Science and Technology Law Review

Volume 16 | Number 3 Article 5

December 2017

The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age

W. Cagney McCormick

The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age

*W. Cagney McCormick**

I. Introduction

The Internet's evolving nature makes it difficult for the United States to develop and implement electronic criminal and civil laws that protect Americans, while continuing to follow constitutional fundamentals. Computer fraud and cyber attacks are carried out every day against citizens and corporations while the federal government continues to fight cybercrime with an inadequate, outdated federal statute. The statute, known as the Computer Fraud and Abuse Act ("CFAA"), imposes civil and criminal liability on cybercriminals who undertake Internet attacks on corporations and the government.[1] However, the use of one statute to prosecute both civil and criminal cybercrimes distorts its applicability in case law. The CFAA's outdated language and idea of electronic communications needs to be updated regularly with a proactive mindset instead of the reactive mindset Congress has been using for decades. This article addresses the CFAA's failure to handle new developments such as DDoS attacks, hackivists mobs, cyber soldiers/terrorists and cyber vigilantes and suggests ways to improve the CFAA.

An understanding of the fundamentals of the Internet and identity of hackers is necessary before an adequate discussion and analysis of cybersecurity law may take place.

II. The Internet

The Internet originated in the late 1960s, but similar systems of interconnected computers existed nearly ten years prior.[2] The Pentagon developed the first Internet, and named it ARPANET.[3] ARPANET used TCP/IP, the same underlying protocol for today's modern Internet.[4] In 1991, the first

---

* I would like to thank my wife, Erica McCormick, for her constant encouragement and support. I have the pleasure of working for the Law Offices of Thomas J. Henry, and I appreciate their continual support of my legal career.

1. *See* 18 U.S.C. § 1030 (2006).

2. Kelly Gable, *Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 Vand. J. Transnat'l L. 57, 68 (2010) ("[T]he ARPANET, created by the Pentagon's Advanced Research Projects Agency (ARPA) . . . ultimately became the worldwide system known today as the Internet.").

3. *See id.* at 67.

4. *NSF and the Birth of the Internet—1980s*, Nat'l Sci. Found., www.nsf.gov/news/special_reports/nsf-net/textonly/80s.jsp (last visited Oct. 21, 2013); *see also The Internet Celebrates 30 years of TCP/IP Dominance*, V3.Co.Uk, http://www.v3.co.uk/v3-uk/the-frontline-blog/2233373/the-internet-celebrates-30-years-of-tcp-ip-dominance.

worldwide web page launched after the National Science Foundation began to connect other countries to the United States' Internet.[5]

By 2009, Internet e-commerce contributed approximately $1.67 trillion to the world's gross domestic product ("GDP")—only slightly more than Canada's $1.34 trillion GDP that same year.[6] In 2010, e-commerce comprised almost 4.7% of United States' GDP, an estimated $684 billion.[7] Today, more than two billion people use the Internet to annually exchange more than $8 trillion.[8]

A. How the Internet Works

The Internet works by using protocols to send data. The two protocols enable data, which is broken down into small packets of information, to arrive at the destination in an understandable format.[9] Transmission Control Protocol ("TCP") decomposes data into packets and ensures that they are properly reassembled at the destination.[10] Internet Protocol ("IP") guides or routes the packets of data through the Internet.[11] IP is essential to almost all Internet activities, particularly those that require sending data (such as e-mail).[12] Data is transmitted based on IP addresses, which are a series of numbers regulated by the Domain Name System (DNS).[13] The DNS maps IP numbers into recognizable sets of letters, words or numbers.[14] Hackers often disrupt the DNS flow by flooding the system with information, multiple requests or by gaining access to the system and corrupting or destroying the information that it contains.[15]

---

5. *Id.* ("The first Web page was launched on Aug. 6, 1991.").

6. Annalyn Censky, *Internet Economy: Bigger Than Canada*, CNN MONEY (May 26, 2011), http://money.cnn.com/2011/05/26/technology/internet_economy_gdp/index.htm.

7. Marissa Brassfield, *Internet Economy Statistics: How Does Online Business Measure Up to US GDP?*, PAYSCALE (Mar. 20, 2012), http://www.payscale.com/career-news/2012/03/internet-economy.

8. Censky, *supra* note 6.

9. U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE 29 (2003) [hereinafter NATIONAL STRATEGY].

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. NATIONAL STRATEGY, *supra* note 9, at 30.

