CTRL + SHIFT: DEFINING AUTHORIZATION UNDER THE COMPUTER FRAUD AND ABUSE ACT

Jordan Hutcheson[*]

INTRODUCTION

Judge Alex Kozinski of the Ninth Circuit Court of Appeals, when faced with a case brought under the Computer Fraud and Abuse Act ("CFAA") astutely summarized the interpretational conflict he confronted as follows:

> Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.[1]

Judge Kozinski appropriately underlines two important issues with the CFAA in this passage. First, he points out the fact that computers, having become a staple in society today for both business and social purposes, are still being considered in light of statutes formulated at the outset of computer invention, such as the CFAA, which was originally passed in 1984.[2] The second issue he alludes to is that the repercussions of using computers can potentially impose criminal and civil liability in the most unsuspecting situations, depending on how courts interpret the ambiguous language of the CFAA in today's modern, technologically advanced society.

The CFAA is a computer hacker statute that is used to invoke federal jurisdiction where an individual with unauthorized access gains entry to a protected computer.[3] The statute imposes both criminal and civil liability where an individual accesses and obtains information from a computer that he or she was unauthorized to obtain.[4] While the statute has been amended several times since its introduction in ways that broaden its scope, the ambiguous phrase, "without authorization," contained within two of the sections of the statute, has stood the test of legislative time.[5] Courts have had difficulty

---

[*] J.D. Candidate 2019, Antonin Scalia Law School at George Mason University; B.A. 2015, Virginia Polytechnic Institute and State University.

[1] United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).

[2] *See id.* at 856, 858.

[3] *See* 18 U.S.C. § 1030 (2012).

[4] *Compare id.* § 1030(c) (providing for criminal punishment), *with id.* § 1030(g) (providing for civil remedies).

[5] *See infra* Part I for an in-depth discussion of the amendments to the CFAA.

interpreting this clause, resulting in a pronounced circuit split that the Supreme Court and Congress have not yet addressed.[6] Depending on the jurisdiction, courts have interpreted the phrase in either a broad or a narrow fashion in both the criminal and civil contexts. The jurisdictions that favor the broad approach interpret "without authorization" in such a way that imposes use restrictions on anyone who uses a computer in a way that he or she is not designated to do.[7] The narrow approach, by contrast, defines "without authorization" as any computer access made without receiving approval for the access.[8]

To exemplify the difference between the two approaches, take, for instance, a situation in which you are facing criminal charges under the CFAA for downloading information from your company's password-protected database and giving the information to your employer's competitor. You were given the password and allowed to access the database for the purposes of your duties as an employee; however, you were prohibited under company policy—and likely your employment contract and noncompetition agreement—from disbursing the information contained on the database. Once your employer finds out about the wrongful dissemination, your employer terminates you then brings a civil suit against you alleging, among others, a cause of action under the CFAA. Assuming your employer could meet the other statutory requirements of the CFAA, the question would come down to what "without authorization" means in the context of the statute. Should your employer file suit in a narrow interpretation jurisdiction, the court would likely conclude that you had authorization to do this under the CFAA because you were given a password and allowed to access the database for your job, thereby concluding that you are not liable under the CFAA. However, should your employer file in a broad interpretation jurisdiction, the court would likely find that while you were authorized to access the database, company policy and your employment contract prohibited you from disbursing the information, thus finding you did act without authorization under the CFAA, leaving you subject to liability.

This example, while simplified and rather rudimentary, highlights the two approaches taken by the courts and the significant consequences the two interpretations have. Courts that adopt a broader interpretation typically follow what has been described as the "contract-based" approach, which allows "without authorization" to be defined by an employer or other provider of

---

6 *See infra* Part II for an in-depth discussion of the existing circuit split.

7 *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (quoting 18 U.S.C. § 1030(a)) (noting the "paper thin" difference between being "without authorization" and just "exceeding authorized access").

