Washington Law Review

Volume 91 | Number 4

12-1-2016

# Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform

Tiffany Curtiss

# COMPUTER FRAUD AND ABUSE ACT ENFORCEMENT: CRUEL, UNUSUAL, AND DUE FOR REFORM

Tiffany Curtiss

*Abstract*: This Comment argues that the Computer Fraud and Abuse Act (CFAA) uses an outdated concept of technology in everyday activities that can lead to unexpected and grossly disproportional federal criminal charges. The CFAA's vague definitions passively provide broad prosecutorial discretion that may turn millions of everyday internet users into criminals, even in cases of a common breach of an online terms-of-service agreement. Congress should look to the Eighth Amendment and draw from its principles in reforming the CFAA. The Comment concludes with a proposed interpretation of the CFAA that would better align the statute with other criminal laws, namely trespass. Courts should require the owners of protected computers to give notice to a user before that user can be found to violate the CFAA based on unauthorized access.

## INTRODUCTION

Congress enacted the Computer Fraud and Abuse Act (CFAA) in 1986 at a time when computer crime concerns largely focused on threats to government computers and critical infrastructure networks.[1] In the 1980s, most homes did not have a computer, and computer crimes generally required a user with sophisticated skills.[2] Fast-forward thirty years and this is no longer the case. Technology has made its way into the hands and homes of everyday consumers. Given the CFAA's vague definitions, nearly anyone with access to the internet could easily and unknowingly commit a felony.

This Comment argues that courts should look to Eighth Amendment principles when interpreting the CFAA and its definitions.[3] Such principles suggest courts should compare the seriousness of the offense and severity of the sentencing with sentences of similar severity and sentences for the same criminal act.[4] Unless and until Congress amends the CFAA to clarify its boundaries, courts should interpret unauthorized access similar to trespass in order to more clearly distinguish between

1. *See* Joseph M. Olivenbaum, *<Ctrl> <Alt> <Delete>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 586 (1997).

2. *Id.* at 580.

3. *See infra* Part II.

4. *See infra* section II.B.

encouraged, condoned, and forbidden online activities, especially when put in the context of today's technological proliferation.

Congress has broadened the range of devices protected under the CFAA to now include private servers.[5] Congress designed the CFAA to protect critical government infrastructure from outsider hacking, but the CFAA has been used to prosecute violations of a private website's terms of service[6] and is frequently used in tandem with trade secret misappropriation claims against departing employees.[7] Despite harsh criticism and calls for reform, proponents of the CFAA argue that the statute needs to be broad and flexible for national security purposes.[8] This desire to catch bad actors results in wide-ranging prosecutorial discretion that may or may not shield everyday internet users from CFAA liability.[9]

The difficult decisions regarding proper enforcement of the CFAA have fallen to the courts. For example, it is increasingly common for consumers to access software programs when connecting to service providers' servers instead of downloading a copy to their local hard-drive.[10] This near-constant access to private servers exponentially increases the instances of access to protected computers that form the base of any CFAA violation.[11] Due to vague definitions and evolving technological norms, the courts are split on how to interpret the CFAA.[12]

Part I of this Comment explains the history and intent of the CFAA and the circuit split resulting from the mismatch between its broad language and today's reality. Part II discusses how CFAA reform should look to evolving standards of decency and Eighth Amendment

---

5. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–71 (2010).

6. *See* Marcia Hofmann & Rainey Reitman, *Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service*, ELEC. FRONTIER FOUND. (Feb. 4, 2013), https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service [https://perma.cc/VXH3-P6R5].

7. *See, e.g.*, Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

8. *See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1388–89 (2011).

9. *Id.*

10. *See, e.g.*, Brief of Elec. Frontier Found. of Defendants-Appellants, Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012) (Nos. 13-17102, 13-17154), 2014 WL 1004574.

11. *Id.*

12. *See* Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 685–86 (E.D. Mich. 2012) (discussing how this split of authority originates from competing interpretations of CFAA terms).

principles. Part III proposes that Congress reform the CFAA to require owners to provide notice of revoked access to users before a term of service violation can be used for a CFAA charge.

## I. THE CFAA IS OUTDATED AND VAGUE

### *A. Congress Enacted Computer Crime Laws to Deter Outside Hacking of Government Computers*

Before home computers became prevalent, prosecutors viewed crimes that involved a computer or network as traditional crimes, such as internet gambling or cyberstalking.[13] The use of a computer did not affect the elements of the crime. Computer crimes remained susceptible to federal prosecution under existing criminal statutes.[14] In essence, crimes committed using computers were not necessarily crimes of computer misuse.[15] Therefore, prosecuting crimes committed while using computers did not require new laws.

Yet relying on established criminal laws was not always sufficient.[16] The government had difficulty prosecuting malicious computer conduct under criminal statutes such as trespass and theft because the elements of those crimes relied on physical interaction with property.[17] Responding to computer proliferation across government agencies and the threat of rogue employees and hackers, Congress created the category "crimes of computer misuse."[18] Congress aimed to create new "computer misuse" crimes specifically to deter and combat those who "intentionally access[] a protected computer without authorization."[19]

Fear of hackers played a role in driving Congress to address computer crimes.[20] A frequently noted example is the movie *WarGames*, in which a teenage hacker inadvertently compromised a government weapons

13. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602 (2003).

14. For example, the distribution of child pornography in digital format would fall under the same criminal statutes had the distribution been in print form despite the involvement of computer or network.

15. *See* Kerr, *supra* note 13, at 1603.

16. *See, e.g.*, H.R. REP. NO. 98-894, at 9–10 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3695 ("It is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes.").

17. *See* Kerr, *supra* note 13, at 1605–06.

18. *Id.* at 1602.

19. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B) (2012). *See also* Urban, *supra* note 8, at 1388–89.

20. Olivenbaum, *supra* note 1, at 596–97.

system and almost started a nuclear war, causing a great deal of apprehension among congressional leaders.[21] A House Report on computer crime legislation mentions *WarGames*, specifically describing *WarGames* as a "realistic representation of the automatic dialing and access capabilities of the personal computer."[22]

### *1. Congress Originally Designed the CFAA to Complement Existing Tort Law*

Starting in the mid-1980's, Congress sought to create computer crimes law to protect government computers and property by filling the gap between existing criminal statutes and harms created through the assistance of computers.[23] Prior to the enactment of computer-specific criminal laws, prosecutors used mail fraud and wire fraud statutes to prosecute computer crimes, although the statutes were often insufficient.[24] One House Report stated that other statutes also provided insufficient coverage, noting "traditional theft/larceny statutes [we]re not the proper vehicle to control the spate of computer abuse and computer assisted crimes."[25]

In 1984, Congress passed the Comprehensive Crime Control Act (CCCA),[26] including the Counterfeit Access Device and Computer Fraud and Abuse Act,[27] codified at 18 U.S.C. § 1030. Congress designed the CCCA to target hackers who accessed computers to disrupt or destroy computer functionality or to steal information.[28] Congress viewed such hackers as criminals who had the capacity to "access and control high technology processes vital to our everyday lives."[29]

The CCCA was the first federal computer crime statute established by Congress. It created three new federal crimes for knowingly accessing a

---

21. *Id.*

22. H.R. REP. NO. 98-894, at 10 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3696. *See also* Olivenbaum, *supra* note 1, at 596–97.

23. *See* COMPUTER CRIME & INTELL. PROP. SECT., U.S. DEP'T OF JUST. CRIM. DIV., PROSECUTING COMPUTER CRIMES (2007), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf [https://perma.cc/7YGE-X6NC] [hereinafter DOJ MANUAL ON PROSECUTING COMPUTER CRIMES].

24. *See* H.R. REP. NO. 98-894, at 6.

25. *Id.* at 9.

26. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984).

27. *Id.* § 2101.

28. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009).

29. H.R. REP. NO. 98-894, at 8.

computer without authorization or exceeding one's authorization.[30] Congress intended each offense to address specific government interests: (1) national security threats; (2) financial records security; and (3) security of government property.[31]

Although the Comprehensive Crime Control Act was notably robust,[32] Congress nonetheless found the computer crime provisions lacking.[33] Two years after the CCCA's enactment, Congress amended the statute[34] to include three new crimes: computer fraud,[35] hacking another person,[36] and trafficking passwords.[37] Section 1030 is also known as the Computer Fraud and Abuse Act (CFAA) after the short title of this 1986 amendment.[38] Congress has amended the CFAA nine times since its enactment.[39] While originally intended to fill the gap between existing tort law and malicious computer conduct to make whole those who suffered harm to intangible property, the broad drafting of the CFAA definitions has overextended the digital divide bridge beyond tort law and into contract law.

### *2. The Introduction of a Private Cause of Action in the CFAA Led to an Unintended Expansion of Criminal Liability*

As computers became ubiquitous in businesses and homes across the country, concerns about harm caused to and through computers rose. Notorious stories of highly destructive hacking led to further expansions of the CFAA.[40] The scope of the CFAA broadened with each

30. Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(1)–(3) (2012).

31. Kerr, *supra* note 5, at 1564.

32. *Id.*

33. Computer Fraud and Abuse Act of 1986, S. REP. NO. 99-432, at 2, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2479 ("[C]oncern about these problems has become more pronounced as computers proliferate in businesses and homes across the nation and as evidence mounts that existing criminal laws are insufficient to address the problem of computer crime.").

34. Pub. L. No. 99-474, 100 Stat. 1213 (1986).

35. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) (2012) (Accessing to Defraud and Obtain Value).

36. *Id.* § 1030(a)(5) (Damaging a Computer or Information).

37. *Id.* § 1030(a)(6) (Trafficking in Passwords).

38. Pub. L. 99-474, 100 Stat. 1213 § 1 (1986).

39. *See* Matthew Kapitanyan, *Beyond* WarGames*: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 414 n.48 (2012).

40. *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 453.

amendment, expanding the types of conduct that fell within its reach.[41] For example, in 1996, Congress replaced the term "federal interest computer" with "protected computer."[42] After the attacks on the World Trade Center in 2001, Congress used the USA PATRIOT Act to amend the 1996 definition of "protected computer"[43] to "make clear that this term includes computers outside of the United States so long as they affect 'interstate or foreign commerce or communication of the United States.'"[44] In 2008, Congress added the phrase "affecting interstate commerce" to the definition of "protected computer" in an effort to align the CFAA's jurisdiction with that of the Commerce Clause.[45]

The addition of a private cause of action was a significant change to the CFAA.[46] A 1994 amendment added a provision that allows a complainant to bring a private civil cause of action for several of the violations of the CFAA, allowing anyone harmed by a violation to seek compensatory and injunctive relief.[47] Section 1030(g) authorizes a private cause of action for compensatory damages and injunctive and other equitable relief by any person "who suffers damage or loss by reason of a violation," but only if the conduct involves one of the following factors set forth in subsection 1030(c)(4)(A)(i):

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;[48]

---

41. *See* Kerr, *supra* note 5, at 1563–71 (stating that the statute's history "shows a clear and uniform trend of expansion").

