University of Massachusetts Law Review

Volume 10 | Issue 1 Article 7

January 2015

Aaron's Law: Reactionary Legislation in the Guise of Justice

Matthew Aaron Viana

UMass Law Review

Aaron’s Law: Reactionary Legislation in the Guise of Justice

Matthew Aaron Viana

10 U. MASS. L. REV. 214

ABSTRACT

This Note argues that the proposed amendment to the Computer Fraud and Abuse Act dubbed “Aaron’s Law,” created in the wake of the prosecution and subsequent suicide of hacktivist Aaron Swartz, should not be enacted as it is overly reactionary legislation which would have unfortunate and unjust repercussions in the realm of civil litigation. This Note first describes the circumstances under which Mr. Swartz found himself prosecuted under the Computer Fraud and Abuse Act, namely his intrusion into, and downloading massive amounts of data from, large internet databases like PACER and JSTOR. This Note also explores the disputed interpretation of the CFAA phrase “exceeds authorized access” by the Circuit Courts of Appeal and according to the maxims of statutory interpretation, the particular phrase which Aaron’s Law seeks to amend. Then this Note examines *Robbins v. Lower Merion School District*, a case utilizing the existing language of the CFAA. Amending the language as proposed by Aaron’s Law would potentially remove a civil remedy in *Robbins*. This Note concludes that prosecutorial discretion should be used in cases like Aaron Swartz’s, so as to allow the CFAA to function as intended by Congress and to provide the *Robbins* plaintiffs, and similarly situated individuals, a meaningful remedy.

AUTHOR NOTE

Matthew Aaron Viana expects to receive his J.D. in May, 2015 from the University of Massachusetts School of Law - Dartmouth. He earned his B.A. in 2010 from the University of Massachusetts, Amherst. The author would like to thank his editing team for their diligence and Alan Battista for the many illuminating discussions sparked by this topic. Also, the author gives special thanks to his wife and family, without whose love and support so many things would be unattainable.

I. INTRODUCTION

The federal indictment and subsequent suicide of computer programmer and hacktivist[1]Aaron Swartz sparked tremendous controversy surrounding the Computer Fraud and Abuse Act ("CFAA")[2]. Aaron Swartz was charged with eleven counts of violating the CFAA for allegedly downloading and distributing a substantial portion of JSTOR's digitized academic journal archive.[3] The CFAA criminalizes, among other things, activities which stem from "knowingly access[ing] a computer without authorization or exceed[ing] authorized access."[4] This is, arguably, broad language that could encompass a wide range of computer activities. An implementation based on its broad language makes this provision of the CFAA unfortunately vulnerable to possible injustice. Aaron was a victim of such injustice. However, the broad language of the CFAA has its merits and should not be amended by way of reactionary legislation crafted in the guise of justice.

The statutory language, "knowingly accesses a computer without authorization or exceeds authorized access," itself, has been subject to varying interpretations.[5] There is a Circuit split regarding the meaning of both phrases: "without authorization" and "exceeds authorized access" under the CFAA. The Fifth, Seventh, and Eleventh Circuits have each held that the CFAA broadly covers violations of corporate computer use restrictions.[6] In contrast, the Ninth and Fourth Circuits have narrowly interpreted "exceeds authorized access" so as not to

[1] "Hacktivist" is a portmanteau of the words "hacker" and "activist," employed to describe an individual who uses hacking skills to further activist goals.

[2] *See generally* 18 U.S.C. § 1030 (2014) (The CFAA is a statute that provides civil and criminal penalties and targets the practices of computer hacking and misappropriation of information.).

[3] Superseding Indictment, United States v. Swartz, No. 11-CR-10260-NMG (D. Mass. 2012). *Available at* http://www.wired.com/images_blogs/threatlevel/2012/09/swartzsuperseding.pdf.

[4] 18 U.S.C. § 1030 (a)(2) (2014).

[5] *See, supra,* Part III.

[6] See United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (Social Security employee convicted for using computer access to access records for personal reasons); United States v. John, 597 F.3d 854 (5th Cir. 2010) (bank employee convicted for use of computer access to transmit account numbers to accomplice); and Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (employee convicted for using corporate files on company laptop for purposes of setting up a competing business).

include mere violations of corporate computer restrictions.[7] Depending on the jurisdiction, it is arguable regarding whether the statute allows a computer user to be federally indicted for minor crimes such as breaching a terms of service agreement.[8]

Aaron's Law, proposed on June 20, 2013, would amend the CFAA, eliminating the "exceeds authorized access" provision.[9] It would further define "access without authorization" to include only obtaining "information on a protected computer," that the "accesser lacks authorization to obtain," by "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining or altering that information."[10] Therefore, Aaron's law would decriminalize violations of an agreement, policy, duty, or contractual obligation regarding computer use, such as a terms of service agreement.

Aaron's Law, if enacted, would be a prime example of reactionary legislation providing a disservice to harmed individuals in the civil arena. It would eviscerate an essential provision contained in the CFAA, reversing legislative history, raising policy concerns, and, as this note emphasizes, leave harmed plaintiffs with one less avenue for recovery. Keeping in mind the dual nature of the CFAA, having both civil and criminal components, if Aaron's law was to be enacted and the CFAA deprived of the full force of its current wording, the effects would be felt in both arenas. While hackstivists such as Aaron may have benefitted from the different standard of the proposed amendment, the repercussions felt by victims in the civil arena would be unfortunate and unjustified.

This Note proposes that Aaron's Law should not be enacted because the impact of such reactionary legislation, prompted by prosecutorial indiscretion, exacts too high a toll on victims in the civil

[7] See United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (employees transmitting corporate information to ex-employee did not exceed authorized access as the employees had full access to the information); WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (former employee downloading and using corporate information for benefit of competitor is not exceeding authorized access for purposes of CFAA).

[8] Terms of service agreements, or terms and conditions agreements, are ubiquitous and usually encountered when creating online accounts, from email to LinkedIn accounts. They usually are accompanied by a checkbox with the text "I agree."