8 *See, e.g.*, WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (noting that reliance upon the rule of lenity requires selecting a narrow interpretation).

written terms of service.[9] The narrow interpretation courts, by contrast, follow what has been described as the "code-based" approach, which provides that an individual is "without authorization" when he or she must bypass a code or password to access information that was never intended to be accessed by that individual.[10] These two approaches both propose seemingly plausible solutions to defining "without authorization," but both also have significant shortcomings and flaws. In order to strike a balance, courts should seek to use a shifting approach, by employing the contract-based approach in cases arising under civil suits and employing the code-based approach in cases arising under the criminal section of the CFAA. By defining the phrase in this way, courts will leave the original intention of the CFAA intact and endorse the law's preference for freedom to contract, while also avoiding any unconstitutional or statutorily incorrect interpretations of the ambiguous language of the statute.

This Article proceeds in four parts. Part I discusses the statute's origin and tracks its development throughout the legislative process. Part I concludes by summarizing the statute's present statutory language and framework by providing a breakdown of each section. Part II introduces the current unresolved circuit split, highlighting the various arguments made by both the broad- and narrow-interpretation circuits in both the criminal and civil contexts. Part III discusses the code-based, contract-based, and agency-based approaches, the three mainstream interpretive propositions, and elaborates on their foundation. Part IV analyzes the strengths and weaknesses of the three approaches and concludes with an argument that courts should seek to apply a shifting approach between the contract-based and code-based theories, depending on whether the case arises under the civil or criminal context. This reconciliation between the two dominant approaches would placate due process and other constitutional concerns, as well as satisfy the original intent of the statute, support contractual obligations and the right of freedom to contract, and provide the most appropriate solution in interpreting the ambiguous phrase, "without authorization" in cases arising under the CFAA.

I. THE ORIGINS OF THE CFAA AND ITS SUBSEQUENT AMENDMENTS

Congress enacted the CFAA originally for national security purposes to protect government information. The CFAA was meant to protect the United States government's sensitive information and financial records by criminalizing the access and dissemination of such information to foreign nations.[11] But as originally enacted, the CFAA had little to no success in serving its

---

9 Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J. L. & PUB. POL'Y 661, 677 (2009).

10 *Id.*

11 *See* Glenn D. Baker, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/LAW J. 61, 64 (1992).

purpose, resulting in multiple amendments and changes to its language, structure, and scope. This Part documents these changes and the corresponding legislative history and summarizes the framework of the CFAA as it stands today.

A. *The Original 1984 Act*

As a response to the increasing use and accessibility of computers and the growing concerns of the abuses unauthorized access may lead to, Congress implemented the Counterfeit Access Device and Computer Fraud and Abuse Act in 1984.[12] The law made it a felony to access a computer with or without authorization to gain information relating to United States foreign relations or national defense, to cause "injury" to the United States, or disburse such sensitive information to a foreign state.[13] It also made it a misdemeanor to knowingly access a computer with or without authorization to obtain financial information from a financial institution or credit agency or to knowingly use, modify, destroy, or disclose information from a computer "operated for or on behalf of the Government."[14] At the time of this law's implementation, Congress recognized that changes in technology might create difficulty in formulating a timeless law capable of comprehending the technology to come.[15] Additionally, the law was met with little application in reality, as only one person was successfully indicted under this criminal statute until 1986, when Congress addressed the Act's shortcomings with a new amendment.[16]

B. *Subsequent Amendments*

Congress implemented the Computer Fraud and Abuse Act of 1986, which altered the original statute and broadened its scope. The 1986 Act created a federal computer fraud offense and an offense for the alteration,

---

12 *See* Sheri A. Dillon, Douglas E. Groene & Todd Hayward, *Computer Crimes*, 35 AM. CRIM. L. REV. 503, 507–08 (1998); *see also* H.R. REP. NO. 98-894, at 4 (1984) ("[I]t seems clear that we must not only bring our laws up-to-date . . . but also give serious consideration to deterring the criminal element from abusing computer technology in future frauds.").

13 *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub L. No. 98-473, § 2102(a), 98 Stat. 1837, 2190; Baker, *supra* note 11, at 64–65.

