REV. 853, 866–67 (1994).

147 *See* U.S. CONST. art. I, § 8, cl. 8; 17 U.S.C. § 106(1) (2012).

MIT's positions on the matter.[148] However, he also indicated that he had to consider deterring others from committing similar crimes.[149] Swartz seemed to be making a bold stand, the kind of civil disobedience that could certainly impress anyone who opposes intellectual property *per se*. That stand was also audacious for a very serious reason: he had poked the United States government in the eye, deliberately undermining the intellectual property rights that the government is constitutionally bound to defend.[150]

It is possible, however, that Swartz was completely unaware of the seriousness of his actions until after his arrest. When MIT Police accosted Swartz after catching him on camera changing the hard drive on the basement computer, Swartz responded that he "didn't speak with strangers."[151] He then stated that MIT Police are not "real cops," and fled.[152] Shortly thereafter, two MIT Police officers and a United States Secret Service agent apprehended Swartz.[153] His friend Quinn Norton and attorney Elliott Peters both told the MIT Review Panel that Swartz was "shocked" by his arrest.[154] Norton said Swartz "didn't regard what he had done as a big deal and was surprised that people were making so much of it."[155]

Such a perspective would be remarkably obtuse, especially for the man who wrote with such passion about the forces arrayed against him in the worldwide battle for open access.[156] Regardless of whether Swartz understood the magnitude of his actions, the fact remained that almost five million copyrighted works, which derived their monetary value from the limits on their distribution,

---

148 *See* MIT REPORT, *supra* note 29, at 52.

149 *See id.* at 67–69.

150 *See* U.S. CONST. art. I, § 8, cl. 8; 17 U.S.C. § 106(1).

151 MIT REPORT, *supra* note 29, at 25.

152 *Id.*

153 *Id.*

154 *Id.* at 3.

155 *Id.*

156 *See* Swartz, *supra* note 87 ("Large corporations, of course, are blinded by greed. The laws under which they operate require it—their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.").

had come within a few keystrokes of being lost. A non-profit that funds research and makes information available across the world was almost put out of business. This was all in addition to the JSTOR servers that crashed under the weight of Swartz's attacks, the efforts of JSTOR and MIT employees to identify and repel his attacks, and the days that MIT's students and faculty went without access to JSTOR's resources in the aftermath of those attacks. If there was anything that could reasonably prevent the government from seeking imprisonment for Aaron Swartz, JSTOR's supposed absolution was not it.

CONCLUSION: MISSED SIGNALS

The United States has a long and cherished history of civil disobedience, of true believers who openly challenge the status quo. To some, Aaron Swartz was such a freedom fighter:

> In another time, a man with Swartz's dark drive would have headed to the frontier. Perhaps he would have ventured out into the wilderness, like T. E. Lawrence or John Muir . . . . Swartz possessed a self-destructive drive toward actions that felt right to him, but that were also defiant and, potentially, law-breaking. Like Henry David Thoreau, he chased his own dreams, and he was willing to disobey laws he considered unjust.[157]

One might say the same of Jeremy Hammond, a hacker who pled guilty in 2013 to attacking the networks of corporations, government agencies, and law enforcement advocacy groups.[158] At his sentencing in the Southern District of New York, Hammond described his attacks as "acts of civil disobedience" against government surveillance and corporate complicity.[159] After he was

---

[157] Wu, *supra* note 11.

[158] *See* Mark Mazzetti, *Hacker Receives 10-Year Sentence for 'Causing Mayhem*,*'* N.Y. TIMES (Nov. 15, 2013, 4:46 PM), http://bits.blogs.nytimes.com/2013/11/15/hacker-for-anonymous-sentenced-to-10-years-in-prison/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

[159] *See id.*

sentenced to 10 years in prison, he raised a fist in the air and yelled, "Long live Anonymous!" and "Hurrah for anarchy!" while being escorted from the courtroom.[160] To some observers, Aaron Swartz might have seemed like another Jeremy Hammond, but the evidence indicates that Swartz was a very different young man. At least one commentator has suggested that Swartz rejected the Government's offers of minimal sentence guidelines during plea negotiations because he could not bear the thought of being a felon.[161]

There was another, more serious problem. Six years before his suicide, friends and readers posted the following messages on Swartz's blog in response to a short story he had published:

> "Hey Aaron, You're scaring me here. Please s[t]ick around and talk to us. You can always die later. There's no rush."
> "Jeez, Aaron—get some help. Now. Suicides talk about it before they do it."
> "Aaron, you're scaring me. You're one of the most brilliant people around and you have a bright future."
> "Hey Aaron—I'm a little worried here. Please heed the above advice. Let me know if I can help."[162]

