COMPUTER FRAUD AND ABUSE OR PROSECUTORIAL FRAUD AND ABUSE: TIME FOR CHANGE

Victor Manolache[*]

INTRODUCTION

On January 11, 2013, Aaron Swartz hung himself.[1] Swartz was 26, and despite his youth, was already a well-known and accomplished programmer. Most notably, Swartz helped develop Creative Commons, and his company Infogami merged with Reddit.[2] Many prominent computer programmers and scholars considered Swartz a genius and a friend, and mourned his death.[3] Tim Berners-Lee, the inventor of the World Wide Web, reacted to Swartz' death saying "Aaron dead. World wanderers, we have lost a wise elder. Hackers for right, we are one down. Parents all, we have lost a child. Let us weep."[4]

Almost two years to the day before his death, on January 6, 2011, Swartz was arrested in connection with a series of network break-ins of MIT's computer system. The break-ins spanned a few months and Swartz carried them out from a storage closet on MIT's campus.[5] Between September 2010 and January 2011, Swartz, a Harvard graduate student at the time, physically entered MIT campus, and from a storage closet, hooked up his computer to MIT's network. He spoofed his ID on the network to remain undetected and downloaded millions of academic journals from JSTOR.[6]

On July 11, 2011, a Federal grand jury indicted Swartz for wire fraud, computer fraud, unlawfully obtaining information from a protected

---

* Case Western Reserve University School of Law, JD 2015.

1. *See* John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide,* N.Y. TIMES (January 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html.

2. *Id*. Swartz later became a partner in Reddit.

3. *See infra* note 13.

4. *Sir Tim Berners-Lee pays tribute to Aaron* Swartz, THE TELEGRAPH (Jan. 14, 2013), http://www.telegraph.co.uk/technology/news/9800147/Sir-Tim-Berners-Lee-pays-tribute-to-Aaron-Swartz.html.

5. Schwartz, *Internet Activist, a Creator of RSS, is Dead*.

6. Id; JSTOR is a digital academic library that contains academic journals, books, and primary sources. It is mainly licensed to colleges and universities, but unaffiliated individuals may purchase access. *See* http://www.jstor.org/.

computer, and recklessly damaging a protected computer.[7] The charges carried a maximum sentence of 35 years in prison. Swartz refused a plea deal, and on September 12, 2012 Federal prosecutors added nine more felony counts under the Computer Fraud and Abuse Act ("CFAA")[8], increasing the maximum prison time to 50 years.[9]

In all, Swartz was charged with two counts of wire fraud[10] and eleven violations of the Computer Fraud and Abuse Act.[11] Usually, wire fraud charges involving computers are prosecuted along with the CFAA.[12] Thus the essence of the prosecution's case depended on their interpretation and application of the CFAA.

Reaction to Swartz' death was very opinionated, dividing legal scholars and prompting a public debate about whether Swartz was overcharged[13] – or whether he even committed a crime to begin with.[14] At Swartz' funeral, his father, Robert Swartz, condemned the prosecution, saying "[Aaron] was killed by the government, and MIT betrayed all of its basic principles."[15] Prosecutor Carmen Ortiz declined to comment, but her

7. Schwartz, *Internet Activist, a Creator of RSS, is Dead*

8. *See* 18 U.S.C. § 1030 (2008).

9. Schwartz, *Internet Activist, a Creator of RSS, is Dead*

10. *See* 18 USC § 1343 (2008).

11. *Id.*

12. *See* Orin Kerr, *The Charges Against Aaron Swartz (Part 1: The Law)*, THE VOLOKH CONSPIRACY (Jan. 14, 2013 2:50 AM), http://www.volokh.com/2013/01/14/aaron-swartz-charges/.

13. *Compare* Lawrence Lessig, *Prosecution as a Bully*, (Jan. 13, 2013) http://www.bloombergview.com/articles/2013-01-17/the-overzealous-prosecution-of-aaron-swartz (strongly expressing that the prosecution should not have charged Swartz), *accord*, Jennifer Garnick, *With the CFAA, Law and Justice Are Not The Same: A Response to Orin Kerr*, THE CENTER FOR INTERNET LAW AND SOCIETY (Jan. 14, 2013 11:55 PM), http://cyberlaw.stanford.edu/blog/2013/01/cfaa-law-and-justice-are-not-same-response-orin-kerr, Stephen L. Carter, *The Overzealous Prosecution of Aaron Swartz*, BLOOMBERG VIEW (Jan. 17, 2013 6:30 PM), http://www.bloombergview.com/articles/2013-01-17/the-overzealous-prosecution-of-aaron-swartz, James Boyce, *The Prosecution of Aaron Swartz: A Reply to Orin Kerr*, THE HUFFINGTON POST (Jan. 18, 2013 10:00 PM), http://www.huffingtonpost.com/james-boyle/prosecution-aaron-swartz_b_2508242.html, *with* Kerr, *The Charges Against Aaron Swartz supra* note 12 at 2.

14. *See* Lessig, *Prosecution as a Bully*; *See also* David Boeri, *Retired Federal Judge Joins Criticism Over Handling Of Swartz Case*, WBUR, http://www.wbur.org/2013/01/16/gertner-criticizes-ortiz-swartz (interviewing retired federal judge who stated: "Just because you can charge someone with a crime, just because a technical crime has been committed, doesn't mean you should").

15. Sandra Guy, *Aaron Swarz was 'killed by government,' father says at funeral,* CHICAGO SUN-TIMES (Jan. 15, 2013), http://www.suntimes.com/business/17594002-420/aaron-swartz-memorialized-at-service.html (last accessed December 21, 2013).

husband replied through Twitter, writing: "Truly incredible that in their own son's obit[uary] they blame others for his death and make no mention of the 6 month offer."[16]

Perhaps Robert Swartz' words were an emotional reaction by a mourning father, but many legal scholars' reaction targeted the CFAA's harsh criminal treatment of Swartz in light of an intrusion that was neither malicious nor prolonged.[17] Jennifer Garnick, director of Civil Liberties for the Center of Internet and Society at Stanford Law School wrote: "The CFAA is incredibly broad and covers swaths of online conduct that should not merit prison time." A former criminal defense attorney and friend of Swartz', Garnick concluded: "Exactly because the CFAA arguably applies to Aaron's alleged actions, it should be amended."[18]

Others differed. Professor Orin Kerr[19] believed the charges were based on an appropriate reading of the law.[20] But Kerr recognized that the CFAA, in its current form, lead to undesired outcomes: "The problem raised by the Swartz case is ... [that] felony liability under the statute is triggered much too easily. The law needs to draw a distinction between low-level crimes and more serious crimes, and current law does so poorly..."[21] The back and forth correspondence, publicized through blogs and online editorials[22] differed in sympathy expressed towards Swartz, but agreed in principal that the CFAA no longer worked well as a viable, well-balanced, computer crime statute.