14 *See* Counterfeit Access Device and Computer Fraud and Abuse Act § 2102(a); Baker, *supra* note 11, at 64.

15 *See* H.R. REP. NO. 98-894, at 9 (1984) ("As these computer technologies and the means for abusing them have rapidly emerged, they have been confronted by a criminal justice system which is largely uninformed concerning the technical aspects of computerization, and bound by traditional legal machinery which in many cases may be ineffective against unconventional criminal operations.").

16 Baker, *supra* note 11, at 65.

damage, or destruction of information contained in a "Federal interest computer."[17] It also amended the scienter requirement by raising the standard from "knowingly" to "intentionally."[18] The purpose of this scienter amendment was to differentiate between those who knowingly, yet inadvertently, accessed another's computer file or data, and those who indicated a clear intent to access another's computer files and data without authorization.[19] Additionally, it created a law enforcement and intelligence activity exception, clarifying that the statute did not prohibit "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States."[20]

Lastly, and most importantly, in an effort to clarify the statute, the 1986 Act tacked on "or exceeds authorized access" to eliminate the language criminalizing authorized access, defining the new term as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[21] The original language of the subsection did not specify that the criminal conduct was limited to those who did not already have authorized access to government computers through their employment.[22] Congress sought to ensure that federal employees would not be prosecuted for acts of computer access of computers to which they were meant to have access to because that "did not rise to the level of criminal conduct."[23] The Judiciary Committee, which enacted the 1986 bill, stated that this amended section of the Act was intended to be limited "to cases where the offender is completely outside the Government."[24]

---

17 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, 1215 (amending 18 U.S.C. § 1030(e) and defining a federal interest computer as "a computer . . . exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or . . . [a computer] which is one of two or more computers used in committing the offense, not all of which are located in the same State"); Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 474–75 (1990).

18 Computer Fraud and Abuse Act of 1986 § 2 (amending 18 U.S.C. § 1030(a)(2)); Griffith, *supra* note 17, at 475.

19 S. REP. NO. 99-432, at 6 (1986) (stating that the "knowingly" standard "might not be sufficient to preclude liability on the part of those who inadvertently 'stumble into' someone else's computer file or computer data"); *see also* Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.S. DAVIS L. REV. 283, 293 (1997) ("[U]nder the 1986 Act, even if a person does not intend to damage the computer system, liability will attach if the person intended to access the computer system.").

20 Computer Fraud and Abuse Act of 1986, 100 Stat. at 1216 (amending 18 U.S.C. § 1030).

21 *Id.* at 1213, 1215.

22 *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub L. No. 98-473, § 2102(a), 98 Stat. 1837, 2190.

23 *See* S. REP. NO. 99-432, at 7 (1986); Griffith, *supra* note 17, at 477.

24 *See* S. REP. NO. 99-432, at 8 (1986).

The 1986 Amendments were a step in the right direction, but they still resulted in various concerns of inadequacy.[25] The Judiciary Committee was concerned that the statute would be too broad in that it would allow the federal government to have broad jurisdiction over computer-related crimes better left to be handled by states, despite the Committee's attempts to limit the statute to apply only to computers active in interstate commerce.[26] And despite legislative efforts to clarify the CFAA, commentators still expressed concerns over key terms lacking clarity by definition, including the terms "computer" and "access," as well as the problem that no civil remedies were available, while jail terms did not adequately provide redress in some computer trespass situations.[27] Additionally, it became apparent that the amendments could not accommodate arising computer viruses and malware.[28]

The next most significant amendments to the CFAA occurred in 1994 and 1996, where Congress again modified the CFAA to address some of these concerns.[29] In 1994, Congress addressed the computer virus and malware issue by adding a section criminalizing "the transmission of a program, information, code, or command to a computer or computer system" with intent to "damage or cause damage to" a computer or its data.[30] Additionally, Congress added a private cause of action by providing for a civil remedy for persons who suffer damage by anyone who violates the criminal provisions of the statute.[31] The amendments also once again adjusted the scienter requirements, applying "knowingly" to access in some sections, and "intentionally" in others.[32] The first subsection of the CFAA made it a crime to *knowingly* cause the transmission of a code or program with intent to cause damage to a protected computer.[33] And the second subsection was altered to apply to hackers who *recklessly* cause damage.[34] In 1996, Congress further

---

25 *See id.* at 4; Baker, *supra* note 11, at 71.