III. Profile of a Hacker

The perpetrators of hacking crimes are usually juveniles and young adults.[16] They tend to be male, bored with school or work, nonsocial, and have few outside activities.[17] "According to the United States Sentencing Commission, between 1988 and 1996, 80% of all perpetrators of computer crime had no prior criminal history and over 60% had at least some college experience or were college graduates."[18] As that study suggests, the early 1990s typical American profile of a hacker was a young, well-educated citizen with minimal (if any) criminal history. These hackers were typically motivated by a desire for the excitement or mental challenge, rather than money.[19]

The profile of a hacker has broadened as the Internet continues to grow.[20] "The [hacker] profile now includes disgruntled employees, foreign spies, fraud perpetrators, political activists, conventional criminals, terrorists and very young juveniles."[21] These hackers like to brag or even taunt law enforcement and their victims with their exploits.[22] The increase of identity theft cases has created an additional profile of identity theft hackers, who are only out for money and are more sinister than conventional hackers.[23]

There are several types of cybercriminals: script kiddies, hackers, hacktivists, cyber vigilantes and cyber terrorists.[24] As the name implies, script kiddies are usually young and inexperienced. They use free downloadable virus programs to attack others.[25] Script kiddies lack coding skills sufficient to understand the effects and side effects of the hack.[26] Rather than write code, they reproduce old code.[27] Often these reproductions can leave significant traces, which leads to their detection.[28] True "professional" hackers

16. Scott Tulman, *Unique Characteristics of Computer Crime Prosecutions and Offers*, 1B-40A Criminal Defense Techniques § 40A.03 [2] (2011).

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. Tulman, *supra* note 16, at [2].

23. *Id.*

24. *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 Berkeley Tech. L.J. 909, 918 (2003).

25. *Id.*

26. *Id.*

27. *Id.*

28. Skibell, *supra* note 24, at 919.

make the code script kiddies use, and are distinguishable due to their higher level of sophistication and hacking skill.[29]

Hacktivists use their skills in furtherance of their beliefs or against opponents of their beliefs.[30] Similar to hacktivists, cyber vigilantes believe they are fighting back against bad people.[31] Cyber vigilantes attack identity hackers, child pornography exploiters, kidnappers, and the like.[32] Cyber terrorists attack a country or a group of people in support of their own beliefs and look to cause great harm or damage in the attack.[33] The term "cyber terrorist" is theoretical, as there are no known incidents where cyber terrorists have attacked the public, or have accepted public liability.[34]

B. Cyber Attacks

1. Vulnerabilities in Software

In 2003, a Congress Research Service Report ("the Report") explored the reasons why computer attacks were successful.[35] The Report found that computer hackers opportunistically scan the Internet for computer systems that lack necessary or current software security patches or those with improper computer configurations, which leave them vulnerable to potential security exploits.[36] The Report ultimately blamed computer owners—both individuals and corporations—for failing to take necessary steps to maintain their security.[37] However, the report mentions that even up-to-date computer software security patches may still be vulnerable to a type of attack known as a "zero-day exploit."[38]

29. *Id.*

30. *See* Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383, 385 (2002).

31. *See Steiger v. United States*, 318 F.3d 1039 (11th Cir. 2003) (Alabama citizen arrested after anonymous Turkish hacker found child pornography on citizen's computer and sent images and the associated computer IP address to local law enforcement); *Morris v. United States*, 549 F.3d 548 (7th Cir. 2008) (citizen arrested for attempting to have sex with minor after the minor's parent created a fake myspace account and pretended to be a fifteen year old female, interested in consensual sex).

32. *Steiger*, 318 F.3d at 1042–45; *Morris*, 549 F.3d at 549–52.

33. Gable, *supra* note 2, at 57.

34. *Id.*

35. CLAY WILSON, CONG. RESEARCH SERV., RL 32114, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 5 (2003).

36. *Id.* at 13.

37. *See id.*

38. *Id.*

A zero-day exploit occurs when a computer hacker discovers a new vulnerability and launches a malicious attack program onto the Internet before the software vendor can create and provide a protective security patch to protect software users.[39] Therefore, the Report concedes that the average cybercriminal cannot be stopped due to the constant possibility of new vulnerabilities in all software.[40] Fortunately, the expertise needed to hack all software is hardly ubiquitous. Unfortunately, as the report implies, anything that was digitally created can be jailbroken, cracked, pirated, hacked and reproduced.[41]

Though it is not possible to completely eliminate vulnerabilities, there are practical ways to reduce them.[42] Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate training in computer security, and poor quality in software products.[43] For example, often within companies and organizations the IT specialists do not install timely security patches.[44] Another example is that commercial software vendors consistently release products with vulnerability-creating errors.[45] Government observers have reportedly stated that approximately eighty percent of successful intrusions into federal computer systems can be attributed to software errors, or poor software quality.[46]

There is no current regulatory mechanism or legal liability for software manufacturers who sell defectively designed products.[47] Often the licensing agreement contains a disclaimer protecting the software vendor from all liability.[48] In a trend that has continued to grow since 2003, the CRS Report stated that many software manufacturers contract the development of large portions of their software code to foreign nations.[49]

2. Planning a Computer Attack

The five basic steps hackers use to gain access to a computer are: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.[50] Automated tools created by professional hackers (such as spyware)