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

[10] *Id.*

arena who are seeking relief under a statute uniquely suited to ever-evolving computer technology. The language of the CFAA, as it currently exists, is well suited to be used as necessitated by pervasive, potentially damaging and evolving security vulnerabilities. Prosecutorial overreach as regrettable as it is, should not result in a limiting effect upon victims in the civil arena who have been harmed and should be entitled to specific and varied avenues of recovery. Part II of this Note provides a background of Aaron Swartz's rise as a prominent hacktivist and the unfortunate results of his indictment. Part III discusses the current Circuit split as well as cases interpreting the CFAA. Part IV discusses the case of *Robbins v. Lower Merion School District*, which demonstrates a circumstance to which the CFAA's broad language is well suited.[11] It is in light of the CFAA's legislative history, its interpretation by the Circuit Courts of Appeal and its real life impact in society as illustrated by Aaron's story, that this Note questions the soundness of legislation proposed under the guise of preventing the type of injustice that occurred in the case against Aaron.

II. AARON SWARTZ AND HIS LEGACY

A. Aaron Hillel Swartz

According to his obituary, Aaron Swartz was a programmer and "open-data crusader."[12] By the age of fourteen he had helped develop RSS software, which enables syndication of information on the internet.[13] The following year, he wrote code for Creative Commons, which promotes alternatives to standard copyright licenses.[14] At nineteen years of age, Aaron was a developer of the social networking news website Reddit, which is perhaps his best known, and certainly most utilized, project.[15] However, it was his conduct regarding his title as an "open-data crusader," that earned him the name recognition attributed to him today.

[11] Complaint, Robbins v. Lower Marion School Dist., 2010 WL 581739 (E.D. Pa. Dec. 16, 2010) No. 10CV00665 (hereinafter "Robbins Complaint").

[12] *See* Jack Schofield, *Obituary of Aaron Swartz*, THE GUARDIAN, (Jan. 13 2013, 2:22 P.M.), http://www.theguardian.com/technology/2013/jan/13/aaron-swartz.

[13] *See* Larissa MacFarquhar, *Requiem For a Dream*, THE NEW YORKER (Mar. 11, 2013), http://www.newyorker.com/reporting/2013/03/11/130311fa_fact_macfarquhar.

[14] *See id.*

[15] *See id.*

After his success developing Reddit, Aaron became a political activist, focusing on open access to academic information. He penned the well-known—in the open-access world— *Guerilla Open Access Manifesto* in July, 2008.[16] Later in his life, Aaron went on to fight against anti-piracy legislation in furtherance of his position regarding open-access to data on the internet.[17] By this time in his career as an activist, Aaron had already, allegedly, taken actions that placed him at serious odds with federal anti-hacking law.

B. PACER & RECAP

To better understand Aaron's motives and to better appreciate the negative ramifications of enacting Aaron's Law, it is important to briefly discuss Aaron's work advancing open access before the "MIT/JSTOR Incident"[18] that ultimately led to Aaron's federal indictment and subsequent suicide. In 2008, Aaron began work on a project that bears resemblance to the actions he took with JSTOR's database.[19] At the time, however, public court records were Aaron's target, as opposed to academic documents.[20] The court records Aaron sought to liberate are digitally stored by the Public Access to Court Electronic Records system, or PACER, which is an electronic public access web service that provides users with case and docket information from Federal Appellate, District and Bankruptcy courts.[21] On top of regular fees, PACER charges $0.10 per page retrieved.[22]

[16] Aaron Swartz, *Guerilla Open Access Manifesto*, (Jul. 2008), http://ia600808.us.archive.org/17/items/GuerillaOpenAccessManifesto/Goamjuly2008.pdf.

[17] Daniel Wagner and Verena Dobnik, *Swartz' Death Fuels Debate Over Computer Crime*, The Associated Press (Jan. 13, 2013, 8:25 P.M.), http://bigstory.ap.org/article/swartz-death-fuels-debate-over-computer-crime.

[18] The MIT/JSTOR Incident refers to allegations that, in 2011, Aaron Swartz illegally accessed JSTOR archives at Massachusetts Institute of Technology (MIT). JSTOR is a digital library of academic journals. *See New to JSTOR? Learn more about us*, JSTOR.ORG, http://about.jstor.org/10things (describing JSTOR's mission and designed functions). For additional discussion of the MIT/JSTORR Incident, *see infra* Section IIC.

[19] Sam Klein, *Aaron Swartz vs. United States*, THE LONGEST NOW (Jul. 24, 2011, 11:04 P.M.) http://blogs.law.harvard.edu/sj/2011/07/24/aaron-swartz-v-united-states/.

[20] *See id.*

[21] *Frequently Asked Questions*, PACER.GOV, http://www.pacer.gov/psc/hfaq.html (last visited Sep. 20, 2014).

[22] *See id.*

According to PACER, the case information made available to its users is a matter of public record and, as such, can be reproduced without permission.[23]

There are some open-access advocates who deride the fact that access to the court documents is subject to an out-of-date fee-based service.[24] PACER was, after all, originally designed to provide electronic access to court records in 1988.[25] . In 2007, four years after the U.S. Government Printing Office (GPO) first requested non-fee access to PACER, the Judicial Conference approved and instituted a one-year pilot to assess the effects of free public access to PACER documents.[26] The pilot program provided free public access to Federal court records at seventeen depository libraries.[27] Although slated to run for up to twenty-four months, the pilot would abruptly end just eleven months after its inception.[28] Even a Senator, Joe Lieberman of Connecticut, wrote to the judiciary inquiring as to whether PACER's fee structure complies with the legislation that funds the service.[29] According to Senator Lieberman, the fees collected by PACER are higher than the cost of dissemination.[30] This has resulted in a surplus of funds coming into the Judiciary Information Technology Fund as a result of fees being charged for obtaining public information.[31]

Enter Carl Malamud, an open-government advocate who is the President and Founder of Public.Resource.Org, a website which aims

[23] *See id.*

[24] *See* John Schwartz, *An Effort to Upgrade a Court Archive System to Free and Easy*, THE NEW YORK TIMES (Feb. 12, 2009), http://www.nytimes.com/2009/02/13/us/13records.html?_r=0 (Malamud stating "The system is 15 to 20 years out of date.").