26 *See* S. REP. NO. 99-432, at 4 (1986) ("Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling federal interest . . . .").

27 Baker, *supra* note 11, at 71.

28 *Id.*

29 *See* Hong, *supra* note 19, at 294–95; Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. No. 1-12, ¶ 8 (2010).

30 *See* Computer Abuse Amendments Act of 1994, Pub L. No. 103-322, tit. 29, 108 Stat. 2097 (amending 18 U.S.C. § 1030(a)(5)).

31 *Id.* § 290001(d) (codified at 18 U.S.C. § 1030(g)); Pollaro, *supra* note 29, ¶ 8.

32 *See* National Information Infrastructure Protection Act § 201, 110 Stat. at 3491–92; Hong, *supra* note 19, at 294–98.

33 *See* 18 U.S.C. § 1030(a)(5)(A).

34 National Information Infrastructure Protection Act § 201, 110 Stat. at 3492; Hong, *supra* note 19, at 297–98 ("Unlike the intentional damage requirement of the first felony subsection, the second felony subsection requires the much lower mens rea level of recklessness." (footnote omitted)).

broadened the scope of the statute by specifying that a "protected computer" (formerly a "Federal interest computer") is any computer "which is used in interstate or foreign commerce or communication."[35] Thus with the 1994 and 1996 amendments, the CFAA was broadened considerably to impose criminal and civil liability on inside violators and outside hackers in both the federal government and private sector, so long as the subject computer was used in interstate commerce in some way.[36]

Congress has ultimately amended the CFAA nine times since its original creation in 1984.[37] What originated as a computer crime statute aimed at protecting government interests in the name of national security and security of government property on federal computers became a broad law capable of applying to any computer used within the United States and imposing civil or criminal liability to anyone who intentionally in some instances, and knowingly in others, accesses a computer without authorization and causes damage.[38] As one can imagine, following these amendments, civil claims and criminal charges under the CFAA began to appear more readily in federal courts.

C. *The Current Framework of the CFAA*

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, now operates under ten subsections. The relevant sections are summarized as follows:

Subsection (a) lists the actions prohibited under the statute. Most significantly, paragraph (a)(1) still applies to national defense or foreign relations data, and prohibits the act of "having knowingly accessed a computer without authorization or exceeding authorized access" obtaining and communicating (or attempting to do so) data relating to national defense or foreign relations, with intent to cause injury to the United States.[39] Paragraph (a)(2) prohibits intentionally accessing a computer "without authorization or exceed[ing] authorized access" and obtaining "information contained in a financial record of a financial institution" as well as, more generally, "information from any protected computer."[40] In addition to these broader provisions, Subsection (a)

---

35 National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, tit 2, 110 Stat. 3491, 3493; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1568 (2010) ("The critical difference between a 'Federal interest' computer and a 'protected computer' was that the former required computers in two or more states, while the latter merely required a machine 'used' in interstate commerce.").

36 *See* Kerr, *supra* note 35, at 1568; Hong, *supra* note 19, at 295–96; Pollaro, *supra* note 29, at ¶ 8.

37 Tiffany Curtiss, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1817 (2016).

38 *Id.*

39 18 U.S.C. § 1030(a)(1) (2012).