42. *Id.*

43. 18 U.S.C. § 1030(e)(2)(B) (2006).

44. DOJ MANUAL ON PROSECUTING COMPUTER CRIMES, *supra* note 23, at 5.

45. Computer Abuse Amendments Act of 1990, S. REP. NO. 101-544, at 9 (explaining that the Commerce Clause was an appropriate addition to the CFAA due to "the interstate nature of computer networks and the ease with which computer abuse . . . can spread across State lines").

46. While this Comment focuses on proportionality of criminal punishments under the CFAA, it is important to note that courts can apply civil precedents in the criminal context when the same standard governs. *See, e.g.*, United States v. Bigham, 812 F.2d 943, 948 (5th Cir. 1987) ("[B]etween the criminal and civil statutes the courts recognize the intent of Congress to cover the same cases, though providing different remedies.").

47. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

48. These losses are limited to economic damages. *Id.*

> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment or care of one or more individuals;
>
> (III) physical injury to any person;
>
> (IV) a threat to public health or safety; [or]
>
> (V) damage affecting a computer system used by or for an entity of the United States government in furtherance of the administration of justice, national defense, or national security . . . .[49]

Private companies have used the civil provisions of the CFAA to recover damages from the misappropriation of confidential information by disloyal employees and other business-to-business litigation associated with computer use.[50] In the civil context, some courts have held that a breach of contract results in unauthorized access.[51]

### *B. Courts Have Struggled to Apply the CFAA Consistently Between Civil and Criminal Cases*

Legal scholars anticipated that the introduction of a private cause of action would lead to a broadened interpretation of the CFAA in the criminal context.[52] Indeed, courts became quickly divided in applying the CFAA to civil cases,[53] which in turn provided a wide spectrum of precedents that federal prosecutors could rely on. For example, in *United States v. Drew*,[54] prosecutors charged the defendant for accessing a protected computer without authorization to obtain information in

---

49. 18 U.S.C. § 1030(c)(4)(A)(i).

50. *See* Brenton, *supra* note 40, at 430; Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

51. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that whether the use of a scraper program exceeded authorized access within meaning of CFAA depended on executive's breach of his confidentiality agreement with company); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004) (holding that use of an automated search robot violated the plaintiff's policy and was therefore unauthorized under the CFAA).

52. *See* Kerr, *supra* note 13, at 1599 ("Given the usual rule that civil precedents apply to criminal cases, however, these cases threaten a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace.").

53. *See* Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *4 (D. Minn. Dec. 15, 2008) (discussing the two competing lines of cases interpreting the "without authorization" and "exceeds authorized access" in a civil context with one line of cases holding that unauthorized *use of information* is sufficient and the other holding that the CFAA requires unauthorized *use of access*).

54. 259 F.R.D. 449 (C.D. Cal. 2009).

furtherance of a tortious act.[55] The government relied heavily on civil cases to support its argument that the CFAA's use of "access" was not unconstitutionally vague and cited only one criminal case that did not squarely address the issue.[56]

In *Drew*, the defendant created a MySpace account under a fake name to bully a young girl.[57] Translated into CFAA terms, the defendant used a computer to intentionally access a protected computer—the MySpace servers—used in interstate commerce.[58] Since she was using the account under a fake name, her use violated the MySpace user agreement, and therefore her use was unauthorized and in excess of authorized access.[59] Prosecutors characterized her actions to fit the CFAA by arguing that, via an interstate communication (MySpace messages), Drew committed tortious acts, namely intentional infliction of emotional distress on the young girl.[60] The defense argued that "legislative history demonstrates the Congressional intent to prohibit trespass and theft under § 1030, not improper motive or use. Cyberbullying is not, under any definition, trespass or theft."[61]

The defense in *Drew* also highlighted the issue of prosecutorial discretion in bringing CFAA charges supported by civil precedents. "[T]he problem is not a delegation of legislative power, but rather prosecutorial power. Any website owner can, under the government's view in this case, set terms that can cause a violation of federal laws."[62] The court held that "a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine,"[63] defeating the prosecution's case.

The Ninth Circuit requires civil cases to involve conduct that would meet the criminal standards of lenity, holding that although the CFAA permits private parties to bring a cause of action, it is primarily a

---

55. This was a violation under the CFAA. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2012).

56. *See generally Drew*, 259 F.R.D. 449 (C.D. Cal. 2009).

57. *Id.*

58. Indictment, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (No. CR08-00582), 2008 WL 2078622.

59. *Id.*

60. *Id.*

61. Consolidated Reply to Government's Opposition to Motions to Dismiss, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (No. CR-08-0582), 2008 WL 3889184.

62. *Id.*

63. United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

"criminal statute."[64] However, several circuits uphold criminal convictions if the conduct would have been a violation in the civil context. The Fifth Circuit in 2010 upheld the criminal convictions in *United States v. John*,[65] where a former employee misused customer account information for a fraudulent scheme, thereby exceeding the employer's authorization.[66] The court stated that while his employer authorized his *access* to customer account information, the employee's *use* of the information violated the employer's policies.[67]

The next year the Eleventh Circuit in *United States v. Rodriguez*[68] upheld a CFAA conviction of an employee who used information accessed through the employer's computer databases.[69] The defendant's role with the Social Security Administration gave him access to view individuals' personal information.[70] He used this access to gain information about women he was romantically involved with or interested in.[71] The court acknowledged that the defendant did not use the information he obtained to commit any additional crimes, but stated that the manner in which Rodriguez used the information was not welcomed by the victims.[72] The court found the conduct in violation of a company policy that employees agreed to by signing an acknowledgement form.[73] The court held that a sentence of twelve months of imprisonment was reasonable.[74]

---

64. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (discussing that the rule of lenity should require courts to interpret "without authorization" from a criminal perspective—where interpretations are not surprisingly and unexpectedly burdensome to defendants and where ambiguity will cut against the government).

65. 597 F.3d 263 (5th Cir. 2010), *cert. denied*, __ U.S. __, 133 S. Ct. 1237 (2013).

66. *Id.* at 269.

67. *See id.* at 271–72 (finding that John exceeded her authorized access because her actions were both an explicit violation of company policy and part of an illegal scheme, not an intended use of the computer system).

68. 628 F.3d 1258 (11th Cir. 2010), *cert. denied*, 563 U.S. 966 (2011).

69. *Id.*

70. *Id.*

71. *Id.* at 1260–61.

72. *Id.* at 1265.

73. *See id.* at 1260 (involving a Social Security Administration employee who accessed private information about several women for personal reasons).

74. *Id.* at 1265.

### *1. CFAA Definitions Are Difficult to Apply Given Today's Computer Norms*

The CFAA's definitions are difficult for courts to apply because software and services are often distributed through a constant connection to protected servers. An end user agreement granting access to a server governs nearly every webpage.[75] This access provides a starting point for many of the ambiguous and divided CFAA opinions. The threshold for when that access differs from, or is in excess of, the contractual grant is the bane of defense attorneys and judges.[76]

In a broad sense, the CFAA criminalizes both accessing a computer "without authorization" and "exceeding authorized access" to a computer.[77] The CFAA creates liability for a person who:

> (1) "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," in violation of § 1030(a)(2)(C); (2) "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value," in violation of § 1030(a)(4); or (3) "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,] or . . . causes damage and loss," in violation of § 1030(a)(5)(B)-(C).[78]

Prosecutors generally use the CFAA to pursue cases of computer intrusion and hacking.[79] Often the cases involve the use of malware or worms to penetrate a firewall in order to steal or destroy data.[80]

---

75. *See* Brittany Johnson, *Live Long and Prosper: How the Persistent and Increasing Popularity of Fan Fiction Requires a New Solution in Copyright Law*, 100 MINN. L. REV. 1645, 1679 (2016) ("Terms of service exist on almost every website and form a type of contractual relationship between the user and the website owner.").

76. *See* Kerr, *supra* note 13, at 1650–51 (discussing how the sensible discretion of prosecutors and judges is frustrated due to confusing CFAA definitions as well as advances in computer technology).

77. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(1) (2012).

78. WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

79. *See* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015, 7:00 AM), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/ [https://perma.cc/6QZ3-W483].

80. *See* Kerr, *supra* note 13, at 1603.

Additionally, prosecutors commonly included section 1030(a)(5)(A) violations in Economic Espionage Act cases.[81]

**Table 1**
**CFAA Criminal Offenses and Statutory Sections**

| **Offense** | **Statutory Section** |
|---|---|
| Obtaining National Security Information | 18 U.S.C. § 1030(a)(1) |
| Accessing a Computer and Obtaining Information | 18 U.S.C. § 1030(a)(2) |
| Trespassing in a Government Computer | 18 U.S.C. § 1030(a)(3) |
| Accessing to Defraud and Obtain Value | 18 U.S.C. § 1030(a)(4) |
| Damaging a Computer or Information | 18 U.S.C. § 1030(a)(5) |
| Trafficking in Passwords | 18 U.S.C. § 1039(a)(6) |
| Threatening to Damage a Computer | 18 U.S.C. § 1030(a)(7) |
| Attempt and Conspiracy | 18 U.S.C. § 1030(b) |
| Forfeiture | 18 U.S.C. §§ 1030(i) & (j) |

### *2. Most Cases Hinge on the Court's Interpretation of "Authorization"*

Congress did not define the phrase "without authorization" in the CFAA.[82] This has led to a circuit split concerning the proper interpretation of the terms "without authorization" and "exceeds authorized access."[83] Seven circuits have wrestled with the proper interpretation for the meaning of "authorization"[84] since 2001.[85] The

81. *See* Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 157 (2008) (discussing the use of the CFAA as a gap-filler).

82. *See* 18 U.S.C. § 1030 (2012).

83. *See* Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 685–86 (E.D. Mich. 2012) ("The split of authority specifically originates from competing interpretations of the terms 'without authorization' and 'exceeds authorized access' . . . .").