39. *Id.*
40. *See id.*
41. WILSON, *supra* note 35, at 13.
42. *Id.* at 15.
43. *Id.*
44. *Id.* at 16, 34.
45. *Id.* at 34.
46. *Id.*
47. WILSON, *supra* note 35, at 34.
48. *Id.*
49. *Id.* at 15.
50. *Id.* at 36, 37.

usually accomplish the majority of these five basic steps.[51] Reconnaissance involves employing extensive surveillance to find detailed information about the computer user or company.[52] Hackers commonly do this by tricking users or employees into sharing sensitive information.[53] Other methods include dumpster diving and finding old hard drives or unshredded information.[54]

Once inside, the hacker begins scanning the network for entry points. Scanning is an arduous process and sometimes lasts months.[55] After developing an inventory of the software and network vulnerabilities, a hacker gains access to the network and decides what kind of attack he or she may want to carry out.[56] Maintaining access is another key step for a hacker.[57] Hackers want to maintain access so they can come and go. Often hackers will try to make themselves "system administrators" so they can maintain access.[58] Experienced hackers will cover their tracks after maintaining and gaining access to a network.[59] Often these hackers will change the computer logs with hacker-constructed "root kits" or "Trojan horse" to evade detection or even wipe the hard drives.[60]

3. Types of Cyber Attacks

Computer software and hardware has evolved at an amazing rate, but vulnerabilities are still present according to the CRS Report for Congress.[61] Cybercrime is committed by a number of different attacks that continue to evolve with the evolving web and tech hardware.[62] The seven most popular cybercrime methods of attack for hackers are: (1) worms; (2) viruses; (3) spyware; (4) bots; (5) Trojan horses; (6) identity spoofing; and (7) distributed

51. *Id.* at 36.

52. *Id.*

53. WILSON, *supra* note 35, at 36.

54. *Id.*

55. *Id.* at 36, 37.

56. *Id.* at 37.

57. *Id.*

58. *Id.*

59. WILSON, *supra* note 35, at 37.

60. *Id.*

61. *Id.*

62. *Id.* at 14. *See also* Bhakti Satalkar, *Types of Computer Attacks*, BUZZLE (June 13, 2011), http://www.buzzle.com/articles/types-of-computer-attacks.html (last visited Sept. 18, 2013).

denial of service attacks.[63] Within these seven popular attacks, various other alterations of these attacks make up many more attacks.[64]

Cyber attacks occur when a computer is infected with a malicious payload program that corrupts data or manipulates the system or network.[65] Downloading malicious code or visiting malicious websites that secretly download the code can infect computers.[66] Worms are self-replicating programs that spread through email address books to attack specific vulnerabilities in software.[67] Viruses are malicious programs that attach themselves to executable (.exe) files.[68] When a computer user downloads a program from a website or P2P program, a virus could be attached.[69] Trojan horse viruses ("Trojans") disguise themselves within working software like screen savers or games.[70] Once the Trojan is copied on a system hard drive, the Trojan kicks in and infects the system.[71] Spyware is a surveillance program that secretly records and automatically transmits keystrokes, passwords, and other information back to a remote attacker.[72] Compromised computers can be used as zombies or "bots" which can go undetected and transmit data.[73] Often these "bots" are used in the worst of cyber attacks in distributed-denial-of-service attacks.[74]

The United States Computer Emergency Readiness Team released an unclassified report on DDoS attacks describing them as the "most significant cyber threat to businesses, local and federal government agencies."[75] A DDoS occurs when an attacker commands a number of computers to send numerous requests to a target computer.[76] The overwhelming flood of requests can cause the website or computer network to shut down; alternatively, the target may be unable to handle the request of legitimate users,

63. Satalkar, *supra* note 62.

64. *Id.*

65. WILSON, *supra* note 35, at 28.

66. *Id.*

67. Satalkar, *supra* note 62.

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.*

72. WILSON, *supra* note 35, at 29.

73. *Id.* at 27.

74. *Id.*

75. *Understanding Denial-of-Service Attacks*, U.S. DEP'T OF HOMELAND SEC. (Feb. 6, 2013), http://www.us-cert.gov/ncas/tips/ST04-015.

76. *Id.*

much like a freeway traffic jam.[77] The zombie computers, or "bots," are often used as the soldiers in this type of attack.[78] Experienced hackers can use a combination of all of these types of attacks in order to gain and maintain entry in committing cybercrimes.[79] Criminal software, or "crimeware," has become increasingly available on the cyber black markets and can enable a potential adversary to rent a botnet or execute a DDoS attack.[80] "It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution."[81]