40 *Id.* § 1030(a)(2).

further prohibits various other actions, including intentionally "access[ing] any nonpublic computer of a department or agency of the Unites States," as well as knowingly causing the transmission of a command to a protected computer and thereby intentionally causing damage.[41]

Subsection (b) expounds that "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) . . . shall be punished as provided in subsection (c)."[42] Subsection (c) provides for the criminal punishment of violating subsections (a) or (b), which consists of specific fines and imprisonment for damages or loss caused by a violation.[43] Subsection (d) provides that the United States Secret Service, the Federal Bureau of Investigation, or any other agency having authority may investigate offenses under the CFAA.[44] Subsection (e) defines, among others, the terms "computer," "protected computer," "exceeds authorized access," "damage," and "loss."[45] Subsection (f) specifies that the statute does not prohibit any law enforcement agency of the United States or any state from engaging in "lawfully authorized investigative . . . activity."[46] Subsection (g) stipulates that any person who suffers economic damage or loss pursuant to the prohibited action under subsection (a) "may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief" as long as the action is brought within two years of the offense.[47]

The CFAA today reflects the original intent of the Act as it stood in the 1980s, in that it maintains provisions for protecting government information and financial records.[48] However, as the amendments to the Act and the current language of the statute indicate, the CFAA expands into much broader territory.[49] But one consistency between the original 1984 statute and the CFAA as it reads today is the use of the terms "without authorization" and "exceeds (or 'exceeding') authorized access."[50] Courts have found that this qualifying language is ambiguous, which has led to a circuit split in the interpretation and application of the statute in both the criminal and civil contexts.

---

41 *Id.* § 1030(a).

42 *Id.* § 1030(b).

43 *See id.* § 1030(c).

44 *Id.* § 1030(d).

45 18 U.S.C. § 1030(e).

46 *Id.* § 1030(f).

47 *Id.* § 1030(g).

48 *See id.* § 1030(a); Matthew Gordon, Note, *A Hybrid Approach to Analyzing Authorization in the Computer Fraud and Abuse Act*, 21 B.U. J. SCI. & TECH. L. 357, 360–61 (2015).

49 *See* 18 U.S.C. § 1030; Gordon, *supra* note 48, at 360–61.

50 *See* 18 U.S.C. § 1030; Gordon, *supra* note 48, at 361–62.

II. CIRCUIT SPLIT: DEFINING "WITHOUT AUTHORIZATION" BROADLY AND NARROWLY UNDER THE CFAA

The term "exceeds authorized access" is defined by subsection (e) of the CFAA as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[51] However, the legislative drafters at no point in the CFAA's developmental history specifically defined what "without authorization" means. In its modern application, courts have split, with some jurisdictions interpreting "without authorization" broadly, and other jurisdictions interpreting the ambiguous phrase narrowly.

A. *The Broad Interpretation Jurisdictions*

The First, Fifth, Seventh, and Eleventh Circuits abide by the broad interpretation of "without authorization" and maintain that the CFAA extends liability in both the criminal and civil contexts where a person has authorization to access information but misuses that authorization.

For instance, the Seventh Circuit found in *International Airport Centers, LLC v. Citrin*,[52] a civil case brought by an employer against its former employee, that the defendant-employee was liable where he erased files from a work computer.[53] The employer gave the defendant-employee a work computer to collect and record data, and after some time, the defendant-employee decided to quit the company.[54] Before returning the work computer, he deleted all the data the computer contained.[55] The court found that the defendant's actions fell within the definition provided in the statute for "exceeding authorized access," although admitting that the difference between "without authorization" and "exceeding authorized access" was "paper thin."[56] The court further found that the defendant-employee violated the CFAA, proclaiming that he violated the "duty of loyalty that an agency law imposes on an employee."[57] The court focused on the defendant's breach of the agency relationship and found that even though his employment contract provided that he was authorized to "return or destroy" data, the purpose of the provision was to limit disclosure of confidential information and thus was not applicable to the defendant's actions.[58]

---

51 18 U.S.C. § 1030(e)(6).

52 Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

53 *Id.* at 421.

54 *Id.* at 419.

55 *Id.*

56 *Id.* at 420.

57 *Id.*

58 *Citrin*, 440 F.3d at 420–21 (emphasis removed).