Originally, the CFAA created three federal crimes limited to federal

16. Karen McVeigh, *Aaron Swartz: husband of prosecutor criticizes internet activist's* family, THE GUARDIAN (Jan. 15, 2013), http://www.theguardian.com/technology/2013/jan/15/aaron-swartz-husband-prosecutor-criticises.

17. *See* Lessing, Garnick, Carter, Boyce *supra* note 13.

18. Jennifer Garnick, *Towards Learning from Losing Aaron Swartz: Part 2*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 15, 2013 3:54 PM), http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2.

19. Orin S. Kerr is a nationally recognized computer crime law scholar, and current George Washington Law School professor, *See http://www.law.gwu.edu/Faculty/profile.aspx?id=3568* (last accessed December 19, 2013).

20. Orin Kerr, *The Charges Against Aaron Swartz (Part 1: The Law)*, THE VOLOKH CONSPIRACY (Jan. 14, 2013 2:50 AM), http://www.volokh.com/2013/01/14/aaron-swartz-charges/ ("I think the charges against Swartz were based on a fair reading of the law. None of the charges involved aggressive readings of the law or any apparent prosecutorial overreach. All of the charges were based on established case law").

21. Orin Kerr, *Aarons Law, Drafting the Best Limits of the CFAA, And a reader Poll on A Few Examples*, THE VOLOKH CONSPIRACY (Jan. 27, 2013 11:46 PM) http://www.volokh.com/2013/01/27/aarons-law-drafting-the-best-limits-of-the-cfaa-and-a-reader-poll-on-a-few-examples-part-i/.

22. *See supra* note 13 at 2.

interest computers. Those crimes were: accessing national security information, private financial information, or a computer owned by the US Government without authorization.[23] A federal interest computer was any computer on which national security or private financial information was found.[24]

The CFAA's scope has been expanded through revisions. Today, the CFAA is over-inclusive of criminal activity, creating over-criminalization that is only checked by prosecutorial discretion. There are two reasons for this. First, Congress never defined "authorization." This creates vagueness and has resulted in a Circuit split between the Seventh and Ninth Circuit. Second, the CFAA is a bright line rule with no exceptions.[25]

This Note shall explain both problems and offer a possible solution to each. Section I discusses the history of computer crime law. Section II presents the circuit split and offers a solution. Section III discusses consequences of the CFAA's bright line approach. Section IV proposes an amendment to the CFAA that creates an exception for types of uses that, although unauthorized, should not merit criminal prosecution. Swartz' case is revisited, and the discussion from the previous sections is applied.

I. HISTORY OF COMPUTER CRIME LAW

A. Pre-CFAA

Computer misuse prosecution can be traced back to 1972.[26] Defendants were charged with computer crimes under existing laws such as trespass, burglary, and theft, because no specific computer crime statute existed.[27] Conceptually, the cyber world and physical world were different, and courts struggled to find a satisfactory approach to prosecuting computer crime.

Prosecution under a theft statute might have required a property interest in the computer and a showing that the defendant's misuse of the computer deprived the owner of their property interest.[28] In *United States v.*

23. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV 1561, 1564 (2010) (discussing Congressional intent for enacting a computer crime statute in 1984).

24. Kerr, *Vagueness Challenges* at 1564 (defining federal interest).

25. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. REV. 1596, 1601 (2003) (questioning why the "same one-size-fits-all prohibitions on unauthorized access" still govern in light of rapid technological advancement since 1984 that has made a bright line rule obsolete in the face of modern society).

26. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. REV. 1596, 1605 (2003).

27. *See* Kerr, *Cybercrime's Scope*, at 1605.

28. *Id.* at 1609.

Seidlitz,[29] a former employee of a military contractor used a stolen password, logged onto the company's network, downloaded, and made a copy of software. Identifying a property interest was easy: the company owned the software and it was protected by password. Showing how, by making a copy of the software, defendant depraved the company of the software was difficult. The original copy remained in the company's possession, but it was clear the defendant's action impacted the company's financial interests.[30]

Because of such trivialities, courts took a case-by-case, results-oriented approach. If computer misuse caused harm, then property was taken and defendants were liable.[31] If misuse did not cause appreciable harm, then property was not taken and defendants had not committed a crime.[32] In *Seidlitz*, the defendant intended to use the software for his own business.[33] This would have caused the company that owned the software financial harm by depriving it of a competitive advantage, and the Fourth Circuit found him guilty of wire fraud.[34]

The pre-CFAA approach premised liability on an actual showing of harm, evaluated case-by-case. If computer misuse passed a certain threshold of harm, it was considered theft, and, prosecuted.[35] If the Government did not demonstrate that defendant's conduct met the burden of harm, the case was dismissed.[36]

B. 1984: First Computer Crime Legislation

The CFAA was codified as part of the Comprehensive Crime Control Act of 1984 and named the "Crime Fraud and Abuse Act" in 1986.[37] In the last 30 years, the CFAA has been amended five times. With each amendment, the scope of the CFAA has been enlarged. In 1984, the CFAA was a narrow and specific piece of legislation, limited to unauthorized

29. *See* United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (ruling that jury could find defendant had fraudulent intent to use the information from plaintiff's computer system).

30. *See* Seidlitz, 589 F.2d at 160.

31. *See* Kerr, Cybercrime's Scope at 1611 ("Faced with such riddles, courts tended to reach results-oriented outcomes").

32. *See* Kerr, *Cybercrime's Scope*, 1611.

33. *See* Seidlitz, 589 F.2d at 154 ("In June, 1975, Seidlitz resigned this job and returned to work at his own computer firm in Alexandria, Virginia").

34. *Id.* at 160.

35. *See* Seidlitz *supra* at note 30.

36. *Compare Seidlitz with* United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997) ("Curiosity on the part of an IRS officer may lead to dismissal, but curiosity alone will not sustain a finding of participation in a felonious crime scheme to deprive the IRS of its property").

37. *See* Kerr, *Vagueness Challenges* at 1564-1565 (discussing history of CFAA).

access of a "federal interest" computer, defined as a computer that held national security or financial information, or was property of the Government.[38]

The first offense, codified at § 1030(a)(1), prohibited unauthorized access to a computer for the purpose of obtaining national security information with intent, or reason to believe, the information would be used against the USA's interests.[39] The second offense, codified at §1030(a)(2), prohibited unauthorized access to a computer to obtain financial information from an institution or consumer reporting agency.[40] The third offense, codified at §1030(a)(3) prohibited a person from unauthorized access to a Government computer if doing so affected the computer's operation.[41] The purpose of all three statutes was to protect three specific Government interests.[42]

The next two amendments, in 1986 and 1994, brought additional liabilities and a civil remedy, but the scope of the CFAA remained limited to "federal interest computers".[43]

C. 1996: Significant Expansion

Congress expanded the CFAA in three significant ways in 1996. Congress' intent was "addressing in a single statute the problem of computer crime".[44] First, a new felony enhancement section for crime and extortion was added. The two other changes created more significant legal consequences. The scope of "unauthorized access" in 1030(a)(2) was expanded beyond only financial information. And, the limitation to "federal interest computer" was expanded to "protected computer."[45]

The scope of 1030(a)(2), prohibiting unauthorized access to financial information, was expanded to include unauthorized access to obtain *any* information of *any* kind *if* the conduct involved an interstate or foreign

38. *See* Kerr, *Vagueness Challenges* at 1564.