IV. Flaws in the Law

A. Computer Fraud and Abuse Act

"The Computer Fraud and Abuse Act ("CFAA") is the cornerstone of the federal government's strategy for combating computer crime."[82] The original version of the Act was written by Congress in 1984 and has been revised frequently.[83] The first revision occurred in 1986 after the original CFAA was widely criticized for vagueness.[84] The 1986 amendments broadened the scope of the CFAA by adding computer fraud and hacking as offenses.[85] These new offenses included a mens rea of "intentionally," rather than the original and less burdensome mode of culpability requirement "knowingly."[86] In 1996, another revision again changed the mens rea requirements of the CFAA by completely restricting subsection (a)(5), consequently creating two felonies and one misdemeanor to cover a wide range of crimes and, thus, applied a different mens rea to each offense.[87] The first felony required an intentional act of damaging a computer by *knowingly* transmitting a harmful program.[88] The second felony applied to persons who intentionally access a computer without authorization and *recklessly* cause damage.[89] The misdemeanor required intentionally accessing a computer

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. Ken Thompson, *Reflections on Trusting Trust*, 27 Comm. ACM 8 (1984).

82. Skibell, *supra* note 24, at 910.

83. *Id.* at 944.

84. *Id.* at 912.

85. *Id.* at 913.

86. *Id.* at 913–14.

87. *Id.* at 915.

88. Skibell, *supra* note 24, at 915.

89. *Id.* at 915–16.

without authorization and *negligently* causing damage.[90] Therefore, the 1996 CFAA amendment unequivocally broadened the applicability of the statute by expanding the mens rea requirement.[91] The last major revision came as a result of the USA PATRIOT Act of 2001 which raised the maximum penalties for violating the CFAA's felony provisions from five to ten years; maximum punishment for repeat offenders was raised from ten to twenty years.[92] The USA PATRIOT Act imported the definition for "loss," as created in *United States v. Middleton* in 2000.[93] Section 1030(e)(11) states the term "loss" can represent the cost of damages, any lost revenue or costs associated with an interruption in service, and the damages from a single attack may be aggregated across many computers.[94]

The current CFAA punishes seven computer criminal offenses. First, the CFAA is applicable when a computer user trespasses into the United States government's cyberspace.[95] This section condemns hacking any computer that holds a federal government interest—not exclusively computers owned by the federal government.[96] This offense merely requires the intentional and unauthorized access of information—no damage is required—of a government computer maintained exclusively for the use of the federal government or a government computer partly used by or for the federal government with such access affecting the federal government.[97] The second offense is the theft of information by unauthorized computer access.[98] This offense is aimed to protect three types of government information: information on the federal government; consumer credit or another form of financial information; and information acquired through interstate or foreign access.[99]

A hacker who causes damages without authorization to access a computer faces criminal charges under section 1030(a)(5) and computer fraud subsection 1030(a)(4).[100] Section 1030(a)(5) describes cyber attacks as worms and viruses; however, any type of cyber attack that creates an aggregated loss greater than $5,000 in a non-government computer during a one-year period after the attack will fall under this section as a federal crime.[101]

90. *Id.* at 916.

91. *Id.*

92. *Id.* at 917.

93. *See* United States v. Middleton, 231 F.3d 1207, 1212–13 (9th Cir. 2000).

94. *See* 18 U.S.C. § 1030(e)(11) (2006).

95. *See id.* § 1030(a)(3).

96. *Id.*

97. *Id.*

98. *Id.* § 1030(a)(2).

99. *See id.*

100. *See* 18 U.S.C. § 1030(a)(5).

101. *See id.* § 1030(a)(4).

To prosecute under section 1030(a)(5), a hacking crime must satisfy the $5,000 loss requirement *or* reach a special government interest.[102] Modification or impairment to medical examinations or information is considered damage, and causing physical injury to any person or threatening public health or safety will impact the applicability of section 1030(a)(5).[103] The damage has to be made on a "protected computer."[104]

Five types of protected computers are listed: 1) computers used by or for the U.S. government; 2) computers used for or by a financial institution; 3) computers whose damage affect the U.S. government interest; 4) computers whose damage affect financial institutions; and 5) computers used in interstate or foreign commerce or communications.[105] The other type of damage under the CFAA is computer fraud.[106] Section 1030(a)(4) bans fraud by computer intrusion.[107] The four crucial elements to this offense are: 1) "knowingly" with intent to defraud; 2) accessing a protected computer; 3) "without authorization" or "exceeding authorization;" and 4) furthering a fraud or obtaining anything of value.[108] An interesting exception in exists in section 1030(a)(4): when a defrauder only obtains use of your computer and the time of use is valued less than $5,000 in a one-year period.[109] Without satisfaction of this threshold damage amount, a prosecutor would likely have to seek a state charge for computer abuse.

A hacker who uses his hacking skills with the intent to extort money, traffic sensitive passwords, or spy on the United States are the final three acts prohibited by the CFAA.[110] Subsection 1030(a)(7) states that no one shall "transmit in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer" for the purpose of extorting from any person.[111] Additionally, subsection 1030(a)(6) forbids trafficking in computer access or passwords.[112] Trafficking references transferring, disposing, or obtaining control with the intent to make a transfer or disposal.[113] The computer passwords or keys must be used either to attack a federal computer or in a manner that affects interstate or foreign com-

102. *Id.*

103. *Id.* § 1030(c)(4)(A)(i).