The First Circuit, when faced with a CFAA civil claim in *EF Cultural Travel BV v. Explorica, Inc.*[59] looked to the existing contract between the parties to define "without authorization."[60] In this case, Explorica, Inc. used a "scraper," a type of internet robot, to download EF Cultural Travel's tour prices and information to undercut their prices and compete in the global student tours market.[61] The court concluded that the contractual and technical restraints between the two companies clearly notified Explorica, Inc. that its use of a scraper was unauthorized, but that Explorica, Inc. did have authorization to access the website where it employed the scraper.[62] The court concluded, "because of the broad confidentiality agreement," Explorica, Inc. exceeded authorized access, as defined in 18 U.S.C. § 1030(e)(6), and was therefore liable under the CFAA.[63]

When faced with a criminal case brought under the CFAA, the Eleventh Circuit, like the First Circuit, looked to employer contract and policy documents as applicable to the "exceeds authorized access" phrase of the statute in *United States v. Rodriguez*.[64] The defendant was authorized by the Social Security Administration to access a database as an employed TeleService representative, which he did to obtain information for his own personal use.[65] The court turned to the employment policy in place, which provided that the use of databases to obtain personal information is only authorized when done for business purposes, and concluded that the defendant did not have authorization because of the language in the employment policy.[66] The defendant argued that he should not be convicted under the CFAA because he did not use the information he accessed to defraud anyone or for financial gain.[67] The court disagreed, finding that the plain language of the Act and the entire statutory context rendered that argument irrelevant.[68] The court further concluded that the defendant on appeal could not prove that his one-year jail sentence for violation of the CFAA was unreasonable.[69]

The Fifth Circuit, similar to the Eleventh Circuit, supported the broad interpretation of "without authorization" in a criminal suit brought under the

---

59 274 F.3d 577 (1st Cir. 2001).

60 *See id.* at 582.

61 *Id.* at 579.

62 *Id.* at 580.

63 *Id.* at 581–82.

64 628 F.3d 1258, 1263 (11th Cir. 2010).

65 *Id.* at 1260, 1263.

66 *Id.* at 1263.

67 *Id.* at 1264.

68 *Id.* at 1264 ("The misdemeanor penalty provision of the Act under which Rodriguez was convicted does not contain any language regarding purposes for committing the offense.").

69 *Id.* at 1264–65.

CFAA in *United States v. John*.[70] In this case, the defendant, an employee of Citigroup, viewed and printed information she was authorized to view through her employment position.[71] However, she provided the information she accessed to her half-brother for fraudulent purposes.[72] Similar to the defendant in *Rodriquez*, the defendant in this case argued that she was authorized to use Citigroup's computers and view and print the information, just not to use it for fraudulent purposes, and therefore the CFAA charges did not apply.[73] The court, considering this argument, determined that the question before them was "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."[74] The court held that "exceeds authorized access" encompasses situations where "the user knows or reasonably should know that he or she is not authorized to access a computer and [use] information obtain[ed] from that access . . . to perpetrate a crime."[75] The court found that the defendant was clearly aware that she violated Citigroup's employment policy, and therefore "exceeded authorized access" which exposed her to criminal liability.[76]

These cases exemplify that the jurisdictions that employ the broad approach focus on a few important aspects when determining liability under the CFAA. Most notably, these courts find very little difference between "without authorization" and "exceeds authorized access."[77] In coming to that conclusion, they look to the employers and providers to determine authorization. In some instances, that involves looking to contracts, employment agreements and policies, and other written provider terms of service. In other instances, the courts look for a breach of an agency relationship or situations in which the defendant knew or should have known he did not have authorization from his principal to access or disseminate the information. Ultimately, these jurisdictions find criminal and civil liability under the CFAA by looking to define "authorization" by actions or agreements between employers and providers, and the employees or computer users accused.[78]

---

70 597 F.3d 263, 271–72 (5th Cir. 2010).

71 *Id.* at 269.

72 *Id.*

73 *Id.* at 271.

74 *Id.*

75 *Id.*

76 *John*, 597 F.3d at 272 ("While we do not necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural Travel BV* would give rise to criminal culpability, we do agree with the First Circuit that the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'").

77 *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); *John*, 597 F.3d at 271; Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001).