39. *See* 18 U.S.C. 1030(a)(1)-(a)(3) (1984).

40. *Id.*

41. *Id.*

42. *See* Kerr, *Vagueness Challenges* at 1564 ("All three statutes were tailored to a specific government interest: national security, financial records, and government property").

43. *Id.* at 1564-1566; *See also* 18 U.S.C. 1030(a)(4)-(6); *See also* 1030(g) (1994) (allowing private cause of action to recover damages resulting from unauthorized use).

44. S.REP. NO. 104-357, at 5 (1996) ("As intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology").

45. *See* Kerr, *Vagueness Challenges* at 1566-1567.

communication.[46] Finally, and most significantly, Congress expanded the CFAA's limitation to "federal interest computers" was expanded to "protected computers."[47] A "protected computer" was defined to include any computer "used in interstate or foreign commerce or communication."[48] This gave the Government jurisdiction over virtually any business's computer that was connected to the Internet.[49]

D. Post 9-11

In response to the September 11, 2001 terrorist attacks, Congress expanded the meaning of "protected computer" to include computers outside the United States "used in a matter that affects interstate or foreign commerce or communication of the United States."[50]

E. 2008: Revisiting 1996

The requirement of an "interstate or foreign communication" as means was removed from 1030(a)(2), so that, under 1030(a)(2)(C), *any* unauthorized access to *any* protected computer that results in retrieval of any information of any kind is covered by the CFAA.[51]

But, more importantly, the definition of "protected computer" was again expanded. The word "or affecting" was added, and currently the phrase now reads, "used in *or affecting* interstate or foreign commerce or communication."[52] "Affecting interstate commerce" is a term of art, showing Congressional intent as far as legally permissible under the Commerce Clause. In application, the Commerce Clause gives the Government power to "regulate purely local activities that are part of an economic class of activities that have a substantial effect on interstate

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.* at 1568.

51. *Id.* at 1569.

52. *Id.; See also*18 U.S.C. 1030(e)(2)(B) (2008); *See also* 18 U.S.C. 1030(e)(2) (defining protected computer to include any computer: "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States").

commerce."[53] In effect, the CFAA has, almost blanket jurisdiction to criminalize any form of unauthorized access.[54]

Throughout every revision, Congress expanded the scope of unauthorized use, but Congress never defined authorization. Furthermore, no exceptions were added, despite constant expansion of criminalization, which engulfed previously innocuous actions. The result in the present day is, that the CFAA is a blanket rule. Once triggered, its only constraint is prosecutorial discretion. The remainder of this Note discusses issues arising from this.

II. CIRCUIT SPLIT

A. Defining Authorization

The Seventh Circuit interprets authorization more expansively than the Ninth Circuit. The split emerged from employer-employee disputes about when an employee acts without authorization or exceeds authorization. The Seventh Circuit ruled that an employee's authorization is terminated when the employee's actions violate a duty of loyalty owned to the employer.[55] The Ninth Circuit has declined to interpret authorization so broadly.[56] Because Congress has not defined authorization, the Ninth circuit interpreted the word according to its common meaning. It ruled that an employee's authorization only ends if the employer revokes it, even if the employee uses his authorization in a way that is harmful to the employer or in violation of a state law.

B. The Seventh Circuit

In *International Airport Centers, LLC v. Citrin*[57] the Seventh Circuit ruled that an employee's use of his employer's computer terminated his authorized access because he used it in a way that violated a duty of loyalty he owed the employer. Defendant Citrin was an employee of International Airport Centers ("IAC"). He was given a laptop by IAC to perform his job and was authorized to "return or destroy" data on the laptop before returning it.[58] Citrin quit and started a competing business. Before returning the computer, Citrin deleted all data and uploaded a secure-erasure

53. *See* Gonzales v. Raich, 545 U.S. 1, 17 (2005) (ruling that Congress is allowed to regulate marijuana grown for home use because the aggregate effect is to reduce demand for marijuana in the national marijuana market).

54. *See* Kerr, *Vagueness Challenges* at 1571 (concluding that after 2008, the CFAA basically covers everything with a microchip).

55. *See* International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

56. *See* LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

57. *Citrin*, 440 F.3d at 419.

58. *Id.*

program to prevent discovery and recovery of the files he deleted.[59]

IAC sued Citrin under the CFAA for, among other reasons, intentionally accessing a protected computer without authorization or exceeding authorization.[60] Citrin argued that he was authorized to delete files by IAC before returning the computer, and, therefore he did not exceed authorization when he deleted the files and uploaded the secure-erasure program.[61] The District Court agreed and dismissed the case, but the Seventh Circuit reversed and remanded. The Seventh Circuit reasoned that it was unlikely IAC intended Citrin to destroy files that IAC did not have duplicates of, or which would show Citrin's misconduct.[62] Citrin used his authority to deprive IAC of something they wanted. This constituted a breach of a duty of loyalty he owed IAC. Violating that duty triggered termination of his authorized use of the computer.[63]

C. The Ninth Circuit

The Seventh Circuit's ruling in *Citrin* implies that the manner in which an employee uses his access can terminate his authorization. IAC did not explicitly tell Citrin his access was terminated. Citrin's use of the computer terminated his authority because he covered up his misconduct.

In contrast, the Ninth Circuit declined to follow *Citrin* when it decided *LVRC Holdings LLC v. Brekka*.[64] The Court implied that the CFAA is primarily an access statute, not a use statute. It ruled that access could only be terminated by the employer's manifestations towards the employee, not by the employee's use, even if the employee violated a duty of loyalty owed to the employer or a state law.[65]

LVRC Holdings ("LVRC") operated a substance abuse rehabilitation center. It hired Brekka to oversee Internet marketing programs.[66] Brekka had a personal business that provided consulting to rehabilitation centers. In September 2003, using LVRC's computer, Brekka emailed himself and his wife LVRC usage statistics. The emailed documents included budget information, patient admission reports, and names of past and current patients. This is the type of information Brekka's personal consulting business provided to rehabilitation centers that competed with LVRC's center. In October 2003, Brekka left LVRC. A year later when LVRC

59. *Id.*

60. *Id; See also* 1030(a)(5)(A) (2008) ("intentionally causes damage without authorization, to a protected computer").

61. *See Citrin*, 440 F.3d at 419.

62. *Id.* at 421.