[25] *See id.* (discussing the origins of PACER); *see also* Timothy B. Lee, *The inside story of Aaron Swartz's campaign to liberate court fillings*, ARS TECHNICA (Feb. 8, 2013), http://arstechnica.com/tech-policy/2013/02/the-inside-story-of-aaron-swartzs-campaign-to-liberate-court-filings/.

[26] *Public Access to Court Electronic Records (PACER)*, FDLP.GOV (Oct. 25, 2012), http://www.fdlp.gov/23-about/projects/140-pacer (last updated July 23, 2104).

[27] *Id.*

[28] *Id*.

[29] Joseph Lieberman, *Letter to the Honorable Lee H. Rosenthal* (Feb. 27, 2009), https://public.resource.org/scribd/13252410.pdf.

[30] *See id.*

[31] *See id.*

to make "government information more available."[32] Malamud encouraged fellow activists to go to the pilot libraries, where PACER access was free to the public, download as many documents as possible, and send them to him for publication on the internet.[33] Aaron answered Malamud's call to arms. Aaron recruited a friend to visit one of the pilot libraries where he extracted an authentication cookie[34] set by PACER's site.[35] This authentication cookie was not tied to any specific IP address.[36] Thus, the authentication cookie could be used by any computer on the internet to access the PACER service for free as if it were located in a pilot library.[37][38]

On September 29, 2009, it came to the attention of court administrators that the pilot library in Sacramento, while receiving the free service, would have accumulated a $1.5 million PACER bill.[39] By the time the hack was discovered and the pilot program was suspended, Aaron had downloaded 2.7 million documents from PACER.[40] Both the Federal Bureau of Investigation and the Department of Justice investigated Aaron's actions but filed no charges.[41] Today, those looking to obtain court documents from PACER without paying fees may do so by downloading a Firefox extension, known as RECAP, which searches for free copies of

[32] PUBLIC.RESOURCE.ORG-A501(C)(3) NONPROFIT CORPORATION, https://public.resource.org/index.html (last visited Sept. 20, 2014).

[33] Schwartz, *supra* note 24.

[34] MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 274 (11th ed. 2004) ([a cookie is] a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)).

[35] Lee, *supra* note 25.

[36] *See id.*

[37] Malamud did not support Swartz's use of an authentication cookie. An email to Swartz from Malamud reads "[T]his is not how we do things. . .[W]e don't cut corners, we belly up to the bar and get permission." Malamud told Swartz that if they were going to access PACER documents from sites other than the pilot libraries, then they would need a valid account and should pay the PACER fees, *available at* https://public.resource.org/aaron/pub/msg00197.html.

[38] *See id.*

[39] *See id.*

[40] *See id.*

[41] *See id.*

documents already uploaded by other users.[42] In its development RECAP was pre-loaded with the documents Swartz obtained from the PACER service.[43] Aaron's work with PACER was, indeed, an important first step toward breaking down the "paywall" that hinders full public access to court documents online.

C. The MIT/JSTOR Incident and the CFAA Violation

On January 6, 2011, Aaron allegedly broke into an MIT building where he infiltrated a closet containing computer networking equipment.[44] The networking equipment in this closet could provide access to MIT's computer network, as well as access to JSTOR archives, to those who are savvy enough to perform the functions necessary to access that information.[45] JSTOR is a not-for-profit digital library designed to help university and college libraries.[46] The subsequent prosecution alleged that Aaron broke into this closet in order to access and download a substantial portion of JSTOR's archive of digitized academic journal articles.[47] An estimated four million academic articles were downloaded from subscription-based JSTOR as a result of the network breach.[48]

A federal indictment was filed on September 12, 2012 alleging that Aaron contrived to, among other things, violate the CFAA.[49] The CFAA prohibits unauthorized access to any "protected computer," which is defined as any computer "in or affecting interstate commerce or communication."[50] Although the CFAA punishes seven activities,

[42] Bobbie Johnson, *Recap: cracking open US courtrooms*, THE GUARDIAN (Nov. 11, 2009), http://www.theguardian.com/technology/2009/nov/11/recap-us-courtrooms.

[43] Lee, *supra* note 25.

[44] *See* Application for Criminal Complaint (Jan. 7, 2011), http://mitcrimeclub.org /SwartzFilings-state.pdf.

[45] *See id.*

[46] *New to JSTOR? Learn more about us* (Sep. 20, 2014), http://about.jstor.org /10things (describing JSTOR's mission and designed functions).

[47] Application for Criminal Complaint, *supra* note 44.

[48] *See Alleged Hacker Charged With Stealing Over Four Million Documents From MIT Network*, US ATT'Y'S OFFICE DISTRICT OF MASS (Jul. 19, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/07/Swartz-Aaron-PR.pdf .

[49] *See* Superseding Indictment, United States v. Swartz, *supra* note 3.

[50] 18 U.S.C. § 1030(a)(2)(C) (2012); Id. § 1030(e)(2)(B).

its most important criminal provision is Section (a)(2)(C).[51] This section provides that any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer" violates the CFAA.[52] However, the CFAA does not define "exceeds authorized access," providing no guidance to distinguish between authorized and unauthorized forms of computer use.

Consequently, Aaron's actions constituted unauthorized access in violation of the CFAA. This indictment exposed Aaron to an extraordinary and disproportionate level of criminal liability in the range of thirty-five to fifty years imprisonment and approximately one million dollars in fines.[53] Regardless of which estimate is more accurate, it is certain that Aaron Swartz was living with the possibility of losing, in a practical sense, the very principle that he had been fighting for so fervently: freedom.