84. *See* United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015).

85. *See id.*; United States v. Nosal, 676 F.3d 854 (9th Cir. 2012); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. v. Citrin,

United States Supreme Court has recognized the CFAA's "authorization" as a word "of common usage, without any technical or ambiguous meaning."[86] Black's Law Dictionary defines "authorization" as "[o]fficial permission to do something."[87]

In *International Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*,[88] the district court rejected both the broad interpretation of authorization and the argument that an employee's illegitimate use of information obtained from a computer rendered the access unauthorized.[89] Werner-Masuda, the defendant and a union officer, was charged with exceeding her authorization to use a computer when she violated a terms-of-use agreement that granted her access to a membership list.[90] The court looked to the CFAA's legislative history and found that Congress intended the statute to apply primarily to outside computer hackers rather than employees.[91] The court held that even if the defendant breached a contract, that broken promise did not mean her access to that information was unauthorized or criminal.[92] According to the *Werner-Masuda* court, the CFAA does not "prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do [its] terms proscribe authorized access for unauthorized or illegitimate purposes."[93]

An *en banc* Ninth Circuit decision significantly limited the scope of the CFAA in *United States v. Nosal*.[94] *Nosal* marked the first instance where a federal circuit court held that that the government may not prosecute so-called "insider" cases under the CFAA where the defendant knowingly obtained or altered information for a purpose prohibited by the computer owner.[95] In doing so, the Ninth Circuit articulated that its interpretation of the CFAA was "a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not

---

440 F.3d 418 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

86. United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991).

87. *Authorization*, BLACK'S LAW DICTIONARY 159 (10th ed. 2014).

88. 390 F. Supp. 2d 479, 495–96 (D. Md. 2005).

89. *See* Brenton, *supra* note 40, at 437.

90. *Werner-Masuda*, 390 F. Supp. 2d at 479–80.

91. *See id.* at 498–99.

92. *Id.* at 499.

93. *Id.*

94. 676 F.3d 854 (9th Cir. 2012) (en banc).

95. *See id.* at 863.

misappropriation of trade secrets—a subject Congress has dealt with elsewhere."[96] The *Nosal* Court stated that a broader criminalization based on use would impact more people[97] and the rule of lenity required a narrower reading.[98] Judge Kozinski reasoned that "[b]asing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved."[99]

Recently, in *United States v. Valle*,[100] the Second Circuit settled on the interpretation that "one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all."[101] The court further interpreted "exceeds authorized access" as a limitation on access and not on use.[102] In *Valle*, the defendant was a New York City police officer charged with exceeding his authorized access to police databases to find a woman he allegedly intended to kidnap and torture.[103] "It [was] undisputed that the NYPD's policy, known to Valle, was that these databases could only be accessed in the course of an officer's official duties and that accessing them for personal use violated Department rules."[104] He was convicted at trial and the district judge denied his motion for judgment of acquittal.[105]

The Second Circuit reversed and directed a judgment of acquittal, stating the "[t]he dispositive question [was] whether Valle 'exceeded authorized access' when he used his access to [police databases] to conduct a search for [the intended kidnapping victim] with no law enforcement purpose."[106] The Second Circuit wanted to avoid "criminaliz[ing] the conduct of millions of ordinary computer users."[107] The court relied on the legislative history which "characterize[d] the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the

96. *Id.*

97. *Id.* at 859 ("Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct.").

98. *Id.* at 863.

99. *Id.* at 860.

100. 807 F.3d 508 (2d Cir. 2015).

101. *Id.* at 524 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

102. *Id.* at 527–28.

103. *Id.* at 512–13.

104. *Id.* at 513.

105. *Id.* at 515.

106. *Id.* at 523.

107. *Id.* at 527.

portion of the computer's data to which one's access rights extend."[108] Therefore, employees who, like Valle, had access but violated company policy by using that access for a prohibited use would not trigger section 1030(a)(2) of the CFAA.

### *3. Other Terms Like "Protected Computer," "Damage," and "Loss" Broadened the Reach of CFAA Prosecution*

The meaning of "protected computers" has also played a role in the evolution of CFAA interpretation.[109] The CFAA prohibits unauthorized access to "protected computers"[110] which are "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."[111] Any computer or device capable of connecting to the internet is a "protected computer" within the CFAA's scope.[112] Similarly, a "protected computer" includes any computer connected to the internet.[113] The Department of Justice has provided additional guidance about the role the internet plays within elements of the CFAA:

> Note that the computer must be "used in or affecting" not "used *by the defendant* in"—that is, it is enough that the computer is connected to the Internet; the statute does not require proof that the defendant also used the Internet to access the computer or used the computer to access the Internet.[114]

---

108. *Id.* at 525.

109. *See, e.g.*, Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2167 (2004) (noting that the term "protected computer" includes any computer connected to the internet).

110. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5) (2012).

111. *Id.* § 1030(e)(2)(B).

112. *See* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101, 1 (2001).

113. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 849–50 (1997) (describing the internet as an international network of interconnected computers); Paradigm Alliance, Inc. v. Celeritas Techs, LLC, 248 F.R.D. 598, 602 (D. Kan. 2008) ("As a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement."); Becker v. Toca, No. 07-7202, 2008 WL 4443050, at *5 (E.D. La. Sept. 26, 2008) (concluding law firm's allegation that its computers were connected to the internet satisfied the statutory requirement that owners must at least use the computers in interstate commerce or communication for protection); Credentials Plus, LLC v. Calderone, 230 F. Supp. 2d 890, 906 (N.D. Ind. 2002) (finding computer used to send and receive e-mail to customers throughout the country qualified as a protected computer).

114. DOJ MANUAL ON PROSECUTING COMPUTER CRIMES, *supra* note 23, at 4 (emphasis in original).

Unlike "authorization," the CFAA defines both "damage"[115] and "loss."[116] Damage is "any impairment to the integrity or availability of data, a program, a system, or information,"[117] and encompasses injury to the computer itself, its software, or the information stored on it. Loss is "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."[118] The destruction or deletion of data generally constitutes damage under the Act.[119]

### *C. Prosecutors Have Used the CFAA to Deter Undesirable, Yet Legal, Conduct*

Many commentators see abuses of prosecutorial discretion for three purposes: (1) to punish morally outrageous conduct;[120] (2) to protect private business interests;[121] and (3) to intimidate and chill political activists.[122]

#### *1. Prosecutors Use the CFAA to Prosecute Morally Outrageous Conduct When No Other Statute Prohibits the Conduct*

Legal scholars criticize the CFAA for inviting prosecutors to abuse their discretion.[123] In the highly-publicized "MySpace Mom"

---

115. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified as amended at 18 U.S.C. § 1030(e)(8) (2012)).

116. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended at 18 U.S.C. § 1030(e) (2012)).

117. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(8) (2012).

118. *Id.* § 1030(e)(11).

119. *See, e.g.*, B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) (finding that deletions that make data unavailable to the plaintiff are damage within the statutory definition).

120. *See* Kristin Westerhorstmann, *The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work*, 5 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 145, 152 (2015).

121. *See* Brenton, *supra* note 40.

122. *See* Sarah A. Constant, *The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare—The Case Against Aaron Swartz and the Need to Reform the CFAA*, 16 TUL. J. TECH. & INTELL. PROP. 231 (2013).

123. *See id.*; Hanni Fakhoury, *The Matthew Keys Case, the CFAA, and Why Maximum Sentences Matter*, ELEC. FRONTIER FOUND. (Mar. 14, 2016), https://www.eff.org/deeplinks/2013/03/3-months-or-35-years-understanding-cfaa-sentencing-part-1-why-maximums-matter [https://perma.cc/6LXX-C9VN].

cyberbullying case,[124] defendant Lori Drew and others allegedly seduced a young girl using a fake profile of a teenage boy and then told the girl that "the world would be a better place without [her] in it," in an effort to hurt her emotionally, resulting in the girl committing suicide.[125] At the time, Drew's conduct was not a criminal act under Missouri law.[126] The absence of any state or federal charges sparked outrage in the community and among virtual vigilantes—Drew's home address, phone numbers, email address, and photos were posted online for purposes of sending threats; calls were made to the family members' employers to call for their termination; the family was even "swatted," whereby a call was placed to their local police department giving their address as the location of a murder in progress so police would break in.[127]

After about six months of protests and pleas to bring charges against Lori Drew, the government charged Drew under the CFAA for the intentional breach of a website's user agreement.[128] The government argued the creation of a false profile amounted to a criminal violation of the CFAA.[129] Ultimately, the court rejected the argument and declined to extend criminal penalties to a violation of a website's terms of service.[130] The court reasoned that the government's theory was inconsistent with the original purpose of the CFAA, which was to prevent hackers from interfering with federal interest computers.[131] For these reasons, the judge acquitted Drew in 2009 after she was convicted by the jury.[132]

*Drew* highlights the tension between the retributivist desire to seek justice for victims and the belief that a private contractual breach opens the door to federal criminal indictments. Many proponents of CFAA

---

124. *See* Ars Staff, *"MySpace Mom" Lori Drew's Conviction Thrown Out*, ARSTECHNICA (July 2, 2009, 2:30 PM), http://arstechnica.com/tech-policy/2009/07/myspace-mom-lori-drews-conviction-thrown-out/ [https://perma.cc/CER8-QLMS].

125. Indictment, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (No. CR080582), 2008 WL 2078622.

126. *See* Andrew M. Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law to Include Electronic Communications*, 74 MO. L. REV. 379, 380 (2009) ("Despite Josh Evan's deceitful actions, no state charges were brought against any individuals involved in Megan's death. This is because the behavior that prompted Megan to commit suicide was not a criminal act under Missouri law.").

127. *See* P.J. Huffstutter, *A Town Fights Back in MySpace Suicide Case*, L.A. TIMES (Nov. 22, 2007), http://www.latimes.com/local/la-me-myspace22nov22-story.html [https://perma.cc/C9QX-NQFQ].

128. *Id.*; *Drew*, 259 F.R.D. at 451.

129. *Drew*, 259 F.R.D. at 451.

130. *Id.* at 461.

131. *Id.* at 460.