63. *Id.*

64. *See Brekka*, 581 F.3d at 1134.

65. *Id.* at 1135.

66. *Id.* at 1129.

uncovered Brekka's emails from September, they sued him under the CFAA.[67]

LVRC alleged that, under *Citrin*, Brekka intentionally accessed its computer without authorization, or, in excess of authorized access.[68] The District Court concluded Brekka had authorization because he was employed by LVRC in September 2003 and LVRC did not present any confidentiality agreement requiring Brekka to keep emailed documents confidential.[69] On appeal, the Ninth Circuit agreed.

In rejecting *Citrin*, the Ninth Circuit interpreted authorization by the word's plain meaning because the CFAA does not define it. The plain meaning of authorization is "permission or power granted by an authority."[70] The Court concluded this meant authorization depended on the employer's action. *Citrin's* interpretation did not comport to the plain language because the Seventh Circuit interpreted authorization by the manner in which the employee used his employer's computer. In contrast, the Ninth Circuit said an employee remains authorized to use a computer even if the employee uses his authorization in a way that harms the employer or breaks a state law because authorization is determined by the employer's assent of authorization to the employee.[71]

Brekka was authorized to use LVRC's computer. He likely violated a duty of loyalty to LVRC because he could, and likely did, give LVRC's information about potential and past patients to rival rehabilitation center facilities. But the Ninth Circuit did not consider how Brekka used the information as a factor. Therefore Brekka's violation of his duty to LVRC was inconsequential to whether or not he exceeded authorization.

D. Nosal: Brekka Applied

In *United States v. Nosal*,[72] the Ninth Circuit applied *Brekka* to a criminal case. The Court dismissed five counts of CFAA violations against a former employee and his accomplices (together, the "defendants") because the Government failed to show that defendants' accessing confidential information on their employer's network was without authorization or in excess of authorized access.[73] Nosal was a former

67. *Id.* at 1130.

68. *Id.; See also* 18 U.S.C. 1030(a)(2) (2008) (" … intentionally accesses a computer without authorization or exceeds authorized access …"); *See also* 1030(a)(4) (2008) (" … knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access … ").

69. *See Brekka* 581 F.3d at 1132.

70. *Id.* at 1133.

71. *Id.*

72. *See* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (dismissing five counts of unauthorized use under CFAA).

73. *Id.* at 856.

executive at Korn/Ferry International ("Korn/Ferry"), an executive search firm. He left Korn/Ferry to start a competing firm and asked three former colleagues, who were still employed at Korn/Ferry, to access Korn/Ferry's computer system and give him confidential information consisting of source lists, names, and client information.[74]

Nosal was argued before *Brekka* was decided. The Government argued that Korn/Ferry's computer use policy gave employees certain rights that, when violated, resulted in exceeding authorized access. Presumably, accessing confidential information with the intent to use it against Korn/Ferry terminated their authorized use.[75] Nosal argued that "exceeds authorized access" refers to someone who is authorized to view only certain information but views additional information he is unauthorized to view.[76] Initially, District Court rejected Nosal's argument, but reversed and dismissed after *Brekka* was decided.[77] On appeal, the Ninth Circuit originally reversed the District Court, but granted an interlocutory appeal. On review de novo, the Ninth Circuit re-instated the District Court's original judgment and dismissed all CFAA charges against Nosal.[78]

The Ninth Circuit declined the Government's broader interpretation. Specifically, the Court noted that Congress enacted the CFAA in 1984 to deal with computer hacking, not with misappropriation of information or with the breach of confidentiality agreements by employees.[79] The Government's construction would have expanded the CFAA's scope beyond computer hacking and criminalized many innocuous computer uses that people would have no reason to believe constitute a federal crime.[80] Furthermore, employers could manipulate computer-use and personnel policies traditionally governed by tort and contract law into policies governed by criminal law. Since policies vary from company to company, criminal liability could be premised on subjective standards.[81]

Here, like in *Brekka*, defendants had authorization to access the information. The Court noted that the Government could prosecute Nosal

74. *Id.*

75. *Id.* at 857.

76. *See Nosal* 676 F.3d at 856.

77. *Id.*

78. *Id.*

79. *Id.* at 858 ("While the CFAA is susceptible to the government's broad interpretation, we find Nosal's narrower one more plausible. Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking").

80. *Id.* at 859 ("The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime").

81. *Id.* (generally discussing hypotheticals in which an employee may violate a company policy, such as internet use, and be criminally liable for an innocuous act such as visiting ESPN.com).

and his accomplices on other charges, but not under the CFAA because using the confidential information against Korn/Ferry's interests did not establish lack of authorization.

E. Solution to the Split

The CFAA is not an effective statute because it can be interpreted in two equally plausible ways. The Supreme Court should adopt *Brekka* because it is the more narrow reading of the law and the vagueness doctrine[82] requires courts to reject the broader view of authorization in *Citrin*.[83]

Adopting *Brekka* would eliminate vagueness as to what authorization means. The vagueness doctrine requires the legislature to establish general guidelines.[84] Establishing the literal definition of "authorization" would create a clear guideline for law enforcement. *Citrin* fails to do this because it would criminalize millions of innocuous acts by turning everyday computer use into a potential crime.[85] On the other hand, *Brekka* would exclude routine employee computer use from criminal liability.[86]

Furthermore, interpreting authorization by its literal meaning is most fair to defendants.[87] *Brekka* would put responsibility on employers to clearly define rules and enforce them through tort and contract law in civil court.[88] Under *Citrin*, employers would have an unfair advantage in disputes with employees, because along with a civil remedy, they would have the force of criminal enforcement for subjective circumstances

82. *See* Kolender v. Lawson, 461 U.S. 352 (1983) (establishing that vagueness doctrine does not require actual notice, only that "legislature establish general guidelines to govern law enforcement").

83. Kerr, *Cybercrime Vagueness* at 23-24 (arguing that courts should adapt *Nosal*).

84. *See Lawson*, 461 U.S. at 361 (ruling that a California statute requiring loiterers to carry "credible and reliable" identification violated the due process clause because it did not clarify what satisfies "credible and reliable identification" thereby facilitating arbitrary law enforcement).

85. *See* Kerr, *Cybercrime Vagueness* at 25 (concluding that routine employee use for personal reasons would renter a criminal anyone who even for one second uses their computer in a way not benefitting the employer).

86. *Id.* (reasoning that it is unrealistic to have a rule criminalizing all use against the employer's interest because virtually every person uses their employer's computer for personal use, and an instantaneous unauthorized use should not trigger criminal liability).

87. *See Brekka,* 581 F.3d at 1134 ("The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants").