On January 11, 2013, two years to the day after his arrest on the indictment, Aaron committed suicide by hanging himself in his apartment.[54] Following this event, his family stated it was not merely a personal tragedy but "the product of a criminal justice system rife with intimidation and prosecutorial [sic] overreach."[55] They further intimated that "[d]ecisions made by officials in the Massachusetts U.S. Attorney's Office and at MIT contributed to his death."[56] Needless to

[51] Such proscribed activities include: obtaining information concerning national defense or foreign relations; the unauthorized/exceeds authorized access of information contained in a financial record of a financial institution, or information from a US Department or Agency; the obtainment of information in furtherance of a fraud; transmission of a program or code to cause damage to computer systems; communications threatening damage to systems for the purposes of extortion. *See* 18 U.S.C. 1030 §(a_(1)-(7).

[52] *Id*. § 1030(a)(2)(C).

[53] *Compare* Senate Request for Brief from Attorney General Eric Holder (2013), *available at* http://oversight.house.gov/wp-content/uploads/2013/01/2013-01-28-DEI-EEC-to-Holder-re-Aaron-Schwartz-prosecution.pdf (indicating 50 years imprisonment and $1 million in fines), *with* US ATT'Y'S OFFICE DISTRICT OF MASS Press Release, *supra* note 48, (indicating 35 years imprisonment and $1 million in fines).

[54] *See* Joe Kemp et al., *Aaron Swartz, co-founder of Reddit and online activist, hangs himself in Brooklyn apartment*, NY DAILY NEWS (Jan. 12, 2013), http://www.nydailynews.com/new-york/co-founder-reddit-hangs-brooklyn-apartment-article-1.1238852 (discussing the timing of Aaron's death).

[55] *See id.*

say, Aaron's legacy has continued to have an impact in the world of open-access activism.[57]

D. Introducing Aaron's Law: An Attempt to Limit the Broad Language of the CFAA

In January 2013, in the wake of Aaron's suicide, United States Representative Zoe Lofgren (D-CA 19th District) posted drafts of a bill she dubbed "Aaron's Law" to solicit public feedback.[58] In June 2013, Lofgren submitted a final version of the proposed amendment H.R. 2454.[59] Lofgren cites Aaron's victimization by overzealous prosecution under the CFAA as the inspiration for its overhaul.[60] The Congresswoman further indicated that the law must distinguish between everyday internet activity and criminal activity designed to cause serious damage to public or private business.[61] In her proposed law, Congresswoman Lofgren aimed to establish that the mere breach of terms of service, employment agreements, or contracts would not be considered to be violations of the CFAA.[62]

Aaron's Law radically changes the CFAA, as it removes the phrase "exceeds authorized access" and replaces it with "access without authorization."[63] Aaron's Law then goes on to define the phrase "without authorization" as "knowingly circumvent[ing] one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals" from accessing particular information.[64] This law, in turn, significantly narrows the scope of conduct that qualifies as hacking. One of its effects would be to limit a prosecutor's ability to charge a computer user under the CFAA with severe penalties for minor infractions.[65]

[56] *See id.*

[57] This note itself exists as a result of Aaron's legacy.

[58] Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*, (Jun. 20, 2013), *available at* http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/.

[59] Zoe Lofgren, *Rep Zoe Lofgren Introduces Bipartisan Aaron's Law*, U.S. HOUSE OF REPRESENTATIVES PRESS RELEASES (Jun. 20, 2013), http://lofgren.house.gov/news/documentsingle.aspx?DocumentID=365647.

[60] *See id.*

[61] *See id.*

[62] *See id.*

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

[64] *Id.*

[65] *See id.*

It is unclear whether Aaron's law would have prevented the injustice Aaron suffered had its provisions been in effect when he downloaded and disseminated the JSTOR documents. Put another way, could Aaron have been charged with violating of the CFAA if the amendment proposed in his name had been in effect when he downloaded the JSTOR documents? In order to analyze the question, however, we must also ask: were Aaron's actions "everyday internet activity" of the type that Congresswoman Lofgren cites in her goals for the Computer Fraud and Abuse Act? If Aaron's actions were not "everyday internet activity," then where should the line be drawn?

III. THE CFAA CIRCUIT SPLIT: CASE LAW INTERPRETING "EXCEEDS AUTHORIZED ACCESS"

There is currently a circuit split as to whether the term "exceeds authorized access," as defined in the CFAA, should be interpreted broadly or narrowly.[66] This section will explore the majority of Circuit Courts of Appeal which have ruled on the issue and have interpreted the meaning of the phrase broadly.[67]

A. EF Cultural Travel BV v. Explorica, Inc.

The First Circuit, in the case of *EF Cultural Travel BV v. Explorica, Inc.*, found that an employee who was in breach of a broad confidentiality agreement prohibiting certain use of company information was exceeding authorized access.[68] In *EF Cultural*, an employer sued former employees under the CFAA based on allegations that the former employees, who now worked for EF's competitor, Explorica, used their knowledge of EF's system to design a program that would gather information about EF's pricing for the purpose of undercutting its business.[69] The former employees previously had access to that kind of information.[70] The court ruled

[66] *See generally* Stephanie Greene & Christine Neylon O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281, 285 (2013).

[67] See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001), United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 854 (5th Cir. 2010); and Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[68] EF Cultural Travel BV v. Explorica, Inc. 274 F.3d 577 (1st Cir. 2001).

[69] *See id.*

[70] *See id.*

that the former employees' access under the circumstances of the confidentiality agreement, however, exceeded their authorized access.[71]

B. International Airport Centers, L.L.C. v. Citrin

The Honorable Judge Posner, writing for the Seventh Circuit, expounded on the approach found in *EF Culture* in finding that an employee was without authorization once he violated a duty of loyalty to his employer.[72] In *Int'l Airport*, an outgoing employee deleted files from a company laptop and loaded a secure erasure program onto the computer that prevented recovery of the system's memory.[73] Even though the defendant's employment agreement allowed him to "return or destroy" data on the laptop, the court found that his authorization terminated when his conduct went against the interests of his employer, and furthermore violated the duty of loyalty that he owed to his employer.[74]

C. United States v. Rodriquez

In *U.S. v. Rodriguez*, the Court of Appeals for the Eleventh Circuit found that the defendant had exceeded his authorization of computer access when he accessed personal information in his employer's database for non-business reasons.[75] The defendant argued that because he accessed only databases and because he was authorized to use the database as an employee, he had not exceeded his authorized access.[76] The court emphasized that the defendant's access had violated his employer's policy.[77]

D. United States. v. John

In *United States v. John*, the Fifth Circuit held that authorization, for purposes of the CFAA, "may encompass limits placed on the use of information obtained by permitted access to a computer system and

[71] *See id.*

[72] Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

[73] *See id.*

[74] *See id.*

[75] United States v. Rodriguez, 628 F.3d 1258, 1258 (11th Cir. 2010).