104. *Id.* § 1030(c)(4)(A)(i)(I).

105. *Id.* § 1030(e)(2).

106. 18 U.S.C. § 1030 (e)(2).

107. *See id.* § 1030(a)(4).

108. *Id.*

109. *Id.*

110. *See id.* § 1030.

111. *See id.* § 1030(a)(7).

112. *See* 18 U.S.C. § 1030(a)(6).

113. *Id.* § 1029(e)(5).

merce.[114] Computer espionage is outlawed in section 1030(a)(1), which specifically bans any disclosure of information detrimental to the United States' national defense.[115]

B. Judicial Interpretation

CFAA litigation has included numerous disputes attempting to define the scope of a user's authorization when that user uses a computer to damage digital information or use it "without authorization" or when "exceeding authorized access."[116] Particularly, defining a violation of "exceeding authorization" has been the more difficult task.[117] When an employee has permission to access the entire network, exceeding authorization can be increasingly difficult to define for particular offenses. Significant portions of the CFAA are automatically not applicable to an employee who has complete computer access, such as the company's lead computer engineer. For instance, section 1030(a)(3) does not apply to an employee if federal information is accessed while having the authorization to do so because there is no trespass of government cyberspace.[118] Similarly, section 1030(a)(2)(A-B) is not applicable if the stolen information is not property of a financial institution or department of the United States.[119] Therefore, only section 1030(a)(2)(C) would apply because the employee exceeded authorization of "any protected computer;" however, courts have had differing views on how to apply the definition of "exceeding authorized access" provided in section 1030(e)(6).[120]

The first case to try and define the scope of authorization under the CFAA was *Morris v. United States*.[121] Robert Morris was a graduate student at Cornell University who created a worm designed to exploit several weaknesses in certain targeted programs and the Internet.[122] Morris accessed several Ivy League networks to study cybersecurity.[123] Once Morris released the worm it quickly multiplied across the United States, even though he never intended to cause extensive damage.[124] Morris' unsuccessful appeal claimed

114. *Id.* § 1030(a)(6).

115. *See id.* § 1030(a)(1).

116. *See id.* § 1030.

117. *See id.*

118. *See* 18 U.S.C. § 1030.

119. *Id.*

120. *See* Morris v. United States, 928 F.2d 504, 510 (2d Cir. 1991).

121. *Id.*

122. *Id.* at 505.

123. *Id.*

124. *Id.* at 506.

he never intended to cause the amount of damage required by the CFAA.[125] From Morris' appeal, the Second Circuit developed the Intended Function Test to determine when access was unauthorized.[126] Unauthorized access is found when a defendant does not use the features in the attacked program or network "in any way related to their intended function."[127] The Intended Function Test created a workable definition to both "unauthorized access" and "exceeding authorization."[128] The Fifth Circuit accepted this test in *United States v. Phillips*.[129] In *Phillips*, the court stated the typical analysis begins with "the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."[130]

Subsection 1030(e)(6) defines "exceeds authorized access" as the "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the person with access is not entitled to *obtain or alter*."[131] While the Intended Function Test creates a test to determine when a user has made unauthorized attempts to access a computer or network, courts have continuously found it difficult to decide when a user has exceeded authorization when the user did not "alter" or "obtain" any information.[132] The issue "is whether 'authorized access' or 'authorization' may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system."[133]

The circuit courts are split as to whether an employee has exceeded proper authorized access when there are no limits to the authorization.[134] The majority view, supported by the Fifth Circuit, follows the Intended Purpose Test.[135] Using authorized confidential information exceeds authorization "when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime."[136] Therefore, the misappropriation of non-government company information is a criminal offense under the CFAA

125. *Id.* at 507.

126. *Morris*, 928 F.2d at 510.

127. *Id.*

128. *See id.* at 509.

129. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).

130. *Id.*

131. *Id.*

132. *See Phillips*, 477 F.3d at 220; *see also Morris*, 928 F.2d at 508.

133. *See* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).

134. *See Lavon*, 597 F.3d at 271; *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009).

135. *See Lavon*, 597 F.3d at 289.