88. *See Nosal*, 676 F.3d at 859 (("Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law").

traditionally governed by tort and contract law.[89]

A narrower interpretation of authority would reduce overcharge. Nosal was charged with over twenty counts, and five were dismissed because they were CFAA charges.[90] In situations such as *Nosal*, the prosecution could stack the case against a defendant by overcharging him.[91] This would lead to the defendant facing a higher prison term under the federal sentencing guidelines. The prosecution could then offer a plea deal and pressure defendant into taking it.[92]

Finally, *Brekka's* reading is closer to Congressional intent. In 1984, Congress intended to address computer hacking, not employer-employee disputes.[93] If Congress intended conduct like Nosal's to be criminally liable under the CFAA, it should act.

III. A BRIGHT LINE AND A PROPOSAL FOR CHANGE

A. The Need for Congressional Reform

The CFAA is over-inclusive for two reasons. First, as stated in the preceding section, it criminalizes innocuous crimes. Second, it does not have exceptions permitting certain classes of persons or excluding certain types of infractions. Currently, the only filter on the CFAA is prosecutorial discretion. This is not assuring, because it's not clear the Government, or at least every individual prosecutor, can be trusted to make a responsible, sense-making, and unbiased decision in every case.[94]

The Supreme Court can solve the first problem by solving the Circuit Split in favor of *Brekka*. The Court cannot solve the second. That requires Congressional action to amend the CFAA.

B. Lack of Exceptions

89. *Id.*

90. Kerr, *Vagueness Challenges* at 1587 (using *Nosal* as an example of prosecutorial overreach because the CFAA's vagueness allows prosecution "based on aggressive readings of the statute".

91. *Id.*

92. This is discussed in Section II, and suggests that Swartz was overcharged and pressured to accept a plea.

93. *See Nosal* 676 F.3d at 858 ("The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer "without authorization." According to the government, *that* prohibition applies to hackers, so the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose").

94. Judge Kozinski, Chief Judge of the Ninth District expressed this in *Nosal* at 562("The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor. … And it's not clear we *can* trust the government when a tempting target comes along").

The CFAA can be reduced to a bright-line rule drawn around a box: if a person has no authorization to open the box, or exceeds authorization, then access to information inside the box is outlawed.[95] But authorization is subject to interpretation, especially in a networked environment.[96] For this reason, unless the unauthorized access is done with malice or involve matters of national security,[97] disputes regarding "authorization" under the CFAA are best left to be disputed in civil court between the parties involved. Those parties are best able to address the malleable aspects of authorization.

Authorization is malleable because it is not expressed the same universally. Terms of service, pop-ups, cultural expectations, and employment contracts are all different ways authorization may be conveyed, or revoked.[98] Outside of the computer context, disregarding any of them might not be a crime, or even a civil offense.[99] But, in drawing a bright line rule around the box the CFAA protects the box's contents regardless of social values or other existing laws about the information in the box.

Such a rigid law is generally against social convention. Other laws regarding right to information balance protection of information with social goods.[100] For example, copyright law protects the copyright holder but makes an exception for fair use.[101] Trade secrets protect against misappropriation and must be specifically defined. Classified information is marked, but cultural and legal history permits journalists and news outlets to report on its issues without prosecution.[102]

---

95. Jennifer Garnick, *Towards Learning from Losing Aaron Swartz: Part 2*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 15, 2013 3:54 PM), http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2 (interpreting the CFAA as a bright-line rule around a box with no regard for what's in the box, even if it includes otherwise public data); *See also supra* note 25 at 4.

96. *Id.*

97. *See* 18 U.S.C. 1030(d)(2) (2008) ("The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data … ").

98. Garnick, *Losing Aaron Swartz: Part 2* (writing from her experience as a former criminal defense lawyer).

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id; See also* New York Times Co. vs. United States, 403 U.S. 713 (1971) (ruling that the New York Times could publish the Pentagon Papers, which were still classified at the time, without risk of censorship and punishment. This overruled President Richard Nixon's claimed executive authority to prevent the New York Times from publishing classified information in its possession).

The Supreme Court ruling in favor of *Brekka* will not address the CFAA's rigidity. Under *Brekka*, if a person does not have authorization, or mistakenly goes beyond their authorization on a network, they may have committed a federal crime, despite having done an innocuous thing.[103] *Brekka* would eliminate vagueness and concretely define authorization, but it would not create an exception for situations when use is unauthorized but does not rise to the level of criminality. For these reasons, Congress must step in and create an exception.

C. Prosecutorial Discretion

CFAA criminal prosecution inherently lends itself to abuse of prosecutorial discretion.[104] The problem is two-fold – part human and part systematic. Prosecutors decide in each case whether to charge a person, and if so, with what charges.[105] The other problem is systematic: federal sentencing is determined by federal sentencing guidelines.[106] In practice, the guidelines set "draconian sentences"[107] that almost always increase upwards and never down.

CFAA sentencing is determined according to a calculation of loss incurred. Sentences are more harsh and unpredictable than in other federal cases because the CFAA's definition of loss is very broad and not limited to foreseeable damages.[108] Furthermore, the prosecution's burden of proof

---

103. *See* Stephen L. Carter, *The Overzealous Prosecution of Aaron Swartz*, BLOOMBERG VIEW (Jan. 17, 2013 6:30 PM), http://www.bloombergview.com/articles/2013-01-17/the-overzealous-prosecution-of-aaron-swartz (giving an example of how, if a workplace policy does not allow internet access for any personal use, and an employee accesses their bank account at work to pay a bill, they've committed a felony under the CFAA because they've exceeded their authorized use); *See generally* Kerr, *Cybercrime's Scope* at 1650-1651 (Discussing how in contrast to current law, his proposal would limit scope of unauthorized access, and laws "would no longer threaten to transform disagreements with computer owners into criminal violations").

104. *See* Garnick, *Losing Aaron Swartz: Part 2* ("Voluminous, overlapping charges may be typical …) *See generally* Kerr, *The Criminal Charges Against Aaron Swartz (Part 2: Prosecutorial Discretion)*, THE VOLOKH CONSPIRACY (Jan. 16, 2013 11:34 PM), http://www.volokh.com/2013/01/16/the-criminal-charges-against-aaron-swartz-part-2-prosecutorial-discretion/ (discussing that in general, the charges against Swartz were not outside the usual conduct of prosecutors, who overcharge defendants to induce plea deals).

105 *See* Kerr, *Criminal Charges Against Swartz*, THE VOLOKH CONSPIRACY (Jan. 14, 2013 2:50 AM) http://www.volokh.com/2013/01/14/aaron-swartz-charges/ ("The DOJ has the discretion to charge cases or not, and prosecutors can agree to different plea deals or even agree to have charges dismissed").

106. *See* Garnick, *Losing Aaron Swartz: Part 2* (discussing federal sentencing based on her experiences as a criminal defense attorney and according to federal sentencing guidelines).

107. *Id.*

108. *Id.*

is very low.[109] The effect is that, many defendants are cornered into accepting a plea deal as their only rational legal option, rather than opt for a trial and risk significant prison time and more expenses.