[76] *See id.*

[77] *See id.*

data available on that system."[78] The defendant was charged with violating § 1030(a)(2) based on her misappropriation of customer information to commit fraud.[79] The defendant contended that the statute does not prohibit unlawful use of information that was obtained through authorized access.[80] In its ruling, the court focused on the fact that the defendant was aware of company policies against such use and acted in violation of those.[81]

IV. The Folly in Aaron's Law

Aaron's law, though motivated by good intentions, imposes too great a cost on plaintiffs in the civil arena. The narrowing effect that Aaron's law would have on the CFAA's justifiably broad language could remove the possibility of a cause of action under the CFAA for plaintiffs who have been the victims of serious hacking.

A. Robbins v. Lower Merion School District: Removing a Remedy at Law

The current language of the CFAA provides for a civil cause of action under its provisions.[82] Aaron's law would narrow the scope of activity that is actionable under the CFAA's provisions and, consequently, remove a potential cause of action that currently exists for the benefit of individuals who have been a victim of hacking. One particularly illustrative case is *Robbins v. Lower Merion School District*.[83] *Robbins* is noteworthy not only because of its unsettling facts, but because it is an instance where the CFAA was used as a cause of action by users against their administrator.[84] All of the cases surveyed in Part III of this Note arise from an administrator or the government bringing an action against a user.[85] The change in

[78] *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded.").

[79] *See id.*

[80] *See id.*

[81] *See id.*

[82] *See* 18 U.S.C. § 1030 (2014).

[83] Robbins Complaint, *supra* note 11.

[84] *See generally id.* (noting that the use of the CFAA in a civil matter, by a user against administrators).

[85] *See generally id.* (noting the use of the CFAA in a civil mater, by a user against administrators); *see also generally* LVRC Holdings v. Brekka, 581 F.3d 1172

dynamic brings up a fundamental point that is missed by the proponents of Aaron's Law: the CFAA is, and should be used as, a tool for justice and not, as was Aaron's experience, a disproportionate response to questionably illegal hacktivism.

Robbins was a class action suit brought against a school district for allegedly spying on minor children in their homes via laptop webcams.[86] The laptops were issued to students of Lower Merion School District as part of the District's "one-to-one" laptop program which is described by the District itself as "one of the first in the nation."[87] All ninth grade students within the School District were issued laptops that they were allowed to keep for the duration of their high school career.[88] The Lower Merion School District's practice was to load a program called LANrev on all laptops in order to remotely manage and track misplaced and stolen one-to-one laptops.[89] In case of loss or theft, LANrev allowed school officials to turn on the lost or stolen laptop's webcam to snap photos and take screenshots of the laptop's surroundings.[90] According to the complaint, the School District made no reference to the fact that it could remotely activate the webcams without notice.[91] In fact, the LANrev software apparently disabled the cameras for users, leading the students to believe that the camera was just for show.[92]

(noting that the action was brought by an administrator) *and* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (noting that this action is a criminal matter brought against a user).

[86] Douglas Stanglin, *School district accused of spying on kids via laptop webcams*, USA TODAY, (Feb. 18, 2010, 5:42 PM), http://content.usatoday.com /communities/ondeadline/post/2010/02/school-district-accused-of-issuing-webcam-laptops-to-spy-on-students/1#.UscG8vRDsrU.

[87] Lower Merion School District, *One to One*, LMSD.ORG (last visited Sep. 8, 2014), http://www.lmsd.org/academics/instructional-tech/one-to-one/index.aspx.

[88] *See id.*

[89] Bill Detwiler, *LANrev to lose Theft Track feature following Pa. School spying allegations*, TECHREPUBLIC (Feb. 23, 2010, 1:20 PM PST), http://archive.is /5Lct.

[90] Chloe Albanesius, *Another Lawsuit Filed Over School Webcam Spying*, PCMAG, (Jul. 30, 2010). http://www.pcmag.com/article2/0,2817,2367209,00 .asp.

[91] Robbins Complaint, *supra* note 11.

[92] Jeff Porten, *School District Faces Lawsuit Over Webcam Spying Claims*, PCWORLD, (Feb. 23, 2010, 4:40 PM), http://www.pcworld.com/article/190101 /article.html.

The School District's procedures for activating the tracking software were at best unorganized, and at worst abused or neglected. Approximately ten school officials had authorization to activate the tracking.[93] There were a handful of cases in which a laptop was recovered but the webcam tracking remained active for weeks after, snapping photos of unsuspecting minor students.[94] An investigator for the School District indicated that, in approximately one dozen cases, it wasn't apparent why the webcam was activated at all.[95] Students reported the webcam's green light turn on, signaling that the webcam had been activated, but they dismissed the phenomenon as a glitch.[96] By the time the tracking was brought to light, approximately 56,000 images had been captured by laptop webcams without students' knowledge.[97]

Lower Merion's clandestine laptop tracking program had gone largely undetected until November of 2009. According to the complaint, it was on November 11, 2009, that the plaintiffs were, for the first time, informed of the capability and practice of the School District concerning LANrev webcam tracking.[98] On that day, the plaintiff was approached by Harriton High School's Assistant Principal Lindy Matsko. [99] Matsko informed the plaintiff that the School District believed he had engaged in improper behavior in his home.[100] As proof of such behavior, Matsko cited as evidence a photograph that had been taken by the plaintiff's School District issued laptop.[101] Matsko further informed the plaintiff of the School District's ability to remotely activate the webcam he had kept in his room at home.[102]

Among other causes of action, the plaintiffs alleged that the School District had exceeded its authorized access in violation of the CFAA in

[93] The Associated Press, *School took 56,000 images on student laptops*, USA TODAY, (Apr. 20, 2010, 3:18 PM), http://usatoday30.usatoday.com/news/nation/2010-04-19-laptop-photos_N.htm. (hereinafter "School took 56,000 images")

[94] *See* Stanglin*, supra* note 86.