132. *Id.* at 449.

reform remained loyal to their belief that prosecutors abused the CFAA, even in the face of Drew's morally reprehensible conduct.[133]

Proponents of CFAA reform similarly did not favor a court granting a warrant based on probable cause of violation of a terms of service agreement.[134] In 2009, the Electronic Frontier Foundation (EFF), a civil liberties nonprofit and vocal advocate for CFAA reform, defended computer science student Riccardo Calixte in a state action brought under a Massachusetts law derived from the CFAA.[135] Prosecutors suspected Calixte sent an email to a school mailing list claiming that his dorm roommate was gay.[136] Prosecutors alleged that Calixte sent two false emails; downloaded illegal files; and gained unauthorized access to the college grading system.[137] As a result, local police seized his computers, cellphone and iPod, claiming that he violated criminal law by giving a fake name on his Yahoo account profile.[138] The EFF argued that the sending of a fraudulent or misleading email did not support the claim that the defendant defrauded a commercial computer service.[139]

### *2. Private Sector Companies Try to Enforce Contracts with Federal Criminal Laws*

CFAA critics have also railed against cases where it appears prosecutors used criminal law primarily to enforce private website

---

133. *See, e.g.*, Brief of *Amici Curiae* Elec. Frontier Found., et al. in support of Defendants' Motion to Dismiss Indictment for Failure to State an Offense and for Vagueness, United States v. Drew, 259 F.R.D. 449, 451 (C.D. Cal. 2009) (No. CR-08-0582-GW), https://www.eff.org/document/amicus-brief-support-defendant [https://perma.cc/L39H-EBHS]; Eric Goldman, *The Computer Fraud and Abuse Act Is a Failed Experiment*, FORBES (Mar. 28, 2013, 4:21 PM), http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/ [https://perma.cc/MTP4-M8PP]; Kaveh Waddell, *Aaron's Law Reintroduced as Lawmakers Wrestle over Hacking Penalties*, THE ATLANTIC (Apr. 21, 2015), http://www.theatlantic.com/politics/archive/2015/04/aarons-law-reintroduced-as-lawmakers-wrestle-over-hacking-penalties/458535/ [https://perma.cc/6VQB-Z34R].

134. *See* Matt Zimmerman, *Massachusetts Supreme Judicial Court Tosses Out Warrant in Boston College Case, Says No Probable Cause Existed*, ELEC. FRONTIER FOUND. (May 22, 2009), https://www.eff.org/deeplinks/2009/05/mass-sjc-tosses-calixte-warrant [https://perma.cc/CYY3-H3LL]; In re: Matter of a Search Warrant Executed on March 30, 2009 at the Residence of Movant Riccardo Calixte, Memorandum of Decision and Order, *In re* Riccardo Calixte, No. SJ-2009-0212 (Mass. May 21, 2009), https://www.eff.org/files/filenode/inresearchBC/sjccalixteorder.pdf [https://perma.cc/Y5MH-UATG].

135. *In Re: Matter of Search Warrant (Boston College)*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/re-matter-search-warrant-boston-college [https://perma.cc/UH22-RW3Q].

136. *See* In re: Matter of a Search Warrant, *supra* note 134.

137. *Id.*

138. *Id.*

139. In re: Matter of a Search Warrant, *supra* note 134.

operators' terms of service. In these cases, damage or loss resulting from the act harms the website operators.[140] However, only the broader interpretation, where a violation of a terms of service is immediately considered unauthorized access, provides the basis for a CFAA violation.

In *United States v. Lowson*,[141] the government charged the operators of Wiseguys Tickets, Inc. with violating the CFAA by using bots to purchase event tickets to resell them.[142] Even though this conduct arguably harms consumers and the ticketing market, reform advocates still defended Wiseguys. The EFF argued that "[c]riminal punishment cannot be based on the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service implemented to further the business interest of e-commerce sites, and not necessarily the public interest."[143] The EFF acknowledged that fans "might not like the defendants,"[144] whose bot would automatically purchase posted tickets to resell at a higher price, and that even "[l]egislators agree . . . with consumers that the ticket market is broken."[145] However, the ramifications of criminalizing terms of service violations concerned the EFF. The EFF argued that "public websites cannot decide who is and is not a criminal."[146] The EFF has used the same argument in defense of terms of service violators in civil CFAA cases.[147] Although the court

---

140. *See, e.g.*, United States v. Lowson, Crim. No. 10-114 (KSH), 2010 WL 9552416, at *8 (D.N.J. Oct. 12, 2010) ("The pleaded damage element of at least $5,000 involves defendants' blocking out authorized, individual users from the website by using CAPTCHA Bots, which 'seized' the best seats for events and made those seats unavailable for purchase or consideration until their release by a Wiseguys employee.").

141. *Id.* at *1.

142. *Id.*

143. Brief for Elec. Frontier Found. as *Amici Curiae* Supporting Appellants, United States v. Lowson 20, No. 10-114 (KSH), 2010 WL 9552416 (D.N.J. Oct. 12, 2010), https://www.eff.org/files/filenode/us_v_lowson/lowsonamicusbrieffinal.pdf [https://perma.cc/3BSD-K8MV].

144. Jennifer Granick, *CFAA Prosecution of Wiseguys Not So Smart*, ELEC. FRONTIER FOUND. (July 2, 2010), https://www.eff.org/deeplinks/2010/07/cfaa-prosecution-wiseguys-not-so-smart [https://perma.cc/F65S-5WUN].

145. *Id.*

146. *Id.*

147. *See, e.g.*, Brief of Elect. Frontier Found. as *Amici Curiae* Supporting Defendants-Appellants, Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012) (Nos. 13-17102, 13-17154), 2014 WL 1004574 ("Enforcing private website operators' preferences with criminal law puts immense coercive power behind terms and conditions, and technological measures that may be contrary to the interests of consumers and the public."). The conduct in this case was the defendant's creation of a tool for users to aggregate their own information stored on Facebook. Facebook claimed that the tool violated criminal law because Facebook's terms of service "require users to refrain from using automated scripts to collect information from or otherwise interact with

agreed that the issue of what constitutes criminal fraud in an internet context was "perplexing,"[148] the court denied Lowson's motion to dismiss, stating it "will be in a far better position to meet that challenge after the government presents its evidence."[149] The parties later settled the case out of court prior to a trial.[150]

### *3. Prosecutors Try to Use the CFAA Against Free-Culture Activists and Civil Disobedience Actors*

Internet freedom and data protection goals often conflict.[151] Internet activists have argued that the CFAA "has been used to attack anonymity, pseudonymity, data portability and other consumer rights."[152] Perhaps the most prominent case on this issue was the prosecution of computer programming prodigy[153] Aaron Swartz, a self-described "writer, hacker and activist,"[154] who committed suicide while facing felony charges including offenses under the CFAA. Prosecutors indicted Aaron Swartz in July 2011 for "allegedly attempting to download all of the electronically archived materials maintained by JSTOR while accessing them through a computer network operated by the Massachusetts Institute of Technology."[155]

As part of a fellowship, Harvard provided Swartz with access to JSTOR's services and archives, a not-for-profit digital library that offered paid subscribers access to 2,000 academic journals, as needed for his research.[156] Swartz downloaded nearly 4.8 million articles;[157]

---

Facebook . . . ." Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012)).

148. United States v. Lowson, No. 10-114 (KSH), 2010 WL 9552416, at *8 (D.N.J. Oct. 12, 2010).

149. *Id.*

150. *See* Peter F. Bariso III, *No Need to Fear Robots: Online "Bot" Use Under the Computer Fraud and Abuse Act*, SETON HALL LAW, LAW SCHOOL STUDENT SCHOLARSHIP PAPER 757, 21–22 (2016), http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1771&context=student_scholarship [https://perma.cc/KU6R-NMJQ].

151. *See* Kerr, *supra* note 13, at 1649.

152. Granick, *supra* note 144.

153. Swartz had been involved with data and content distribution technology since age fourteen, when he helped developed the software behind RSS feeds. *See* Noam Cohen, *'Free Culture' Advocate May Pay High Price*, N.Y. TIMES (July 24, 2011), http://www.nytimes.com/2011/07/25/business/media/aaron-swartzs-web-activism-may-cost-him-dearly.html (last visited Oct. 20, 2016).

154. Government's Consolidated Response to Defendant's Motions to Suppress, United States v. Swartz, 945 F. Supp. 2d. 216 (D. Mass. 2013) (No. 11-10260-NMG), 2012 WL 6107933.

155. United States v. Swartz, 945 F. Supp. 2d 216, 217 (D. Mass. 2013).

156. Government's Consolidated Response to Defendant's Motions to Suppress, United States v. Swartz, 945 F. Supp. 2d. 216 (D. Mass. 2013) (No. 11-10260-NMG), 2012 WL 6107933.

however, he never shared them with anyone.[158] Many technology activists thought his conduct in downloading the articles may have been research for civil disobedience, perhaps because Swartz strongly believed that publicly funded research publications should be free to the public.[159]

While facing federal trial in early 2013, Aaron Swartz committed suicide.[160] Many pointed the finger at prosecutor Carmen Ortiz, accusing her of trying to win at all costs by abusing prosecutorial discretion to bully and intimidate[161] Swartz with demands for up to thirty-five years in prison.[162] As one critic put it: "[t]his makes no sense . . . . It's like trying to put someone in jail for allegedly checking too many books out of the library."[163]

The loss of Aaron Swartz was a tragedy for the free culture community, which views itself as striving to preserve free speech and information-sharing over the internet, as well as protecting technology innovators who often find genius in their work through hacking and testing.[164] "How information is able to be distributed over the Internet . . . is the free speech battle of our times."[165] Columbia Law School Professor Tim Wu briefly summed up the answer to whether Swartz would have shared the scientific articles with the world or would have used the articles to develop the next technological leap in digital content management: "[n]ow we will never know."[166]

After Swartz's death, there was an outpouring of calls to reform the CFAA. For example, the EFF submitted a proposal seeking to remove redundancies and double-counting offenses, as well as, making more of

---

157. *JSTOR Evidence in United States vs. Aaron Swartz*, JSTOR (July 30, 2013), http://docs.jstor.org/summary.html [https://perma.cc/W4H3-NAW5].

158. Cohen, *supra* note 153.

159. *See* Tim Wu, *How the Legal System Failed Aaron Swartz—And Us*, NEW YORKER (Jan. 14, 2013), http://www.newyorker.com/news/news-desk/how-the-legal-system-failed-aaron-swartzand-us [https://perma.cc/KZC4-E8Y7].

160. John Swartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html (last visited Oct. 20, 2016).

161. *See, e.g.*, Lawrence Lessig, *Prosecutor as Bully*, LESSIG BLOG, V2 (Jan. 12, 2013), http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully [https://perma.cc/8XZP-EJ4L].