D. Overcharge

In many typical federal cases, the Government overcharges the defendant.[110] The prosecution then offers the defendant a deal: plead guilty to a felony and waive the right to appeal in return for the prosecution's suggesting a significantly reduced sentence.[111] If the defendant refuses the offer, the prosecutor typically returns to the grand jury and adds more charges. Many times, charges overlap and add more potential prison time.[112]

Overcharging gives the prosecution an unfair advantage. The defendant must defend against every charge, but the Government often needs to prove only one charge to obtain the maximum sentence.[113] Furthermore, overcharging is likely to predispose the jury to find the defendant guilty because jurors are more likely to infer the defendant's guilt from the sheer volume of charges against him.[114] A case tried under the CFAA often requires lay jurors to understand technology, physics, and economic concepts that are outside of common knowledge.[115] The jury's predisposition towards the prosecution, and likely layman knowledge of disciplines a jury must grasp well if the defendant is to be successful, reduces the defendant's chance of acquittal even more.[116]

E. Federal Sentencing

A high flexibility in calculating loss and a low standard of proof give the prosecution unfettered discretion to successfully argue for higher or lower sentences. Federal sentences are usually determined by federal

---

109. *Id.*

110. *Id* ("Voluminous overlapping charges may be typical, but they can give unfair advantage to the prosecution"); *See also* Orin Kerr, *The Criminal Charges Against Aaron Swartz (Part 2: Prosecutorial Discretion)*, THE VOLOKH CONSPIRACY (Jan. 16, 2013 11:34 PM) http://www.volokh.com/2013/01/16/the-criminal-charges-against-aaron-swartz-part-2-prosecutorial-discretion/ (writing that overcharge is a frequent tactic used by prosecutors to scare defendants into pleading guilty).

111. *See* Garnick, *Losing Aaron Swartz: Part 2* (drawing conclusions based on her experiences defending criminal defendants under information statues, including the CFAA).

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

sentencing guidelines in proportion to defendant's past record and the offense characteristics.[117] CFAA sentencing is harsher and less predictable than sentencing under other federal statutes because CFAA sentencing is determined by loss. Loss is defined as reasonable loss to any victim, and is not capped to foreseeable damages.[118] This is in contrast to similar non-CFAA fraud crimes, to which guidelines include only reasonable foreseeable monetary harm.[119] The prosecution in a CFAA case can calculate loss as narrowly or as broadly as it wants.

The standard of proof to show loss is low. Federal sentencing is generally done by preponderance of evidence.[120] A judge need only make a "reasonable estimate of loss." Since the prosecution may find a wide range of reasonable loss in any given case, sentencing unpredictable.[121]

F. Overall Effect

The practical effect of overcharge and sentencing guidelines is to pressure the defendant into accepting the prosecution's plea deal. Many innocent persons plead guilty because it is the most rational choice given the odds, even if it means serving prison time.[122] Often, the plea deal is so reduced, that the difference between risking trial and accepting a plea deal could be the risk of serving a few years in prison versus serving a few months.

G. Applied to Swartz

Recall that Swartz hacked into JSTOR, from MIT's computer system, and downloaded millions of articles from JSTOR's secure servers.[123] Swartz' prosecution followed the pattern outlined above. Prosecutors filed duplicative charges[124] carrying up to 50 years in prison.[125] Then,

---

117. *Id.*

118. *Id.*; *See also* 1030(d)(12) ("the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service").

119. *See* Garnick, *Losing Aaron Swartz: Part 2* (explaining how loss is calculated in a typical CFAA pleading).

120. *Id.*

121. *Id.*

122. *See* Garnick, *Losing Aaron Swartz: Part 2* (implying many innocent persons plead guilty to not risk a significant amount of prison time).

123. *See* Introduction.

124. *See* Garnick, *Losing Aaron Swartz: Part 2*(stating she, and others, believe Swartz was overcharged); *See also supra* note 14 at 2.

125. *See* Introduction.

prosecutors offered a plea deal. Supposedly, Swartz had three options: 1. plead guilty to 13 felonies and the Government would argue a six month prison term and Swartz' lawyer could have argued for less; 2. plead guilty to all 13 felonies and the Government would have argued a 4 month sentence; or 3. risk trial, and the Government would argue for seven years.[126]

H. Swartz Overcharged

Swartz was likely overcharged for two reasons. First, the discrepancy between prison-time recommended by the Government if Swartz went to trial versus if he took a plea deal. Second, the Government's calculation of loss.

The plea deal was coercive. If Swartz took the deal, the Government would have argued for 4 or 6 months incarceration. If he went to trial, the Government would have argued for 7 years. Some say Swartz should have pled guilty.[127] But the lenient offer ignores the unaccounted cost of being a convicted felon. Often, felons face social stigma, loss of job opportunities, and loss of voting rights, which they may never gain again.[128] Furthermore, the judge is not restricted to the Government's sentencing suggestion. Pleading guilty to a felony would have meant Swartz was facing at least 5 years prison time according to the sentencing guidelines. Even if the Government argued four to six months, Swartz had no absolute guarantee he would only have served that much.[129]

Second, the Government's calculation of loss could have ranged from a few thousand dollars to millions of dollars. The Government alleged that JSTOR's information was "valued in the tens of thousands of dollars at the time."[130] Swartz downloaded around 4.8 million articles from JSTOR. The cost to download was $19.00. The Government could have argued Swartz caused anywhere from $10,000 to $91 million in damages to JSTOR.[131]

The practical result is that, the spectrum of loss calculations would have allowed the Government to argue for any sentence it wanted, and likely convince a jury by a preponderance of evidence.[132] Furthermore, the Government ignored the fact that Swartz had settled out of court with JSTOR.

---

126. *See* Garnick, *Losing Aaron Swartz: Part 2* (commenting on alleged plea bargains Swartz was offered by the prosecution).

127. *See supra* note 16, at 2.

128. *See* Garnick, *Losing Aaron Swartz: Part 2* (discussing extrajudicial reasons defendants have for not pleading to a much lesser sentence).

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.*

On June 3, 2011, Swartz and JSTOR entered into a civil agreement.[133] Pursuant to the agreement, Swartz certified that he made no copies of the downloaded files. He delivered the only existing disk of the files to JSTOR's attorneys, who delivered the disk to the United States Attorney's Office. Furthermore, Swartz paid $1,500 in damages and $25,000 in attorneys' fees.[134] Afterwards, JSTOR considered the matter closed, and publicly declared its preference that Swartz not be charged. On July 19, 2011, Swartz' federal indictment was unsealed[135] and JSTOR was one of the parties subpoenaed. In response, JSTOR issued the following public statement: "As noted previously, our interest was in securing the content. Once this was achieved, we had no interest in this becoming an ongoing legal matter …"[136] Up until Swartz' suicide, JSTOR's attorneys contacted lead prosecutor Carmen Ortiz numerous times, reaffirming their wishes that charges against Swartz be dropped.[137]

Swartz was charged regardless of his intent, the operational reality of his actions, or the relationship between him and JSTOR - extrajudicial realities that should have mitigated the force of the Government's prosecution.