[95] *See id.*

[96] *See id.*

[97] School took 56,000 images, *supra* note 93.

[98] Robbins Complaint, *supra* note 11.

[99] *See id.*

[100] *See id.*

[101] *See id.*

[102] *See id.*

that it exceeded its authorized access to the plaintiff's laptop.[103] The plaintiffs requested, and were granted, an injunction prohibiting the activation of the tracking software.[104] The implications of what the webcam images showed were enormous. The legal director for the Pennsylvania chapter for the American Civil Liberties Union commented that "[t]his is fodder for child porn."[105]

After litigation, the Lower Merion School District paid approximately $610,000 to settle *Robbins* and a companion suit arising out of similar circumstances.[106] The judge ordered that the temporary injunction prohibiting the activation of laptop computers issued to its students would be superseded by a permanent injunction to the same effect.[107]

Robbins illustrates how the CFAA can be used as a tool by plaintiffs who deserve a range of counts seeking recovery when someone has exceeded their authorized access to their computer. The plaintiffs in *Robbins* had their privacy interests violated by a complete abuse of a computer system by the school district. Without the current language of the CFAA, the plaintiffs would have had one less cause of action and one less reason for Lower Merion School District to settle.

B. Statutory Interpretation Supports the CFAA's Broad Language

Maxims of statutory interpretation support a broad reading of the CFAA, rather than a narrow reading that Aaron's Law calls for. Under the CFAA, "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[108] A narrow interpretation of the phrase may be inconsistent with the last words of the definition as set forth by Congress in the statute itself: "obtain or alter information in the computer that the accesser is not entitled *so* to obtain or alter."[109] "So" means "in the state or manner

[103] *See id.*

[104] Robbins v. Lower Merion School Dist., 2010 WL 3421026 (E.D. Pa. 2010).

[105] *FBI Probing School Webcam Spy Case*, CBSNEWS, (Feb. 19, 2010, 10:00 AM),http://www.cbsnews.com/news/fbi-probing-school-webcam-spy-case/.

[106] John P. Martin, *Lower Merion district's laptop saga ends with $610,000 settlement*, PHILLY.COM (Oct. 12, 2010), http://articles.philly.com/2010-10-12/news/24981536_1_laptop-students-district-several-million-dollars.

[107] Robbins v. Lower Merion School Dist., *supra* note 104.

[108] 18 U.S.C. § 1030(e)(6) (2012).

[109] *See id*. (emphasis added).

indicated or expressed."[110] The inclusion of the word "so" in 1030(e)(6) is unambiguous in that someone exceeds authorized access when he obtains information he is not entitled to obtain or alter *under the circumstances*. The word "so" also indicates that the accesser may have been entitled to obtain the same information for other purposes, but not for illegitimate purposes that contravene the purpose for which restricted access is required.

For instance, suppose an employer grants an employee access to all information on its computer system, but restricts access authority by indicating that the employee only has permission to access medical records on the computer system during the workday, with the written approval of a supervisor. If these circumstances are not present, the employee is not authorized to access medical records and therefore has no right to access the medical records. If the employee accesses a medical record in contravention of his employer's restrictions, he is not "entitled so to obtain" such information and has exceeded his authorized access.

Thus, "exceeds authorized access" indicates that someone exceeds authorized access by obtaining information in a manner which is restricted even if the accesser is entitled to obtain the same information under non-restricted circumstances. There is nothing in §1030 that purports to allay employer-employee use-based restriction agreements. Thus, an employee exceeds authorized access if he acts in contravention of his employer's use-based access restriction by obtaining information for a prohibited reason.[111]

A somewhat unique aspect of the CFAA as a statute is that, besides criminal penalties, it also provides a civil remedy based upon the same "without or exceeding authorized access" standard that is applicable to the criminal penalties.[112] This dual nature makes for a delicate balance when policy and emotion meet, as happened in Aaron's case.

[110] "*So*," MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary /so (last visited Sep. 20, 2014).

[111] *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."); Cont'l Group, Inc. v. KW Prop. Mgmt, *LLC*, 662 F. Supp. 2d 1357, 1372 (S.D. Fla 2009) (finding a "substantial likelihood" that defendant exceeded authorization when she downloaded files for her own purposes, where her employer's computer access policies stated that its computers "are provided for business use" and any equipment is provided "to be used solely for [the employer's] purposes").

[112] *Id*.

Because the Computer Fraud and Abuse Act is a statute with both civil and criminal implications, any discussion of possible ambiguities should touch upon, at least briefly, the possible applicability of the Rule of Lenity to the statute's analysis. Generally, when a term in a criminal statute is ambiguous, that term should be construed narrowly in favor of the defendant.[113] However, the "simple existence of some statutory ambiguity is not sufficient to warrant application of the rule of lenity, for most statutes are ambiguous to some degree."[114] Further, a criminal statute is not improper simply because it might apply to a broad range of conduct.[115] Thus, reliance on the Rule of Lenity to force a narrow interpretation of the term "exceeds authorized access" is tenuous.

C. Aaron's Law Would Reverse Decades of Legislative Intent

The current statutory definition of "exceeds authorized access" was enacted in 1986.[116] The reason for enacting this phrase was to substitute:

> for the more cumbersome phrase in present 18 U.S.C. 1030(a)(1) and (a)(2), "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend". The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase "exceeds authorized access" is defined separately in Section (2)(g) of the bill.[117]

Clearly, the phrase replaced a "more cumbersome" one that specifically spoke to access in violation of use-based restrictions.

> The legislative history of §1030 noted and accepted that the CFAA, as amended, "specifically covers the conduct of a person who deliberately breaks into a computer without authority, *or* an insider who exceeds authorized access, and thereby obtains classified information and then communicates that information to

[113] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1172, 1134 (9th Cir. 2009) (noting that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.").