The short story that inspired these messages, "A Moment Before Dying," describes a young man and his struggles with depression shortly before he commits suicide.[163] Swartz's friends took the post so seriously—the title character in the original version was named "Aaron"—that one of them called the police.[164] Swartz also blogged explicitly about his own struggles with depression, quoting writer George Scialabba to describe his condition:

---

160 *See id.*

161 *See* Amsden, *supra* note 12 ("There was a moment when [Aaron Swartz and ex-girlfriend Quinn Norton] were standing outside the White House . . . when Aaron turned to [Norton] and said, 'You know, they don't allow felons to work there.'").

162 Aaron Swartz, *A Moment Before Dying*, Comments, RAW THOUGHT BLOG (Jan. 18, 2007), http://www.aaronsw.com/weblog/dying.

163 *See id.*

164 *See* Amsden, *supra* note 12.

> [A]cute depression does not feel like falling ill, it feels like being tortured . . . the pain is not localized; it runs along every nerve, an unconsuming fire . . . . Even though one knows better, one cannot believe that it will ever end, or that anyone else has ever felt anything like it.[165]

Other posts in the blog reveal Swartz to be a sensitive, thoughtful, brilliant young man who reveled in discussing a diverse variety of topics, from economic theory to popular films. Frequent themes in the blog included individuals who challenge the status quo and the death of such individuals, including by suicide. These themes appeared in Swartz's last three blog posts, the first of which he published on September 25, 2012.

This third-to-last post was a mostly academic discussion of labor relations and productivity in the automotive industry, and specifically considered how managers might motivate their workers to follow instruction.[166] After a detailed historical and philosophical discussion of organizational theory and the effects of economic incentives, Swartz concluded the post with the following:

> When you're upset with someone, all you want to do is change the way they're acting. But you can't control what's inside a person's head. Yelling at them isn't going to make them come around, it's just going to make them more defiant . . . . No, you can't force other people to change. You can, however, change just about everything else. And usually, that's enough.[167]

Perhaps this offers a glimpse into the mind of a man who turned down a zero-to-six months sentence, after admitting to the charged conduct and knowing that he would likely spend seven years in prison if he went to trial.

---

[165] Aaron Swartz, *Sick*, RAW THOUGHT BLOG (Nov. 27, 2007), http://www.aaronsw.com/weblog/verysick.

[166] Aaron Swartz, *Fix the Machine, Not the Person*, RAW THOUGHT BLOG (Sept. 25, 2012), http://www.aaronsw.com/weblog/nummi.

[167] *Id.*

Any evaluation of the decisions preceding Aaron Swartz's death bears the inevitable tinge of hindsight. As the MIT Report put it, "[H]ow does one maintain a perspective uncolored by the shock and tragedy of Aaron Swartz's suicide[?]"[168] It would not be fair to blame anyone for failing to realize the seriousness of Swartz's condition. His partner, Stinebrickner-Kauffman, said, "I don't think any of us actually realized how much of a toll it had taken, until later, until after he died. He hid it from us well."[169]

Nevertheless, Swartz's attorneys were apparently concerned about his mental health. Andy Good, the first lawyer who represented Swartz in the prosecution, told the *Boston Globe*, "I told Heymann [that Swartz] was a suicide risk . . . . [Heymann's] reaction was a standard reaction in that office, not unique to Steve. He said, 'Fine, we'll lock him up.' . . . [T]hey were aware of the risk, and they were heedless."[170] At least one Swartz supporter raised the issue with MIT's President.[171] The aforementioned "leader in the global movement for open access to scientific publications," wrote that a term in prison would be "fateful, unbearable, in the worst case, deadly" for Swartz.[172]

If it were indeed the case that any prosecutor reacted callously or flippantly to a warning that Aaron Swartz's life was in danger, such a reaction would certainly be the subject of bitter regret. The Central District of California has recently implemented a program to allow prosecutors and others to take steps to mitigate a mentally ill defendant's risk to himself and others.[173] The District Court, working together with the federal defender's office and a mental health provider, crafted a resource program that helps defendants manage their symptoms of anxiety, depression, and suicidal

---

168 MIT REPORT, *supra* note 29, at 12.

169 Stinebrickner-Kauffman, *supra* note 10.

170 Kevin Cullen, *On Humanity, a Big Failure in Aaron Swartz Case*, BOSTON GLOBE, Jan. 15, 2013, http://www.bostonglobe.com/metro/2013/01/15/humanity-deficit/bj8oThPDwzgxBSHQt3tyKI/story.html.