136. *Id.* at 271.

when considering the Intended Purpose Test, even if the misappropriation does not involve a criminal scheme.[137] The Fifth Circuit explained, "the concept of 'exceed[ed] authorized access' may include exceeding the purposes for which access is 'authorized.' Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."[138]

The First and Seventh Circuits have similarly accepted an agency-principle-based standard in civil cases.[139] The First Circuit has held an employment agreement to potentially establish the guidelines for "authorized" access under the CFAA.[140] The Seventh Circuit held a defendant breaching his duty of loyalty terminated his agency relationship, and with it, his authority to access a laptop or company network.[141] Hence, the defendant's basis of authority existed only through his employee-employer relationship.[142] The standard applied in criminal cases within these two circuits has found access to exceed authorization under the CFAA when an authorized user violating the company's employment agreement, regardless of criminal intent, has misappropriated information from a company's digital database.[143]

The minority view rejects the argument that one authorized to obtain information stored in a computer exceeds authorized access when breaching a duty of loyalty to an employer by accessing and using such information to further his independent interests.[144] The minority view, promulgated by the Ninth Circuit, holds that an employee with authority to access his employer's computer system does not violate the CFAA when using his privilege for the misappropriation of accessible information.[145] A Second Circuit district court attacked the Intended Purpose Test by claiming there is "no statutory language that supports interpreting the CFAA to reach misuse or misappropriation of information that is lawfully accessed."[146] Moreover, the court stated this standard would require "an analysis of an individual's subjective intent

137. *Id.*

138. *Id.* at 272.

139. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001); *see also* Int'l Airport Ctrs., v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

140. *Explorica*, 274 F.3d at 582.

141. *Citrin*, 440 F.3d at 420–21.

142. *Id.*

143. *See generally id.*

144. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (noting the plain meaning of CFAA indicates that authorization depends on actions taken by the employer, not whether an employee breached a state law duty of loyalty to an employer).

145. *Id.* at 1137.

146. United States v. Aleynikov, 737 F. Supp. 2d 173, 193 (S.D.N.Y. 2010).

in accessing a computer system."[147] Agreeing with the Ninth Circuit, the court asserted, "an interpretation of the CFAA based upon agency principles would greatly expand the reach of the CFAA to any employee who accesses a company's computer system in a manner that is adverse to her employer's interests."[148] Thereby "convert[ing] an ordinary violation of the duty of loyalty or of a confidentiality agreement into a federal offense."[149]

Supporters of this view insist the CFAA legislative history demonstrates it was intended to prohibit electronic trespassing or hacking, not the misuse of information.[150] This minority view permits a defendant the opportunity to raise a defense in each circuit court, and a potentially provides an opportunity of appeal to the United States Supreme Court.[151] Nevertheless, neither the Supreme Court nor Congress has shown interest in settling this dispute. Despite missed opportunities, modifications may be made to ensure the CFAA is properly applied, consistently enforced, and effectively protects Americans.

V. Creating an Effective CFAA

A. Increased Punishment Ranges

Increasing the maximum punishment under the CFFA from twenty years to thirty years imprisonment will improve the CFAA, in part, by deterring more cybercriminals. Although increasing the maximum punishment to thirty years incarceration may be considered harsh, it should be available (and applicable) only in cases of the most heinous cybercriminals and organizations. Primarily, the punishment increase would affect cyber organizations, which are on the rise, and should be reserved for those who attack the United States and mega-corporations, subsequently causing millions of dollars in damage. For demonstration, the following would effectively target, and restrict its abuse, the application of the maximum thirty-year sentence. An individual is subject to a maximum of thirty years imprisonment, when acting alone or in a group, such individual participates in a computer attack without access authorized by a United States government institution or American business and whose participation results in damages exceeding $1 million.

For decades laws have existed to fight against traditional crime organizations; there should similarly be laws aimed to protect against organized cybercrime because the law—particularly penal codes—must evolve to address how technological advancements have impacted society and the applicability of existing law. A single hacker is dangerous; one hundred organized hackers can instantaneously devastate a conglomerate's website or network.

147. *Id.* at 193–94.

148. *Id.* at 194.

149. *Id.*

150. *Id.* at 192.

151. *Id.* at 194.

Anonymous—the world's most infamous hacker cyber organization—is demonstrative of organized hackers' capabilities.[152] In April 2011, in just a few short minutes, members of Anonymous brought down Sony's PlayStation Network for weeks and reportedly took millions of credit card numbers as "trophies."[153] Over the past two years, Anonymous has attacked conglomerates, countries, and foreign politicians as "hackivists" fighting for privacy rights and freedom.[154] PayPal, Amazon.com, MasterCard, and the Church of Scientology have all had their websites disabled by "denial of service" attacks by members of Anonymous.[155] Anonymous has become known as a loose group of hackers with cells around the world.[156] Brazilian, Iranian, and Turkish government websites have all faced attacks by members of Anonymous in protest of Internet censorship as well as election fraud.[157] Thus, a new anti-cybercrime organization subsection is needed in the CFAA to address the growing technological capabilities of hacking mobs like Anonymous.