162. *See* Wu, *supra* note 159.

163. Cohen, *supra* note 153.

164. *Id.*

165. *Id.* (quoting Glenn Greenwald).

166. Wu, *supra* note 159.

the CFAA violations misdemeanors.[167] The EFF opens its proposal with a message about Aaron Swartz:

> In the wake of social justice activist Aaron Swartz's tragic death, Internet users around the country are taking a hard look at the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking law. As we've noted, the CFAA has many problems . . . . As Aaron's case indicated, the CFAA's current broad language and draconian penalty scheme allow overreaching prosecutors to abuse their discretion. This can turn minor incidents with no real harm into serious criminal prosecutions, with the threat of long prison sentences and the consequences that go along with a felony conviction—like not being able to vote.[168]

Legislators also tried to reform the CFAA following Swartz's death.[169] In 2013, Senators Ron Wyden and Rand Paul, along with Representative Zoe Lofgren, introduced Aaron's Law.[170] The bill sought to resolve the circuit split, prevent a breach of contract from becoming a criminal violation, and bring greater proportionality to CFAA penalties.[171] "I see 'Aaron's Law' as common sense fixes that should be enacted to stop the kinds of abuse Aaron was subjected to from affecting others," Representative Lofgren wrote on Reddit,[172] an online forum with a loyal user base with which Swartz was involved.[173] The House

---

167. Cindy Cohn, et al., *Rebooting Computer Crime Part 3: The Punishment Should Fit the Crime*, ELEC. FRONTIER FOUND. (Feb. 8, 2013), https://www.eff.org/deeplinks/2013/02/rebooting-computer-crime-part-3-punishment-should-fit-crime [https://perma.cc/6ZGL-9LY8]; *see also EFF CFAA Revisions—Penalties and Access*, ELEC. FRONTIER FOUND., https://www.eff.org/document/eff-cfaa-revisions-penalties-and-access [https://perma.cc/5H59-HDUF].

168. Cohn, *supra* note 167.

169. Cindy Cohn, *Aaron's Law Reintroduced: CFAA Didn't Fix Itself*, ELEC. FRONTIER FOUND. (Apr. 29, 2015), https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself [https://perma.cc/E3AK-62XQ].

170. Aaron's Law Act of 2013, H.R. 2454, 113th Cong. § 4; Aaron's Law Act of 2013, S. 1196, 113th Cong. § 4.

171. Zoe Lofgen & Ron Wyden, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), http://www.wired.com/2013/06/aarons-law-is-finally-here/ [https://perma.cc/8TZ4-H773].

172. Zoe Lofgen, *I'm Rep Zoe Lofgren, Here Is a Modified Draft Version of Aaron's Law Reflecting the Internet's Input*, REDDIT (June 20, 2013, 9:30 AM), https://www.reddit.com/r/IAmA/comments/17pisv/im_rep_zoe_lofgren_here_is_a_modified_draft/ [https://perma.cc/85LP-NRXJ].

173. *See* Swartz, *supra* note 160.

never scheduled Aaron's Law for a debate or vote;[174] however, the bill was re-introduced in the 2015 legislative session.[175]

## II. CFAA REFORM SHOULD LOOK TO THE EIGHTH AMENDMENT AND EVOLVING STANDARDS OF DECENCY

### *A. Eighth Amendment History Suggests Congress is the Appropriate Branch to Address CFAA Reform*

Many of the challenges in applying the CFAA stem from changes in how individuals use technology rather than amendments to the CFAA itself. Even though Congress determined that certain conduct warranted punishment at the time of enactment, what matters for an Eighth Amendment analysis is the CFAA's application today.[176] "The [Eighth] Amendment must draw its meaning from the evolving standards of decency that mark the progress of a maturing society."[177] Ultimately, the Eighth Amendment itself is not the appropriate vehicle to force CFAA reform through the judicial system. However, the Eighth Amendment provides principles that can help shape a framework for CFAA reform.

Congress took the text of the Eighth Amendment almost verbatim from the English Declaration of Rights, which provided that "excessive Baile ought not to be required nor excessive Fines imposed nor cruell and unusuall Punishments inflicted."[178] English law was familiar with the principle of proportionality at the time the founders drafted the Declaration of Rights.[179] The Magna Carta provided that "[a] free man shall not be fined for a small offence, except in proportion to the measure of the offense; and for a great offence he shall be fined in proportion to the magnitude of the offence, saving his freehold."[180] However, the drafters of the Declaration of Rights did not explicitly prohibit "disproportionate" or "excessive" punishments.[181] Some courts

174. *See* Thomas Fox-Brewster, *Aaron's Law Is Doomed Leaving US Hacking Law 'Broken'*, FORBES (Aug. 6, 2016, 9:39 AM), http://www.forbes.com/sites/thomasbrewster/2014/08/06/aarons-law-is-doomed-leaving-us-hacking-law-broken/ [https://perma.cc/27QZ-7788].

175. *See* Aaron's Law Act of 2015, H.R. 1918, 114th Cong.

176. *See* Trop v. Dulles, 356 U.S. 86, 100–01 (1958) ("The Court recognized . . . that the words of the Amendment are not precise, and that their scope is not static.").

177. *Id.* at 101.

178. *See* Solem v. Helm, 463 U.S. 277, 285 (1983).

179. *See id.* at 285–86.

180. MAGNA CARTA, https://www.bl.uk/magna-carta/articles/magna-carta-english-translation [https://perma.cc/DP8Y-FMKG].

181. *See* U.S. CONST. amend. VIII.

have found it unlikely that the Cruel and Unusual Clause prohibited disproportionate punishments.[182]

However, the Supreme Court has held that the Eighth Amendment has a "narrow proportionality principle" that "applies to noncapital sentences."[183] In *Rummel v. Estelle*,[184] the Court held that Texas did not violate the Eighth Amendment by sentencing a three-time offender to life in prison with the possibility of parole.[185] The Court noted that it had "on occasion stated that the Eighth Amendment prohibits imposition of a sentence that is grossly disproportionate to the severity of the crime."[186] Successful challenges to the proportionality of noncapital sentences are "exceedingly rare."[187] Courts have upheld many components of criminal justice, such as mandatory minimums, three-strikes laws, pre-trial detention for dangerousness and risk-based sentencing.[188]

In 2003, the Supreme Court considered the grossly disproportionate test, specifically in the context of recidivist statutes.[189] In *Ewing v. California*, the state of California sentenced the defendant to twenty-five-years-to-life for stealing three golf clubs.[190] "The Court held that the sentence did not violate the Eighth Amendment,[191] resting its decision on two fundamental principles: (1) deference to the legislature and (2) identifying the sentence's penological purpose."[192] The plurality opinion recognized that the legislature is primarily responsible for determining

182. *See* Harmelin v. Michigan, 501 U.S. 957, 974 (1991) ("There is even less likelihood that proportionality of punishment was one of the traditional 'rights and privileges of Englishmen' apart from the Declaration of Rights, which happened to be included in the Eighth Amendment.").

183. *Id.* at 996–97 (Kennedy, J., concurring in part and concurring in judgment).

184. 445 U.S. 263 (1980).

185. *Id.* at 284–85.

186. *Id.* at 271.

187. *Id.* at 272.

188. *See* Ewing v. California, 538 U.S. 11 (2003) (upholding sentence of twenty-five-years-to-life for third-strike theft of three golf clubs, with pro-incapacity rhetoric); United States v. Salerno, 481 U.S. 739 (1987) (upholding pre-trial detention for dangerousness); *Rummel*, 445 U.S. 263 (1980) (upholding life sentence for third minor felony fraud against Eighth Amendment challenge, ostensibly on basis of incapacitation); *see also* Sandra G. Mayson, *Collateral Consequences and the Preventive State*, 91 NOTRE DAME L. REV. 301, 361 (2015).

189. *Ewing*, 538 U.S. at 20 (plurality opinion).

190. *Id.* at 28.

191. *Id.* at 30.

192. Christopher J. DeClue, *Sugarcoating the Eighth Amendment: The Grossly Disproportionate Test Is Simply the Fourteenth Amendment Rational Basis Test in Disguise*, 41 SW. L. REV. 533, 543 (2012).

which conduct society condemns and the punishment for that conduct.[193] The Court is not a "superlegislature."[194]

The Court upheld the sentence and reasoned that California had "a reasonable basis" for believing that severe sentences imposed on career criminals substantially advance the goals of its justice system.[195] It recognized that "[r]ecidivism has long been . . . a legitimate basis for increased punishment."[196] The Court further explained that punishing repeat offenders so severely served the purposes of deterrence and incapacitation.[197] It also recognized that other theories may justify a sentence, such as rehabilitation and retribution.[198]

Also in 2003, the Supreme Court addressed the grossly disproportionate test in *Lockyer v. Andrade*.[199] In *Andrade*, the Court upheld two consecutive twenty-five-years-to-life sentences imposed on a defendant convicted of stealing $150 worth of video tapes from two different stores[200] after the defendant sought habeas corpus relief.[201] The Court held that the lower courts correctly relied on *Rummel*[202] in holding that the sentence was constitutional.[203] The Court did express concern regarding the grossly disproportionate test, noting that "we have not established a clear or consistent path for the courts to follow"[204] and "precedents in this area have not been a model of clarity."[205]

Generally, courts show deference to legislative determinations regarding what conduct to criminalize and the severity of the punishment to impose when determining whether a noncapital sentence violates the Eighth Amendment.[206] This deference provides significant obstacles for defendants challenging their sentences.[207] The separation of powers

193. *Ewing*, 538 U.S. at 24.

194. *Id.* at 28.

195. *Id.*

196. *Id.* at 25.

197. *Id.* at 26.

198. *Id.* at 25.

199. 538 U.S. 63, 74 (2003).

200. *Id.* at 66.

201. *Id.* at 69.

202. Rummel v. Estelle, 445 U.S. 263 (1980).

203. *Lockyer*, 538 U.S. at 73–74.

204. *Id.* at 72.

205. *Id.*

206. Ewing v. California, 538 U.S. 11, 23–25 (2003).

207. *See* Eva S. Nilsen, *Decency, Dignity, and Desert: Restoring Ideals of Humane Punishment to Constitutional Discourse*, 41 U.C. DAVIS L. REV. 111, 147 (2007).

doctrine drives the Court's hands-off approach. The federal system recognizes the independent power of a legislature to articulate societal views through criminal law.[208] Each state's government and the federal government have the sovereign authority to enact and enforce criminal laws individually tailored to fit their respective jurisdictions.[209] In this way, penal systems reflect what criminal conduct individual states feel warrant punishment.