[114] Muscarello v. United States, 524 U.S. 125, 138 (1998).

[115] United States v. Banks 514 F.3d 959, 967 (9th Cir. 2008).

[116] S. REP. 99-432, at 7 (1986), 1986 U.S.C.C.A.N. 2479, at 2485.

[117] S. REP. 99-432, at 9 (1986); 1986 U.S.C.C.A.N. 2479, at 2486.

> another person, or retains it without delivering it to the proper authorities.[118]

Further, as amended in 1996, the statute intended to close "gaps in the law to protect better the confidentiality, integrity, and security of data and networks."[119] Thus, the legislative history shows that Congress intended the term to have a broad meaning and applicability.

Further, the legislative intent of the word "loss" must be examined, as for purposes of the CFAA it indicates a broad meaning and application. The CFAA defines "loss" as

> any reasonable cost to any victim, including (1) the cost of responding to an offense, (2) conducting a damage assessment, and (3) restoring the data, program, system or information to its condition prior to the offense, and (4) any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[120]

The legislative history of the 1996 amendments to the CFAA contemplates that "although there is arguably no 'damage,' nevertheless, the victim suffers 'loss.'"[121] Further, it has been noted that "Congress intended the term 'loss' to target remedial expenses borne by a victim that could not properly be considered direct damage caused by a hacker."[122] Such broad language leaves significant discretion to the plaintiff in a civil case or the prosecutor in a criminal case.

D. Lessig's Take: Aaron Swartz Did Not Violate the CFAA as Written

In order to gain a better understanding of the possible implications of Aaron's Law on the MIT/JSTOR incident, it will be helpful to understand Aaron's actions in light of the theories of Lawrence Lessig.[123] Lessig is an advocate of political beliefs, including such as

[118] S. REP. 104-357, 6.

[119] *See id.*

[120] 18 U.S.C. § 1030 (e)(11) (2014).

[121] S.REP NO. 104-357, at 11 (1996).

[122] *In re* DoubleClick Inc. Privacy Litig., 154 F.Supp.2d 497, 521 (S.D.N.Y. 2001).

[123] Lawrence Lessig is the Roy L. Furman Professor of Law and Leadership at Harvard Law School, and serves as the director of the Edmond J. Safra Center for Ethics at Harvard University. Among other accomplishments, Lessig clerked for Judge Richard Posner on the 7th Circuit Court of Appeals, as well as Justice

the need for a second Constitutional Convention.[124] Lessig met Aaron when Aaron was in his early teens.[125] However, Lessig describes Aaron, who was much younger than him, as his mentor.[126]

Lessig defines "hacking" as "the use of technical knowledge to advance a public good."[127] He acknowledges that Aaron was a hacker while distinguishing the title from a "cracker" or one whose intent is not to advance public good.[128] He and Aaron saw the impediments set in the way of open-access to information as a kind of social corruption.[129] With his view that social corruption is hampering open-access to information, Lessig took a sympathetic approach to Aaron's actions in the MIT/JSTOR incident.

According to Lessig, Aaron's actions could not have amounted to unauthorized access in violation of the CFAA because there was no traditional "hacking" involved in the MIT/JSTOR incident.[130] In support of this assertion, he explains that Aaron noticed that the URL on JSTOR's website ends with a number that references a specific article.[131] When Aaron recognized the pattern, he realized that it would be simple to write a "script"[132] to download all of the articles.[133] Aaron

Antonin Scalia of the Supreme Court of the United States. LESSIG: ABOUT, http://www.lessig.org/about/ (last visited Sep. 4, 2014).

[124] Alesh, Houdek, *Has a Harvard Professor Mapped Our the Next Step for Occupy Wall Street?*, THE ATLANTIC (Nov. 16, 2011), *available at* http://www.theatlantic.com/politics/archive/2011/11/has-a-harvard-professor-mapped-out-the-next-step-for-occupy-wall-street/247561/.

[125] Harvard Law School, *Lessig on "Aaron's Laws – Law and Justice in a Digital Age,"* YOUTUBE (Feb. 20, 2013) a*vailable at* http://www.youtube.com/watch?v=9HAw1i4gOU4 (hereinafter "Lessig on Aaron's Laws").

[126] *See id.*

[127] *See id.*

[128] *See id.*

[129] *See id.*

[130] *See id.*

[131] The number is 2.

[132] A computer script is a list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes on a local computer or to generate Web pages on the Web. For example, DOS scripts and VB scripts may be used to run processes on Windows machines, while AppleScript scripts can automate tasks on Macintosh computers. ASP, JSP, and PHP scripts are often run on Web servers to generate dynamic webpage content. "*Script*" TECHTERMS.COM, http://www.techterms.com/definition/script (last visited Oct. 6, 2014).

[133] *Lessig on Aaron's Laws*, *supra* note 125.

simply had to write a script that would generate numbers that fall within the range that JSTOR assigns its articles.[134] Aaron was able to download such a massive volume of documents via this method.[135] Lessig explains that when JSTOR noticed the volume of data being downloaded from Aaron's single IP address,[136] they blocked him.[137] Without missing a step, Aaron took a new IP address. [138] JSTOR became aware of the volume being downloaded on the new IP address, so they blocked a range of IP addresses.[139] Blocking a range of IP addresses rendered JSTOR practically useless on the MIT campus.[140] JSTOR then determined the MAC address of Aaron's computer.[141] A MAC address is a unique identification number tied directly to a specific computer.[142] Aaron then found a way to "spoof" a new MAC address.[143]

Instead of "hacking," Lessig describes these actions as "technical tricks" to enable the download of many articles.[144] Presumably, Lessig would even stretch so far as to categorize Aaron's actions as

[134] *See id.*

[135] *See id.*

[136] Also known as an "IP number" or simply an "IP," [an IP Address] is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. "*IP Address*" TECHTERMS.COM, http://www.techterms.com /definition/ipaddress (last visited Oct. 6, 2014).

[137] *Lessig on Aaron's Laws*, *supra* note 125.