IV. PROPOSED LEGISLATION

A. Reform

It is inequitable and unconscionable for a hacker like Swartz to be charged without taking into account the operational reality of his actions. He returned the copied materials and settled out of court. In return, JSTOR publicly campaigned for charges to be dismissed. JSTOR's public actions suggest that there are societal conventions that the prosecutors should have taken notice of, but did not.

The CFAA is a bright line rule around a box. Once triggered, it does not take notice of the contents inside the box, or who is entitled to them. In this case, JSTOR was the owner of the box, but liability was triggered, regardless of JSTOR's wishes. Rather than a bright line rule governed by prosecutorial discretion, the CFAA should create a bright line exception to a general rule stating that in order for criminal liability to be established, an infraction must pass a certain threshold.[138] If the infraction does not pass

133. *Report to the President MIT and the Prosecution of Aaron Swarz* at 41-42, http://swartz-report.mit.edu/docs/report-to-the-president.pdf (last accessed December 19, 2013) (recounting Swartz' plea with JSTOR in a comprehensive MIT investigative report about the incident).

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *See generally* Kerr, *Cybercrime's Scope at 1648-1649 (suggesting similar mindset to a proposed restructuring of the CFAA).*

the threshold, then legal remedies should be limited to civil litigation. Congress should change the CFAA, either through amendment, or new legislation. A suggestion is the "Hacker's Rule" discussed below.

B. The Hacker's Rule

The Hacker's Rule proposition is a two-part rule that abolishes the current bright line rule. Recall that the current rule establishes criminal prosecution whenever a person uses a computer without authorization, or exceeds authorization. The Hacker's Rule would create an exception for when a person who uses a computer without authorization, or exceeds authorization is not criminally liable.[139] A hacker would be criminally liable if he: 1) acts with malicious intent or 2) if no malicious intent or no federal interest, then his unauthorized intrusion was reckless enough that, regardless of any civil or extrajudicial settlement with the injured party, traditional criminal conventions would seek to punish.

C. Malicious Intent

Professor Orin Kerr stated the charges against Swartz were "pretty much what any good federal prosecutor would have charged."[140] At the same time, Kerr recognized that Swartz' case demonstrates that criminal prosecution under the CFAA is triggered too quickly. Kerr wrote that "[t]he law needs to draw a distinction between low-level crimes and more serious crimes, and current law does so poorly"[141]

Privacy and computer security activist Chris Soghoian, a senior policy analyst at the American Civil Liberties Union, suggests that existing law needs to differentiate between malicious, and non-malicious intrusions by hackers for the purpose of showing off their skill or spreading information they believe should be available publicly.[142]

D. Reckless Use

The second part of the Hacker's Rule creates a general rule, that if the

139. The Hacker's Rule is a proposition for criminal offenses and does not preclude civil liability triggered due to a breach of terms, an employment contract, or other infraction by which the user accessed the computer without authorization.

140. *See supra* note 20, at 3.

141. Orin Kerr, *The Criminal Charges Against Aaron Swartz (Part 2: prosecutorial Discretion)*, THE VOLOKH CONSPIRACY (Jan. 16, 2013 11:34 PM), http://www.volokh.com/2013/01/16/the-criminal-charges-against-aaron-swartz-part-2-prosecutorial-discretion/.

142. *See* Daniel Wagner and Verona Dobnik, *Swartz' Death Fuels Debate Over Computer Crime*, THE BIG STORY (Jan 13, 2013), http://bigstory.ap.org/article/swartz-death-fuels-debate-over-computer-crime (discussing policy experts' opinions).

hacker's intent is not malicious, the prosecution must show it was, nevertheless, reckless enough that the person should be punished, even if, the person settled with the injured party. Furthermore, this part creates a bright line exception to the general rule of recklessness, that if the conduct is contrary to a federal interest, then the person is prosecuted.

Congress would have to define federal interest. A place to start is in § 1030(d)(2) of the CFAA. That section lists instances, involving national security issues that the FBI may investigate.[143] Congress could combine this with the original definition of federal interest.[144] A possible new definition of federal interest could be: unauthorized access to national interest information, personal financial information, Government owned computers or a violation of §1030(d)(2). This would be the bright line exception that automatically triggers liability. The rest would be evaluated case by case.[145] The Government would have the burden of showing that an outcome reached between two parties, such as the settlement between Swartz and JSTOR is inequitable.

E. Application to Swartz

It is unlikely that Swartz would have been prosecuted under the proposed Hacker Rule. First, Swartz did not have malicious intent.[146] Second, the damage he caused was sufficiently cured by his extrajudicial agreement with JSTOR and was not reckless enough that traditional criminal sanctions should seek to punish.[147]

F. Swartz' Conduct

Applying the first prong, Swartz did not have any malicious intent. The

143. *See* CFAA 1030(d)(2) (2008) ("The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations").

144. Federal interest was originally defined as a computer that held national security, or financial information, or was property of the government. *See* Section I(A) *supra* at 6.

145. *See* Section I(A) *supra* at 5-6.

146. *See* James Boyce, *The Prosecution of Aaron Swartz: A Reply to Orin Kerr*, THE HUFFINGTON POST (Jan. 18, 2013 10:00 PM), http://www.huffingtonpost.com/james-boyle/prosecution-aaron-swartz_b_2508242.html (implying that, given Swartz' motivation for past projects, he was likely motivated by his desire to do what he considered a public good).

147. *See* Kerr, *Cybercrime's Scope*, at 1656-7 (discussing traditional theories of punishment).

Government alleged he accessed JSTOR with intent to defraud[148], but Swartz' mental state suggested otherwise.[149] Even if the Government argued that, Swartz' download could have deprived JSTOR of a competitive advantage in attracting customers to sign up, Swartz' intent was not to enter the online journal database market with articles downloaded from JSTOR.[150]

G. Damage is Curable by Extrajudicial Agreement with JSTOR

As mentioned above, Swartz and JSTOR reached a civil settlement. As part of the settlement, Swartz paid monetary damages and gave a disk of the files he downloaded to JSTOR's attorneys. The attorneys then handed the disk to the Department of Justice. This is an equitable solution. JSTOR'S primary concern was the whereabouts of the data. Also, they were compensated for their troubles. There was no future threat because Swartz returned the files and declared he had not kept a copy for himself. In return, JSTOR had shown good faith and publicly supported him.