B. Explicitly Include Denial of Service Attacks as Violation

In order to address the current incongruity between the intent and application of the CFAA, a new subsection should be added to expressly prohibit denial of service attacks. A DDoS attack is meant to flood a website with thousands of request to make the website fold under the pressure and prevent legitimate use.[158] Denial of Service Attacks can be carried out without the need to gain "unauthorized access."[159] Originally, hackers would use a virus-type program to make the infected computer a "bot" to make requests at any website targeted by the hacker.[160] The unauthorized access into the infected "zombie" computer does violate the CFAA but the request to the targeted

152. *CBS News: "Anonymous" Hacker: We Can Shut Your Website* (CBS television broadcast July 19, 2011), *available at* http://www.cbsnews.com/8301-18563_162-20080814.html.

153. Icar Paneda, *Spain Arrests Anonymous Members over Sony Hack* (June 10, 2011), http://uk.reuters.com/article/2011/06/10/uk-spain-anonymous-idUKTRE7593FZ20110610.

154. *CBS News: "Anonymous" Hacker*, *supra* note 152.

155. Paneda, *supra* note 153; *see also CBS News: "Anonymous" Hacker*, *supra* note 153 ("[A] 'denial of service attack,' [is] whe[n] hackers overwhelm websites with a huge volume of requests for information crashing down the company's Web site.").

156. Paneda, *supra* note 153.

157. *See generally id.*

158. Milone, *supra* note 30, at 389.

159. *See generally id.*

160. *Understanding Denial-of-Service Attacks*, U.S. DEP'T OF HOMELAND SEC. (Feb. 6, 2013), http://www.us-cert.gov/ncas/tips/ST04-015.

website has nothing to do with "authorized access."[161] Hackivists groups like Anonymous now make botnet programs in which members or followers can download in order to freely make that computer a "zombie" with the consent of the user.[162] Hackivists believe this is a way to legally protest against a company's website.[163] Outlawing this type of protest would send a clear message to hackivists.

A DDoS attack is prosecuted under section 1030(a)(5), which states it is a crime to "knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer."[164] However, a hackivist lead DDoS attack, like Anonymous advocates, has authorization to make the botnet infected computer a "zombie" and the CFAA should not apply because there is no "damage without authorization" on the targeted website. In this type of DDoS attack, proper "authorization" is never requested or attempted upon the targeted website.[165] Another issue in section 1030(a)(5)(A) is whether the targeted website has experienced any "damage."[166] The website is made inoperable because the servers can no longer handle the thousands of request made by the botnet computers due to the lack of bandwidth the website runs. This "damage" refers to the limits of technology setup by the company and the financial cap the targeted company decided to invest in the website.[167]

Since section 1030(a)(5)(A) does not apply to DDoS attacks—like those carried out by Anonymous—the CFAA should be amended, or another statute should be enacted, to apply to DDoS attacks. In 2006, the United Kingdom created a new denial of service attack act called the Police and Justice Act 2006 amending Britain's Computer Misuse Act that was created before the days of the Internet.[168] The amendment covered all types of DDoS attacks by stating that a person is guilty of an offense if the individual makes unauthorized acts with intent to impair, or with recklessness as to impairing; by

161. *See generally* Graham Cluley, *Are DDoS (Distributed Denial-of-Service) Attacks Against the Law?*, NAKED SECURITY (Dec. 9, 2010), http://nakedsecurity.sophos.com/2010/12/09/are-ddos-distributed-denial-of-service-attacks-against-the-law/.

162. *See generally id.*

163. *See generally* Pierluigi Paganini, *Hacktivism: Means and Motivations . . . What Else?*; INFOSEC INST., (Oct. 2, 2013), http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/.

164. *See* 18 U.S.C. § 1030(a)(5)(A).

165. Cluley, *supra* note 161.

166. *See* 18 U.S.C. § 1030(a)(5)(A).

167. *See id.*

168. *UK Bans Denial of Service Attacks*, OUT-LAW.COM (Nov. 9, 2006), http://www.out-law.com/page-7462.

operation of a computer impairs the operation of any program or data, prevents or hinders access to any program or data held in any computer; and/or impairs the operation of any such program or the reliability of any such data.[169] The key component applying to DDoS attacks is the preventing or hindering of access to any program or data held in any computer and the impairment of the reliability of any such data.[170] A similar addition to the CFAA by the United States Congress would send a strong message to hackivists groups like Anonymous.

C. Develop an Appropriate Suppression Remedy

The CFAA and other Internet surveillance laws have one giant glaring hole: there is no suppression remedy against hacker vigilantes.[171] "A defendant charged with a crime can sue the government for civil damages if the FBI violates the surveillance laws to catch him, and can sue ISPs and other third parties if they violated the surveillance laws as well, but he cannot rely on those violations as a basis for suppression of the evidence against him."[172] The Internet surveillance laws consist of the CFAA, Pen Register Statute, Stored Communications Act, and the Wiretap Act; and within the Internet context, none of these have a suppression remedy.[173]

The CFAA does not have any statutory language giving a defendant an option for suppression if an individual's expectation of privacy was violated on his computer by a hacker.[174] The Fourth Amendment allows state and federal law enforcement to go freely into public spaces that are not protected by a "reasonable expectation of privacy."[175] Generally, a search warrant is required when law enforcement expects to enter into a private area.[176] In contrast, a search by a private person does not implicate the Fourth Amendment, unless he acts as an instrument or agent of the government.[177] Therefore, incriminating evidence discovered by a vigilante hacker—later submitted to police—on a hacked computer would not be subject to suppres-

169. *Id.*

170. *Id.*

171. *See generally* 18 U.S.C. § 1030.

172. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806–07 (2003).

173. *Id.* at 814–15.

174. *See generally* 18 U.S.C. § 1030.

175. United States v. Katz, 389 U.S. 347, 351–52 (1967).

176. *See generally* U.S. CONST. amend. IV.

177. United States v. Ford, 765 F.2d 1088, 1089–90 (11th Cir. 1985).

sion under the Fourth Amendment, unless the hacker was a government agent.[178]

The Eleventh Circuit was faced with whether evidence submitted to law enforcement from an anonymous hacker's discovery of a defendant's child pornography on his computer was admissible under the current Internet surveillance laws.[179] The court ruled the Internet hacking vigilante was not an agent of the government, and the current Internet surveillance laws did not prevent a private individual from "hacking into personal computers to retrieve information stored therein."[180] As such, current case law does not provide a suppression remedy to a vigilante hacker victim.[181]

Internet vigilante issues have primarily stemmed from child pornography and solicitation cases.[182] The Seventh Circuit has stated, "[o]n-line vigilantism against pedophiles, in fact, has taken on unexpected proportions."[183] Discussing the lack of a suppression remedy against Internet intrusions, the court added, "If the law wants to deter private sting operations, real or phony, the way to do that is by imposing criminal liability on private parties who encourage crimes."[184] Further, "[j]ust as there is no defense of private entrapment . . . there is no exclusionary rule applicable to evidence obtained improperly by private persons."[185] A suppression remedy against hackers attacking Americans would fall well within the intended purpose of the CFAA. The CFAA already outlaws vigilante hackers.[186] A suppression-remediless CFAA is a violation of the privacy fundamentals the Constitution is meant to protect. Digital records are kept in most aspects of an American's life and every American is at risk to exposure by vigilante hackers until an appropriate suppression remedy exists.

D. Federal Regulatory Commission

To deter and limit cybercrimes, the government should create a regulatory commission to oversee the software industry, which could eliminate some software vulnerabilities.[187] At a minimum, the government should create code guidelines for developers to follow. Allowing companies to outsource their code production also puts American computer users at risk for

178. United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003).

179. *Id.* at 1050.

180. *Id.* at 1049.

181. Kerr, *supra* note 172, at 807.

182. *See* Morris v. United States, 549 F.3d 548 (7th Cir. 2008).

183. *Id.* at 551.

184. *Id.* at 552.

185. *Id.*

186. *See generally* 18 U.S.C. § 1030.

187. *See* WILSON, *supra* note 35, at 3.

cybercrimes and, on a much larger scale, cyber terrorism.[188] A regulatory committee would be able to create security processes to better protect against such crimes.[189] The committee could recommend strategies to prevent software companies from escaping legal responsibility for design defects often financially crippling companies when code is exploited.[190]

E. Separate Criminal and Civil Statutes

The CFAA applies to both criminal and civil cases. The more these types of cases are litigated, the more likely definitions and concepts appropriate for either criminal or civil cases are applied in the wrong context.[191] The CFAA would be more effective legislation if the statute was separated for distinct criminal prosecution and civil application. Courts would then be able to accurately apply the proper standard in civil and criminal cases. The CFAA, at its creation, did not need a separate criminal and civil section. But the evolving digital world has grown more sophisticated and complicated; hence it necessitates bright line rules for the continued development of case law.

VI. Conclusion

The CFAA should be expanded to represent the digital age in which we live. One federal statute is inexplicably inadequate to cover the expansive number of different cybercrimes. Continued amendment and expansion to the CFAA risk unnecessarily increasing complexity in exchange for civil and criminal applicability. A fair and impartial trial is a fundamental right encompassed in the Bill of Rights.[192] By allowing evidence illegally obtained by vigilante hackers to be admissible is a great departure from the fundamental rights the Founding Fathers sought to protect.[193] All Americans should have available an adequate suppression remedy to protect against vigilante hackers. A society full of smartphones, smart televisions, PRISM, tablets, and Wi-Fi deserves, and requires, better federal statute protections. Congress must respond to the evolution of the Internet and technology by dissecting and resurrecting the Computer Fraud and Abuse Act. Congress must respond with the explicit intention of protecting the different electronic frontiers our society has created.

188. *Id* at 21.

189. *Id.* at 22.

190. *See id.* at 6.

191. *See generally* 18 U.S.C. § 1030.

192. *See generally* U.S. Const. amend. VI.

193. *Id.*