The Supreme Court also recognized that the legislature is the branch of government best equipped to determine the severity of particular crimes and the appropriate sentence to impose.[210] Therefore, courts rarely invalidate sentences.[211] Societies may pressure legislatures to generate criminal codes that differ from each other because they reflect different societal values.[212] In *Harmelin v. Michigan*, Justice Kennedy explained that "differing attitudes and perceptions of local conditions may yield different, yet rational, conclusions regarding the appropriate length of prison terms for particular crimes."[213]

A number of cases provide prominent examples of the broad deference courts grant to state legislatures in determining criminal penalties. In *United States v. Angelos*,[214] the defendant sold bags of marijuana to government informants on several occasions.[215] In two of the drug sales, a gun was visible.[216] However, prosecutors presented no evidence that the defendant used the gun or threatened to use it.[217] In that case, federal law required the judge to impose a fifty-five year

208. *See* McClesky v. Zant, 499 U.S. 467, 491 (1991).

209. *See* Furman v. Georgia, 408 U.S. 238, 268 (1972) (Brennan, J., concurring) ("[L]egislatures have the power to prescribe punishments for crimes.").

210. *See, e.g.*, Harmelin v. Michigan, 501 U.S. 957, 998 (1991) (Kennedy, J., concurring) ("Determinations about the nature and purposes of punishment for criminal acts implicate difficult and enduring questions respecting the sanctity of the individual, the nature of law, and the relation between law and the social order."); Solem v. Helm, 463 U.S. 277, 290 (1983) ("Reviewing courts, of course, should grant substantial deference to the broad authority that legislatures necessarily possess in determining the types and limits of punishments for crimes, as well as to the discretion that trial courts possess in sentencing convicted criminals."); Rummel v. Estelle, 445 U.S. 263, 274 (1980) ("[T]he length of the sentence actually imposed is purely a matter of legislative prerogative . . . .").

211. *Rummel*, 445 U.S. at 285.

212. *See* Hutto v Davis, 454 U.S. 370, 380 (1982) (Powell, J., concurring) (arguing that sentencing disparity is inevitable because trial courts make sentencing decisions).

213. *Harmelin*, 501 U.S. at 1000 (Kennedy, J., concurring).

214. 345 F. Supp. 2d 1227 (D. Utah 2004), *aff'd*, 433 F.3d 738 (10th Cir. 2006).

215. *Id.* at 1231.

216. *Id.*

217. *Id.*

sentence.[218] If prosecutors charged the defendant in state court, based on state sentencing guidelines for Utah, his conviction would have given him a standard range of four to seven years.[219]

In *United States v. Yirkovsky*,[220] the Eighth Circuit held that a fifteen-year sentence for possession of a single bullet was not cruel and unusual punishment.[221] The court noted that "[t]he facts of *Yirkovsky* warrant recitation, because they demonstrate how deferential the judiciary is to legislative determinations of proper punishment."[222] While remodeling a house, the defendant found a .22 caliber bullet and placed the bullet in a box in his bedroom.[223] Later, the defendant's former girlfriend filed a complaint alleging the defendant possessed her property.[224] When the defendant authorized the police to search his room, the police found the bullet.[225] The possession of the bullet subjected the defendant to a fifteen-year mandatory sentence since he had three prior felony convictions, and the Eighth Circuit upheld the sentence.[226] The court recognized that the penalty was extreme, but its "hands [were] tied in [the] matter by the mandatory minimum sentence which Congress established."[227] Lower courts have adhered to a rebuttable presumption that a sentence within the statutory limits is constitutional.[228]

The Eighth Amendment forbids only extreme sentences that are grossly disproportionate to the crime.[229] The Eighth Amendment can provide a useful framework for reforming the CFAA. The principles could guide courts to a reasonable application of the CFAA to novel computer uses by comparing the proportionality of the offense and the sentence.

---

218. *Id.* at 1263.

219. *Id.* at 1242.

220. 259 F.3d 704 (8th Cir. 2001).

221. *Id.* at 705.

222. Phillips v. Iowa, 185 F. Supp. 2d 992, 1020 (N.D. Iowa 2002).

223. *Id.*

224. *Id.*

225. *Id.*

226. *Id.*

227. United States v. Yirkovsky, 259 F.3d 704, 707 n.4 (8th Cir. 2001).

228. *See, e.g.*, United States v. Atteberry, 447 F.3d 562, 565 (8th Cir. 2006).

229. *See* U.S. CONST. amend. VIII.

### *B. The Seriousness of a CFAA Offense and the Severity of its Punishment Often Do Not Align Due to Legislative Lag*

The CFAA's tiered penalties often give prosecutors wide discretion to increase the sentence severity.[230] Several legislators[231] have recognized the opportunity for abuse of prosecutorial discretion and have proposed legislation to curb this power.[232] However, until Congress amends the CFAA or a case makes its way to the United States Supreme Court, a circuit split on the role of civil precedents in criminal CFAA cases will persist.

The need for inherently subjective comparisons is a challenge for courts in applying a proportionality test between the severity of the offense and the sentence.[233] Some courts have opted not to consider sentence severity, characterizing it as "purely a matter of legislative prerogative."[234] These courts leave the severity determinations to Congress to determine the seriousness of a given offense and the appropriate punishment.

#### *1. Technology Norms Should Be Considered When Evaluating the Seriousness of a CFAA Offense*

As discussed in Part I, emerging technologies outpace the CFAA and render its language vague and highly controversial. Unforeseen technologies and increasing electronic interconnectedness[235] create a seemingly moving scale of how society views computer conduct. While one could list many reasons for Congress's delayed or gridlocked attempts to keep laws current, the resulting lag forces courts to continue to deal with sentencing disproportionality.

Without guidance from the Supreme Court, circuit courts may not resolve these disproportionality concerns. Courts are struggling to straddle the increasingly widening gap in the language of the CFAA and

---

230. *See* Press Release, U.S. House of Representatives, Lofgren, Wyden, Paul Introduce Bipartisan, Bicameral Aaron's Law to Reform Computer Fraud and Abuse Act (Apr. 21, 2015), https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397911 [https://perma.cc/7JW5-GFG8] [hereinafter Aaron's Law Press Release].

231. *See* Aaron's Law Act of 2015, H.R. 1918, 144th Cong. (list of co-sponsors).

232. *See* Aaron's Law Press Release, *supra* note 230.

233. *See* Hutto v. Davis, 454 U.S. 370, 373 (1982); Rummel v. Estelle, 445 U.S. 263, 275 (1980).

234. *Rummel*, 445 U.S. at 274.

235. *See, e.g.*, Sean Gallagher, *The Future Is the Internet of Things—Deal with It*, ARSTECHNICA (Oct. 29, 2015, 5:00 AM), http://arstechnica.com/unite/2015/10/the-future-is-the-internet-of-things-deal-with-it/ [https://perma.cc/7948-5ELH].

its applicability to modern technology use. For example, the recent decision in *United States v. Valle* deepened the circuit split on the CFAA authorized access issue.[236] The Second,[237] Fourth[238] and Ninth[239] Circuits have adopted a narrow interpretation of exceeding authorized access and the First,[240] Fifth,[241] Seventh[242] and Eleventh[243] Circuits have adopted a broad interpretation.[244] This indicates some courts are using statutory construction to resolve the sentencing severity with Congress's likely original intent. One should not assume that the seriousness of an offense is inextricably tied to the sentence severity. This assumption would lead to a circular result that precludes applying the proportionality test.[245]

---

236. United States v. Valle, 807 F.3d 508 (2d Cir. 2015). In *Valle*, the defendant was a New York City police officer who prosecutors charged with exceeding his authorized access to police databases to find a woman he allegedly intended to kidnap and torture. It was undisputed that the NYPD's policy, known to Valle, only allowed these databases to be accessed in the course of an officer's official duties, and that accessing them for personal use violated Department rules. The Second Circuit wanted to avoid criminalizing the conduct of millions of ordinary computer users.

237. *Id.*

238. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) (discussing the circuit split and justifying the decision on the rule of lenity).

239. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (discussing how interpretation can turn an anti-hacking statute into a misappropriation statute).

240. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001). The First Circuit held that EF's implied authorization to website users did not extend to the use of all of the information contained on the website. The court found that Explorica's conduct "reek[ed] of use—and, indeed, abuse—of proprietary information." *Id.*

241. United States v. John, 597 F.3d 263 (5th Cir. 2010). The Fifth Circuit upheld criminal convictions where a former employee misused customer account information for a fraudulent scheme and thereby exceeded authorization. *Id.*

242. Int'l Airport Ctrs. v. Citrin, 440 F.3d 418 (7th Cir. 2006). The Seventh Circuit ruled that Citrin's authorization terminated when he breached his duty of loyalty by quitting, and that he exceeded authorized access by deleting the data on his work laptop before returning it. *Id.*

243. United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010). The Eleventh Circuit found an employee of the Social Security Administration criminally liable for using private information about several women from the employer's computer databases for personal reasons. This conduct was in violation of a company policy. *Id.*

244. *See supra* section I.B.

245. *See, e.g.*, David S. Mackey, *Rationality Versus Proportionality: Reconsidering the Constitutional Limits on Criminal Sanctions*, 51 TENN. L. REV. 623, 638 (1984) (suggesting that the "use of the term [proportionality] suggests the development of a constitutional requirement that sentences be imposed on the basis of the particular culpability of an offender and not on the grounds of some independent social goal").

*2. Vagueness Blurs the Tort-Felony Line*

Congress attempted to denote the seriousness of an offense through the CFAA's misdemeanor/felony distinction. The basic offense of improperly using a computer to obtain information is only a misdemeanor.[246] However, the violation becomes a felony when a user takes the information to gain a commercial advantage, to gain a private financial benefit, or to commit another crime or tort.[247] This indicates that Congress intended to increase the punishment for more culpable actors. Unfortunately, felony-triggering conduct easily includes many common and insignificant acts in today's online world.