Traditionally, criminal liability is limited in scope to conduct that satisfies utilitarian and retributive goals.[151] Utilitarianism seeks to punish a defendant in a way that is also beneficial to society, and goals include deterrence, rehabilitation, and incapacitation.[152] The retributive goal is to align the scope of criminal activity with societal values of justice.[153] For computer crime, the most important is deterrence.[154] Criminal prosecution should benefit society by discouraging future harmful conduct.[155] JSTOR's

148. *See* Grand Jury Indictment, U.S. v. Aaron Swartz, 1:11-cr-10260-NMG at 10, (D. Mass., filed Sep. 12, 2012), *available at* http://tech.mit.edu/V132/N40/aaronsw/superseding-indictment.pdf (alleging Swartz sought to defraud by concealing his identity on the network).

149. *See* Lawrence Lessig, *Prosecution as a Bully*, (Jan. 13, 2013). http://www.bloombergview.com/articles/2013-01-17/the-overzealous-prosecution-of-aaron-swartz (offering possible mental state of Swartz by rebuking the notion that academic journals are a profitable endeavor with strong language, and, pointing out that many of Swartz' projects, such as Reddit and Creative Commons, were done with the mindset of building a free service for users).

150. *See generally* Section I(A) discussing *Seidlitz* at 4. There, the defendant intended to use copied material in his own business; *See generally* Section II. *Citrin, Brekka,* and *Nosal* all involved defendants who intended to use information in a competing business. There, an allegation of the plaintiffs was intention to defraud by exceeding authorized access. Here, the facts are distinguished because Swartz did not intend to enter a for-profit business with the articles he downloaded.

151. *See* Kerr, *Cybercrime's Scope*, at 1656-1657 (applying traditional theories of criminal punishment to computer crimes).

152. *Id* at 1656.

153. *Id* at 1657.

154. *Id* at 1656.

155. *Id.*

public support of Swartz is an indication that there might not be a societal benefit from prosecuting him.

The Government did not have a clear federal interest. Swartz did not hack into a financial institution, or a Government computer, or compromise national security. The articles Swartz downloaded were academic, and available to anyone who wished to sign up for JSTOR's services.[156] The Government would have been unlikely to show Swartz was so reckless as to be charged criminally in order to deter future behavior or correct a wrong, as the Hacker's Rule would require.

The Government would have had the burden to show that Swartz' actions were reckless enough that there is a societal interest in prosecuting him. What is reckless requires a case-by-case analysis.[157] For example, a person who hacks into a school's security camera system as a prank may reach a settlement with the school (or, be expelled), but the act compromised the school's safety during the time the system was off, whether or not intended. Society has an interest to deter future conduct because other persons were put at risk. The action is reckless and incurable by a settlement.

Swartz' action may have been inconsiderate of other JSTOR users whose ability to use JSTOR was hampered, but this is a matter of inconvenience limited to only JSTOR users, and did not pose a danger to anyone. If JSTOR subscribers had been severely affected by Swartz' actions, they could have filed a civil suit. Columbia Law professor Tim Wu summarized Swartz' case best, writing: " … was no actual physical harm, nor actual economic harm. The leak was found and plugged; JSTOR suffered no actual economic loss. It did not press charges. Like a pie in the face, Swartz's act was annoying to its victim, but of no lasting consequence."[158]

H. Other Tests

As mentioned above, *Brekka* would be one solution to narrowing the CFAA's scope. As *Nosal* demonstrated, *Brekka* can limit the scope of a criminal prosecution, but *Brekka* does not create an exempt class of users. Under *Brekka*, a user like Swartz would be liable for criminal prosecution because he accessed JSTOR without authorization.[159] *Brekka* is narrowing of the CFAA through clarification but is still a bright line rule.

---

156. *See* Lessig, *Prosecution as a Bully*; *See generally* http://about.jstor.org/ (last accessed March 17, 2014).

157. *See supra* discussion in Part I at 5.

158. Tim Wu, *How the Legal System Failed Aaron Swartz – And us*, THE NEW YORKER (Jan. 14, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/01/everyone-interesting-is-a-felon.html.

159. *See generally* Garnick, *Losing Aaron Swartz* (hypothesizing that under Brekka, Swartz exceeded authorization because MIT had blacklisted his laptop and in response Swartz concealed his identity).

Professor Kerr has postulated a rule based on code-circumvention. Kerr defines access "without authorization" to mean circumventing code-restrictions. The practical effect would be to reduce the scope of unauthorized access statutes.[160] A person would be criminally liable only if they circumvent a computer code to gain access to information. If they just violate the terms of service, or a private contract, no criminal liability is triggered. Kerr's proposal would filter out innocuous use and disagreement among parties from criminal liability.

Kerr gives an example of, a pro-life owner of a computer network inserting a clause in the terms of agreement that only pro-life opinions may be expressed on the network.[161] He concludes that, a pro-choice opinion would violate the terms of use, "making the access 'without authorization' or 'exceeding authorized access' and triggering criminal liability."[162] This is exactly the type of deficiency in criminal liability that the Hacker's Rule would correct. Expressing those views might result in a person's access from the network being rescinded,[163] but the infraction would fall short of recognizable malice, a federal interest, or be considered reckless to trigger criminal liability.

It is unlikely Kerr's proposal would have prevented Swartz' prosecution.[164] The indictment stated MIT had blocked Swartz' laptop's MAC address.[165] Swartz spoofed his MAC address to gain re-entry into the network. The effect was to trick the network into thinking a different computer was accessing it. Although not a literal code circumvention, Swartz' action was in response to MIT's restriction on his use, based on his computer's unique code.

CONCLUSION

The CFAA should be reformed for two reasons. First, innocuous acts are criminalized. Second, in contradiction to the general framework of law, the CFAA does not exempt any class of user or type of use. Consequentially, the CFAA is prone to prosecutorial abuse, because there are no specific guidelines, only a bright line rule.

The author of this Note is sympathetic towards Aaron Swartz. His

160. *See* Kerr, *Cybercrime's Scope* at 1649.

161. *See* Kerr, *Cybercrime's Scope* at 1658.

162. *See* Kerr, *Cybercrime's Scope* at 1659.

163. For example, if it is a web forum, the person's IP address may be blocked.

164. *See* Garnick, *Losing Aaron Swartz* (skeptical that Swartz would have escaped prosecution under Kerr's rule because Swartz repeatedly spoofed his MAC address on MIT's network).

165. A Mac address is a computer's unique physical address. When a computer is connected to the Internet, the IP address is related to the MAC address on the local area network. *See* http://searchnetworking.techtarget.com/definition/MAC-address.

suicide prevented a legal conclusion to his prosecution, but it should not detract from the deficiencies in the CFAA, and the socially unjust consequences that hold true regardless of Swartz' choice. The legal relevance is the charges he was facing, and the law behind them, not his reaction to them. Had Swartz lived, the purpose of this Note would have remained the same. The conclusions made are not intended to be an absolute solution, and not everyone will agree with the views presented. But, as the literature on the subject has shown, legal scholars agree that the CFAA is in need of reform. Ultimately, this Note seeks to raise awareness about this issue, and encourage further thinking and action.