[138] *See id.*

[139] *See id.*

[140] *See id.*

[141] *See id.*

[142] Stands for "Media Access Control Address." A MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed. "*MAC Address*" TECHTERMS.COM, http://techterms.com/definition/macaddress (last visited Oct. 6, 2014).

[143] *Lessig on Aaron's Laws*, *supra* note 125; Another way of spoofing takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. "*Spoofing*" TECHTERMS.COM, http://techterms.com/definition/spoofing (last visited Oct. 6, 2014).

[144] *See id.*

Congresswoman Lofgren sees them: everyday internet activity.[145] However, even Lessig must admit that, while Aaron was permitted to download some JSTOR articles by way of the fact that he was a Harvard fellow, he was not permitted to take all of the articles as it was almost certainly his intention.[146]

In exploring Aaron's motivations for his actions, Lessig points to a conference that Aaron attended where JSTOR indicated that the cost of making its database available to the public would be $250,000,000.[147] He then contends that this conference is where Aaron began preparing for the MIT/JSTOR incident.[148]

E. Other Proposed Reform: The Electronic Frontier Foundation

Lessig views Aaron's Law as an incomplete reform.[149] He points to the Electronic Frontier Foundation (EFF), which proposes three goals for reform of the CFAA.[150] The EFF is a self-proclaimed champion of the public interest "in every critical battle affecting digital rights."[151] According to its website, the EFF is made up of lawyers, political analysts, activists, and technologists, which consequently places it at the forefront of open-access issues.[152] Thus, it has devised the following three goals for reform of the CFAA.

First, there should be no criminal exposure for violating private agreements or duties.[153] The EFF acknowledges that Aaron's Law, as proposed by Lofgren, focuses exclusively on this issue.[154] The EFF claims that it is dangerous for private contracts to be enforceable via punishment of severe criminal penalties subject to vast prosecutorial

[145] See Lofgren, supra note 58 (discussing the problems with the CFAA as written, including the criminalization of some "everyday internet activity").

[146] *Lessig on Aaron's Laws*, *supra* note 125.

[147] *Lessig on Aaron's Laws*, *supra* note 125.

[148] *See id.*

[149] *See id.*

[150] *See id.*

[151] *About EFF*, ELECTRONIC FRONTIER FOUNDATION (last visited Sep. 8, 20140), https://www.eff.org/about.

[152] *See id.*

[153] Parker Higgins, *Critical Fixes for the Computer Fraud and Abuse Acts*, Electronic Frontier Foundation (Jan. 29, 2013), https://www.eff.org/deeplinks/2013/01/these-are-critical-fixes-computer-fraud-and-abuse-act.

[154] *See id.*

discretion.[155] Eviscerating the CFAA by enacting Aaron’s Law, however, could have unintended consequences, by removing a cause of action from those seeking justice. The EFF does, however, indicate that users may face civil or criminal liability under its first proposed goal for more egregious violations, such as destroying data.[156] This goal quickly begins to smack of the same prosecutorial discretion permitted by the CFAA in its current form. Thus, it seems a rather bland reform.

Second, the EFF proposes that, if one is allowed to access information, “doing it in an innovative way shouldn’t be a crime.”[157] It claims that, as it is written today, the CFAA exposes users to criminal liability if they engage in “commonplace ‘circumvention’ techniques like changing IP addresses, MAC addresses, or browser User Agent headers.”[158] Certainly, as commonplace as the EFF would like to think those advanced circumvention techniques are, it would be hard pressed to show that the average user possesses such technical knowledge or that he even knows it is possible. This hole in the reasoning behind the second goal is difficult to swallow.

The EFF further contends that “technological barriers increasingly serve purposes far removed from preventing computer intrusion.”[159] Even the most arbitrary of technological barriers, however, at its very least, serves to prevent intrusion’s unfortunate cousin: misuse.

The third and final goal that the EFF would like to see accomplished in reforming the CFAA is to make penalties more proportionate to offenses.[160] It contends, correctly, that several sections of the CFAA are redundant and vulnerable to prosecutors who seek to pursue multiple offenses based on the same behavior.[161] It is with this proposal that the EFF makes its most reasonable and well-thought out point. Limiting the opportunity for prosecutors to “double dip” by pursuing multiple offenses based on one act would have substantially decreased the criminal exposure and possible prison time Aaron was facing as a result of the MIT/JSTOR incident.[162] Further,

[155] *See id.*

[156] *See id.*

[157] *See id.*

[158] Higgins, *supra* note 153.

[159] *See id.*

[160] *See id.*

[161] *See id.*

[162] *See id.*

limiting the high proportion of punitive measures imputed to each violation would have substantially limited the total amount of prison time Aaron was facing. Regardless, just because sentencing for a first offense is stiff does not make it any less legal, so long as it complies with constitutional requirements, which the CFAA undoubtedly does. There are other circumstances, however, that shine a different light on the Computer Fraud and Abuse Act.

V. CONCLUSION

When assessing future reform of the CFAA, it is important to take heed of and contemplate the distinction between situations like the MIT/JSTOR incident and what happened in *Robbins*. In Aaron's case, the CFAA was abused by means of prosecutorial indiscretion; smothering him with the stress of a potentially long prison sentence and vast financial penalties. Aaron was accused of violating the CFAA by trying to sidestep a network administrator in order to spread access to knowledge. In *Robbins,* the CFAA was used as a cause of action by computer users against an administrator who took liberties with computer privacy. The soundest approach to the broad language of the CFAA is not its evisceration, which would have prevented the plaintiffs in *Robbins* from alleging a count under the CFAA. The soundest approach, what justice calls for as it does in the implementation of all laws, is sound discretion. In essence, we don't need to amend the CFAA by way of reactionary, knee-jerk legislation motivated and driven by prosecutorial indiscretion. The history, both legislative and common law, behind the CFAA's broad language demonstrates sound policy objectives, as is easily illustrated by *Robbins*. No, what we need isn't a change in the law, "we need prosecutors who know the difference between Aaron and evil."[163]

[163] *Lessig on Aaron's Laws*, *supra*, note 125.