The broad scope of misdemeanor conduct encompassed under the CFAA means sentencing can be very severe for offenses that are not. The EFF compiled a list of common, innocuous-yet-criminal behavior highlighting the surprising breadth of the CFAA.[248] For example, the EFF warns users about password-sharing: "before you give your significant other your Pandora password, consider whether he or she is someone you want to put on your visitor's list should you end up in prison."[249] Even the Ninth Circuit criticized the prosecution in *Drew*,[250] citing it as an example of prosecutorial excess in applying the broad interpretation of the term "exceeding authorization" based on terms of service violations.[251] It is unlikely that Congress intended the CFAA to make even minor violations of a terms of service agreement a criminal offense.

Similarly, the technological tide washed away the line Congress drew to distinguish felonious conduct. It is felony-triggering conduct "when a user takes the information to gain a commercial advantage, to gain a

246. National Information Infrastructure Protection Act of 1995, S. REP. NO. 104-357, at 8 (1996).

247. *Id.*

248. Hofmann & Reitman, *supra* note 6.

249. *Id.*

250. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (rejecting arguments that a breach of contract should not be a basis for a CFAA violation because the CFAA requires that the intentional accessing further criminal or tortious act).

251. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (en banc) ("[I]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.") In *Nosal*, the Ninth Circuit held that the government may not prosecute "insider" cases under the CFAA. The court held that the rule of lenity would require a narrowed reading because a broader criminalization based on use would impact more unsuspecting people. *Id.*

private financial benefit, or to commit another crime or tort."[252] Using *Drew* as an example, the indictment alleged that Drew intentionally inflicted emotional distress by bullying a teenage MySpace user.[253] Given that the MySpace Terms of Service prohibit criminal and tortious activity, this bullying formed the basis for the CFAA crime of exceeding authorization.[254] The court held that this would "mak[e] the website owner—in essence—the party who ultimately defines the criminal conduct"[255] and "will lead to further vagueness problems."[256]

The vagueness problems continue to expand when other felony-triggering acts are considered. For example, sharing someone else's photo online may infringe copyright and violate the website's terms of service.[257] The terms violation serves as the act of exceeding authorization, and the copyright violation transforms the conduct into a potential felony.

One company even used the CFAA to enjoin a defendant from visiting a publicly accessible site,[258] raising First Amendment concerns.[259] In short, Congress's attempt to distinguish more culpable computer conduct from the more innocuous activities has failed to stand the test of time, producing charges and convictions for activities Congress did not intend to cover.

---

252. Christopher Dodson, *Authorized: The Case for Duty of Loyalty Suits Against Former Employees Under the Computer Fraud and Abuse Act*, 5 DREXEL L. REV. 207, 215 (2012).

253. *Drew*, 259 F.R.D. at 452. The Ninth Circuit was highly critical of the prosecution in Drew—where the indictment alleged that Drew's conduct was for the purpose of committing the tortious act of intentional infliction of emotional distress by bullying a teenage MySpace user—and declined to apply the broad interpretation of the term exceeding authorization.

254. *Id.*

255. *Id.* at 465.

256. *Id.*

257. *See* Eric Goldman, *Lori Drew Prosecuted for CFAA Violations–Some Comments, and a Practice Pointer*, TECH. & MKTG. L. BLOG (May 23, 2008), http://blog.ericgoldman.org/archives/2008/05/lori_drew_prose.htm [https://perma.cc/4EJW-U2RN].

258. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000) (enjoining defendant from accessing publicly available information on plaintiff's website).

259. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 323 (2004).

### *C. Congress Designed the CFAA's Sentencing Scheme to Deter Computer Crime, but Not Breach of Contract*

Commentators also criticize the CFAA for allowing "heavy-handed" prosecution.[260] Under the current scheme,

> [e]ven first-time offenses for accessing a protected computer without sufficient 'authorization' can be punishable by up to five years in prison each (ten years for repeat offenses), plus fines. Violations of other parts of the CFAA are punishable by up to ten years, 20 years, and even life in prison.[261]

These punishments are similar to sentences for selling or importing drugs.[262]

CFAA felony charges reveal a disconnect between conduct and sentence severity, such as in Aaron Swartz's indictment.[263] Felony convictions can result in the loss of the right to own a firearm or to vote.[264] Some felony convictions can get non-U.S. citizens automatically deported.[265] "Ex-offenders may also find themselves ineligible for educational benefits, military service, commercial driving licenses, gun possession, and other civil rights. Many forfeit their parental rights."[266] In addition to longer prison sentences, the "convicted felon" label comes with a social stigma.[267]

Harvard law professor Lawrence Lessig argued that the felony label distressed Aaron Swartz.[268] Friend Quinn Norton also wrote about the impact of the felony conviction on Swartz:

> We talked about it, about what a felony count would mean to him, to his life and his dreams in politics . . . . To be a felon in this country is to be a pariah, to be unlistened to. Aaron wanted

---

260. Aaron's Law Press Release, *supra* note 230.

261. *Computer Fraud and Abuse Act Reform*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cfaa [https://perma.cc/D67J-QWPT].

262. Joseph P. Daly, *The Computer Fraud and Abuse Act—A New Perspective: Let the Punishment Fit the Damage*, 12 J. MARSHALL J. COMPUTER & INFO. L. 445, 459 (1993) (explaining that sliding-scale aggravating factor schemes are used as a strong deterrence mechanism).

263. *See infra* Part III.

264. Daniel Weeks, *Should Felons Lose the Right to Vote?*, ATLANTIC (Jan. 7, 2014), http://www.theatlantic.com/politics/archive/2014/01/should-felons-lose-the-right-to-vote/282846/ [https://perma.cc/72MR-PGMU].

265. *See* Immigration and Nationality Act, 8 U.S.C. § 1227 (2012) (Deportable Aliens).

266. Weeks, *supra* note 264.

267. *See* Cohn, *supra* note 167 ("Beyond this is the tremendous social stigma that comes with the label of 'convicted felon.'").

268. *See* Lessig, *supra* note 161.

> more than anything to speak to power, to make reforms in the very system that was attacking him now. In most states a felon can't even vote. The thought of him not voting was unfathomable.[269]

The sentencing scheme has strong deterrent effects, and so one can reasonably assume Congress intended to curb outside hackers, not online users who overstay their welcome.

### *D. Online Conduct More Easily Violates Existing Law and More Often Results in Severe Punishment than Analogous Offline Conduct*

Some courts compare CFAA punishments to the sentences for the same criminal act under a different criminal statute.[270] The purpose of this comparative analysis was "to validate an initial judgment that a sentence is grossly disproportionate to a crime."[271] In *Solem v. Helm*,[272] the Court compared the penalty issued with penalties that defendant could have received had he committed the same crime in other jurisdictions.[273] The disproportionality of the sentence persuaded the Court. The fact that the defendant could have received the same penalty of life without parole in only one other state convinced the Court the sentence was disproportionate.[274] Similarly, in *Harmelin*, a comparison to other jurisdictions showed that the defendant received a tougher sentence in Michigan than he could have received in any other state.[275]

Crimes under the CFAA do not have perfect offline analogs. However, the CFAA does share in traditional notions of property and privacy, and in some cases the online/offline comparison can still prove useful. For example, the CFAA now often reaches trade secret misappropriation.[276] If an employee extracts data through digital means

---

269. Quinn Norton, *Life Inside the Aaron Swartz Investigation*, ATLANTIC (Mar. 3, 2013), http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/ [https://perma.cc/9G7M-URF9] (stating what Norton had said in front of the grand jury as part of a subpoena) .

270. *See*, *e.g.*, Harmelin v. Michigan, 501 U.S. 957 (1991).

271. *Id.* at 1005 (1991).

272. 463 U.S. 277, 299 (1983).

273. *Id.*

274. *Id.*

275. *Harmelin*, 501 U.S. at 1027 (White, J., dissenting).

276. *See* U.S. Dep't of Justice, *Introduction to the Economic Espionage Act*, *in* CRIMINAL RESOURCE MANUAL, http://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act [https://perma.cc/BR2X-94AZ].

as opposed to misappropriating the same information by hand, a court could then apply the CFAA simply because the employee used a computer.

Distributed denial of service attacks (DDoS) provide another example.[277] In *The Coming Swarm*, Molly Sauter draws out the analogy between a DDoS and the brick-and-mortar forms of sit-in protests.[278] Both involve occupying the target's open-to-the-public property and occupying that property. Similarly, DDoS and sit-in protests disrupt the target's business and display civil disobedience to potential patrons and the community.[279] The punishments associated with brick-and-mortar sit-ins were generally for trespassing and included imprisonment from a few hours to a few months.[280] However, under the CFAA, the occupation of server capacity results in significantly larger penalties in comparison.[281]

Comparisons to other statutes indicate that the CFAA sentences are likely more severe than the seriousness of the offenses. Protecting against and deterring DDoS attacks and other online activities is important for national security, and prosecutors should have tools to deter and punish computer crimes. However, without a narrow or nuanced application of the CFAA, the government may hand out harsh, unintended punishments, such as punishing First Amendment expression in addition to cyberattacks. Therefore, current CFAA sentences may violate proportionality principles.

Some may argue that individuals can cause more damage with computers, therefore courts should punish people more severely for computer crimes. However, aside from a minimum damages threshold needed for a civil claim, damages are not a factor in trial after the initial threshold to bring a civil claim is met.[282] Instead, the amount of damage is a factor to be considered at sentencing. The medium used to inflict the same harm should not drastically alter the outcome. The theft of $100 from a bitcoin account should not differ dramatically from $100 stolen from a wallet. The potential for harm through the use of a computer

277. MOLLY SAUTER, THE COMING SWARM 15 (2014).

278. *Id.* at 15–17.

279. *Id.*

280. *Id.*

281. For example, in Massachusetts criminal trespass is "punished by a fine of not more than one hundred dollars or by imprisonment for not more than thirty days or both such fine and imprisonment." MASS. GEN. LAWS, ch. 266, § 120 (2016).

282. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); U.S. SENTENCING GUIDELINES MANUAL, § 2B1.1 (U.S. SENTENCING COMM'N 2004).

should not amplify the individual's culpability. This amplification is typical to devices like firearms, which is a very different consumer good from computers. Unlike firearms, computers have many functions that are not inherently dangerous. Further, the notion that computers have the potential for greater harm speaks mainly to economic harms; non-economic conduct, such as cyberstalking, may cause less harm than their in-person counterparts.[283]

## III. CONGRESS SHOULD AMEND THE CFAA TO REQUIRE OWNERS TO AFFIRMATIVELY REVOKE AUTHORIZATION

Most outrage over the CFAA occurs when prosecutors bring criminal charges for violations of private contracts.[284] Courts need clarity on the insider access issue. Clarity would also soothe concerns from the "[n]umerous and recent instances of heavy-handed prosecutions for non-malicious computer crimes [that] have raised serious questions as to how the law treats violations of terms of service, employer agreement or website notices."[285] Therefore, Congress should amend the CFAA to require owners to notify defendants of revoked access. Operators should revoke access they deem is a material breach of their terms. Granted, in many cases an operator will not know if a breach occurred;[286] however, the difficulty of a private party monitoring their contractual relationships does not justify the Government enforcing compliance on their behalf, sometimes without their consent.[287]

The owner could revoke authorized access by disabling the user's access where possible, or filing a police report.[288] This will prevent prosecutors from adding CFAA charges in order to intimidate defendants going into negotiations. Similarly, it would create another bar for punishment of morally reprehensible, yet legal, online conduct. Furthermore, this is similar to the current approach with copyright take-

---

283. *See generally* Orin S. Kerr, *Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases*, 84 GEO. WASH. L. REV. 6 (2016).

284. *See supra* section II.C.

285. Aaron's Law Press Release, *supra* note 230.

286. For example, in instances involving the use of fake names, posting of copyrighted material, or inappropriate communications.

287. *JSTOR Evidence in United States vs. Aaron Swartz*, JSTOR (July 30, 2013), http://docs.jstor.org/summary.html [https://perma.cc/W4H3-NAW5] (JSTOR would not have brought charges against Aaron Swartz: "although we recognized that any charging decision was entirely up to the government, from our perspective, we preferred that no charges be brought").

288. Although a police report may not necessarily provide notice to a user, it could be an alternative threshold for search warrants.

down notices, another area of law also adapting to the introduction of the internet.[289] This approach may permit terms of service violations until owners detect the prohibited conduct; however, the access granters should bear the burden of policing their contracts and appropriately limit and monitor access at their own risk. Relying on contractual commitments may not be sufficient means of protecting organizational interest. If organizations do not feel confident that contract breach remedies or other existing laws[290] can make them whole, then they should employ additional security mechanisms. The Federal Trade Commission considers access limitation and network monitoring important security principles for organizations that control or store information.[291] Organizations should only provide the minimal amount of access needed by each user.[292] Network monitoring should flag or lock out any unusual or suspect activities.[293]

Tort law also provides analogies. While trespass varies from state to state, many consider a trespass an unauthorized entry or *unlawfully* remaining in a place.[294] Unlawfully remaining can occur when a person overstays their permission to enter, when a person enters with criminal intent thereby impliedly revoking an owner's consent to enter,[295] or when an owner revokes access or otherwise exercises their right to exclude.[296] First, exceeding a temporary license is rarely at issue in

---

289. Under section 512 of the Digital Millennium Copyright Act (DMCA), the notice and takedown procedure is one requirement for internet service providers' exemption from liability and centers around the concept requiring knowledge of prohibited conduct before liability will attach.

290. Such as trade secret misappropriation, extortion, or fraud.

291. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business [https://perma.cc/AB2T-DFDX].

292. For example, a summer intern should not have access to sensitive human resource files.

293. For example, an organization can require additional verification when a user logs in from an unknown computer or different location.

294. *See, e.g.*, ALA. CODE §§ 13A-7-2, 13A-7-3, 13A-7-4 (West 2016); ALASKA STAT. §§ 11.46.320, 11.46.330 (West 2016); ARIZ. REV. STAT. ANN. §§ 13-1502, 13-1503, 13-1504 (West 2016); ARK. CODE ANN. § 5-39-203 (West 2016); COLO. REV. STAT. §§ 18-4-502, 18-4-503, 18-4-504 (West 2016); DEL. CODE ANN. tit. 11, §§ 822, 823 (West 2016); HAW. REV. STAT. §§ 708-813, 708-814, 708-815 (West 2016); KY. REV. STAT. ANN. §§ 511.060, 511.070, 511.080 (West 2016); MO. REV. STAT. §§ 569.140, 569.150 (West 2016); MONT. CODE ANN. § 45-6-203 (West 2015); N.Y. PENAL LAW §§ 140.10, 140.15, 140.17 (West 2016); OR. REV. STAT. § 164.245 (West 2016); UTAH CODE ANN. § 76-6-206 (West 2016); WASH. REV. CODE §§ 9A.52.070, 9A.52.080 (West 2016).

295. *See, e.g.*, State v. Collins, 110 Wash. 2d 253, 258, 751 P.2d 837, 839–40 (1988) (recognizing that a person's license to enter is impliedly revoked if the person enters with criminal intent, leaving the person exposed to penalties for unauthorized entry).

296. *Id.*

CFAA cases, as websites generally do not express expiration dates in terms of service but rather reserve the right to suspend or terminate access at their discretion.[297] Second, a breach of contract is not criminal, but civil.[298] So even if a person obtained access to a dating website intending to lie about their height in violation of the terms of service's prohibition on false or misleading information, it would not trigger an implied revocation of the dating site's grant of access.[299] Unlawfully remaining in a place after an owner has revoked permission, however, is an approach that can help distinguish CFAA cases of authorization. When an owner grants access to a user on an ongoing basis without explicit terms of what conduct would terminate that access (not merely prohibited conduct), the owner should exercise their right to exclude. One legal encyclopedia states:

> [T]he claim that the defendant's entry or remaining was unlawful will come down to the contention that . . . a person with a legal interest in the property . . . had exercised a legal right to forbid such entry or remaining . . . . Sometimes the purported exercise of such a right will be found not to have occurred, as where the communication relied upon as manifesting such exercise is too general to be given that interpretation or, in the context in which it occurred, cannot be taken literally.[300]

This approach is consistent with recent Ninth Circuit holdings.[301] In *Facebook, Inc. v. Power Ventures, Inc.*,[302] the court distilled the general rule that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly."[303] In *Power Ventures*, Facebook sent the defendant a cease-and-desist letter and imposed an IP address block in an effort to

---

297. *See, e.g.*, *eBay User Agreement*, EBAY, http://pages.ebay.com/help/policies/user-agreement.html [https://perma.cc/ZRG8-M4QW] ("If we believe you are abusing eBay in any way, we may, in our sole discretion and without limiting other remedies, limit, suspend, or terminate your user account(s) and access to our Services . . . .").

298. *See* Hofmann & Reitman, *supra* note 6.

299. *See* Desnick v. Am. Broad. Cos., Inc., 44 F.3d 1345, 1352–54 (7th Cir. 1995) (holding that no trespass occurred even when an owner explicitly refused permission for a specified purpose, and the defendant knowingly and willfully violated the scope of the permission, because the defendant's violation of the contract did not violate the essential interests protected by the writ of trespass).

300. WAYNE R. LAFAVE, 3 SUBST. CRIM. L. § 21.2 (2d ed. 2003).

301. *See* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068 (9th Cir. 2016); United States v. Nosal, 828 F.3d 865 (9th Cir. 2016).

302. 828 F.3d 1068 (9th Cir. 2016).

303. *Id.* at 1077.

prevent defendant's access.[304] Returning to an earlier case, in *Drew*,[305] MySpace could have disabled the account, disabled communication features, or sent a notice to the account or registered email. Any of these mechanisms would have put Drew on notice that MySpace limited or revoked some or all of her previous access.

In *Drew*, the court acknowledged the potential overbreadth of allowing criminal charges for private contract breaches.

> One need only look to the MSTOS terms of service to see the expansive and elaborate scope of such provisions whose breach engenders the potential for criminal prosecution. Obvious examples of such breadth would include: . . . submit[ting] intentionally inaccurate data about his or her age, height and/or physical appearance, . . . [posting] candid photographs of classmates without their permission, . . . entreating [neighbors] to purchase his or her daughter's girl scout cookies . . . .[306]

However, while the court rejected the Government's arguments, it did not prohibit a breach of a private contract as predicate conduct for a criminal charge under the CFAA.[307] Rather, the court stated that "the question arises as to whether Congress has 'establish[ed] minimal guidelines to govern law enforcement,'"[308] and held that CFAA does not "set forth 'clear guidelines' or 'objective criteria' as to the prohibited conduct in the Internet/website or similar contexts."[309] The court looked for any sort of limiting factor to prevent over-inclusiveness, such as requiring website operators to file a police report or have suffered actual loss or damage, but found nothing to distinguish innocuous online conduct[310] from conduct intended to be covered by the CFAA.[311]

Legal scholars advocating for reform of computer trespass torts often reference concepts found in traditional physical trespass torts.[312] Orin

---

304. *Id.*

305. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

306. *Id.* at 466.

307. *Id.*

308. *Id.*

309. *Id.*

310. The court acknowledged that not only bad actors violate terms of service agreements:

> However, one need not consider hypotheticals to demonstrate the problem. In this case, Megan (who was then thirteen years old) had her own profile on MySpace, which was in clear violation of the MSTOS which requires that users be '14 years of age or older.' No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution.

*Drew*, 259 F.R.D. at 466.

311. *Id.* at 466–67.

312. *See, e.g.*, Kerr, *supra* note 283.

Kerr states that "[m]ost CFAA offenses are rooted in trespass . . . not economic crimes,"[313] and argues that the sentencing guidelines governing CFAA punishments should create a new CFAA trespass offense to differentiate unauthorized accesses that violate privacy but do not result in economic harm.[314] While creating separate sentencing guidelines for trespass without fraud will not address other concerns highlighted in this Comment, it could address the proportionality issues with the CFAA by better aligning sentencing severity with comparable crimes.

Congress and the courts should look to Eighth Amendment principles when interpreting the CFAA and its definitions. Congress should amend the CFAA to provide clarity regarding its intent—unless the United States Supreme Court resolves the circuit split first.

## CONCLUSION

Those defending against terms of service violations may be at risk for disproportionate punishments, contrary to Eighth Amendment principles, until Congress or the Supreme Court resolves the circuit split over the criminal reach of the CFAA. Currently, prosecutors could charge millions of unsuspecting internet users under the CFAA. Congress should reform the CFAA to require owners to affirmatively revoke access, including implementing technical disablement where reasonable, with clear notice to the user. Notice provides an additional safeguard for the rights and liberties of the connected citizenry. Furthermore, requiring an affirmative act would harmonize the CFAA with traditional notions of trespass, and it would align the CFAA with Eighth Amendment principles of proportionality.

313. *Id.* at 1.

314. *Id.* at 18.