171 *See* MIT REPORT, *supra* note 29, at 71–72.

172 *Id.*

173 *See* James M. Byrne, Arthur J. Lurigio & Roger Pimentel, *New Defendants, New Responsibilities: Preventing Suicide Among Alleged Sex Offenders in the Federal Pretrial System*, 73 FED. PROBATION 40, 42–43 (2009).

thoughts, all while protecting their right against self-incrimination.[174] The program includes crisis intervention, support groups, instruction on healthy coping skills, cognitive behavioral therapy, and lessons on keys to successful incarceration.[175]

Similar options are also available to defense attorneys. In fact, the Boston Bar Association hosted an event in November 2013 entitled "Recognizing and Responding to Suicidal Persons: What Lawyers Need to Know."[176] The event included a panel discussion by defense attorneys, prosecutors, and mental health professionals, and the event program provided a directory of mental health resources and advice for attorneys.[177] Given that prosecutors might naturally question a defense attorney's suggestion that his client should not be punished for health reasons, it is even more important that defense attorneys be proactive in monitoring and safeguarding a defendant's mental health, especially when the defendant is not under government confinement.

If nothing else, Aaron Swartz's story is a cause for reflection for all who exercise power over people, machines, or networks. Swartz was born with astounding intellectual gifts, which he developed at a young age into a remarkable power to manipulate networked systems. He wielded his power irresponsibly, and in doing so, he made himself the target of a government whose power is unmatched in history. It appears that Aaron Swartz found, quite reasonably, that it is extremely stressful to confront such a power.

The prosecutors in the Massachusetts USAO, who exercise power on behalf of the government, have certainly been unjustly accused of many things in the wake of Swartz's death. However, a sense of perspective is important here. As awful as it must be for any public servant to face false or unfair accusations in public, how much worse must it have been for that young man, alone in his Brooklyn apartment, confronting the awesome power of the

---

174 *See id.* at 42.

175 *See id.*

176 *Recognizing and Responding to Suicidal Persons: What Lawyers Need to Know*, BOSTON BAR ASS'N (Nov. 19, 2013), *available at* https://www.bostonbar.org/membership/events/event-details?ID=14274.

177 *Id.*

government by himself? There can be little doubt that, misguided as he was, he never stopped wanting to make the world a better place.

The epigraph to this Note is from Oscar Wilde's novel about a young man who kills himself in a desperate attempt to draw support for his own discredited scholarly theory.[178] In the quoted passage, the narrator is addressing a man named Erskine, a friend of the deceased, who refuses to publish the dead man's theory due to its lack of literary support.[179] Appalled, the narrator pleads with Erskine to publish the theory, saying, "[A]nd if you will not tell of his martyrdom, tell at least of his faith."[180] Erskine is adamant that the young man's suicide lends no credence to his theory: "a thing is not necessarily true because a man dies for it."[181]

Aaron Swartz's suicide does not reflect the justice or injustice of the CFAA, but Swartz's theories about the importance of access to scholarship will live on regardless of whether the government acted justly in attempting to punish him.[182] His ideas will endure because in Swartz's short but exceptional life he earned the love and admiration of relatives, friends, and supporters around the world.[183] Those supporters have spoken and written much about what they regard as his martyrdom[184] and they may understandably resent this Note's assertion that Swartz was not the victim of the injustices they have alleged. It is therefore appropriate to give the last word to Swartz's family, who wrote not just of his martyrdom, but also of his faith:

> Aaron's insatiable curiosity, creativity, and brilliance; his reflexive empathy and capacity for selfless, boundless love; his refusal to accept injustice as inevitable—these gifts made the world, and our lives, far brighter. We're grateful for our

---

178 Oscar Wilde, THE PORTRAIT OF MR. W. H. 13 (1889).
179 *Id.* at 14.
180 *Id.*
181 *Id.*
182 *See, e.g.*, Lofgren & Wyden, *supra* note 19.
183 *See, e.g.*, Fiels, *A Memorial Resolution Honoring Aaron Swartz*; Inductees, Internet Hall of Fame Innovator Aaron Swartz, Posthumous Recipient, *supra* note 13.
184 *See, e.g.*, Stinebrickner-Kauffman, *supra* note 10; *see also* Wu, *supra* note 11.

> time with him, to those who loved him and stood with him, and to all of those who continue his work for a better world.[185]

---

[185] *RSS Creator Aaron Swartz Dead at 26*, *supra* note 6.