78 *See, e.g.*, *Rodriguez*, 628 F.3d at 1263; *John*, 597 F.3d at 270–71; *Citrin*, 440 F.3d at 420.

B. *The Narrow Interpretation Jurisdictions*

The Fourth and Ninth Circuits, recently joined by the Second Circuit, paved the way for the circuit split by digressing from the broader interpretation of "without authorization" employed by the aforementioned jurisdictions.

In *WEC Carolina Energy Solutions LLC v. Miller*,[79] the Fourth Circuit weighed in on a civil action brought under the CFAA. In this case, the defendant downloaded proprietary information from his company during his employment and used it to make a presentation to a competitor after resigning.[80] While the defendant had been authorized to access the information from his company laptop, company policy prohibited using the information without authorization and downloading it to a personal computer.[81] The court concluded that acting "without authorization" occurs when an employee "gains admission to a computer without [*any*] approval," and an employee "exceeds authorized access" when he "has approval to access a computer, but uses his access to obtain [information] . . . outside the bounds of his approved access."[82] The court found that this distinction leaves two plausible interpretations, and thus determined the rule of lenity provided they must choose the narrower interpretation, concluding that the defendant was not liable because he had authorization to access the information during his employment.[83]

In *LVRC Holdings LLC v. Brekka*,[84] the Ninth Circuit heard a civil suit brought by an employer who sought to recover from a former employee under the CFAA.[85] The former employee sent several company emails to his private email account during his employment, which was not an unusual employment practice, and accessed this information following his dismissal from the company.[86] In its interpretation of "without authorization," the court rightfully started with the plain language of the statute and found that the dictionary definition of authorization, "permission or power granted by an authority,"[87] supported the employee's argument that he was not liable because he was given authorization by his employer at one point to access the information.[88] The court found that the language of the statute and the

---

79 687 F.3d 199 (4th Cir. 2012).

80 *Id.* at 201.

81 *Id.* at 202.

82 *Id.* at 204.

83 *Id.* at 205–07.

84 LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

85 *Id.* at 1128–29.

86 *Id.* at 1129–30.

87 *Id.* at 1133 (quoting *Authorization*, RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2001)).

88 *Id.* ("[A] person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question.").

definition of "exceeds authorized access" supported this contention.[89] The court further provided that the employer must maintain some responsibility in determining authorization, as "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'"[90] Since in this case the employee not only had permission to access the computer, but also was required to for employment purposes, the court determined he was therefore not liable under the CFAA.[91]

When the Ninth Circuit was faced with a factually similar case brought under the criminal sections of the CFAA, the court again followed the reasoning and holding in *Brekka*. In *United States v. Nosal*,[92] Defendant David Nosal left his position at an executive search firm and subsequently convinced some former colleagues to help start a competing business.[93] The former colleagues accessed the company database at the executive search firm to obtain and disclose confidential information using their login credentials, but in so doing acted contrary to their company policy, which forbade this behavior.[94] The court found in favor of the defendant, reasoning that Congress could not have intended to impose criminal liability upon everyone who uses a computer, given the statute's purpose as an anti-hacking measure.[95] The court reasoned further that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes."[96] The court emphasized this by using the example that Google at the time forbade minors from using its services, a restriction that very few people knew about.[97] While minors inevitably used Google services, the court found that no one could possibly imagine that a minor would be a juvenile delinquent for using Google, nor that a person could be sent to a federal prison for any number of innocuous terms-of-use violations.[98] The court concluded that using the narrow interpretation of "without authorization" was further supported by the rule of lenity, and found therefore that the defendant's accomplices did not act "without authorization" because they used their login credentials to obtain the information.[99]

---

89 *Id.*

90 *Brekka*, 581 F.3d at 1133.

91 *Id.* at 1135.

92 676 F.3d 854 (9th Cir. 2012).

93 *Id.* at 856.

94 *Id.*

95 *Id.* at 857, 864 ("If 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.").

96 *Id.* at 860.

97 *Id.* at 861.

98 *Nosal*, 676 F.3d at 861.

99 *Id.* at 863–64.

The Second Circuit is the most recent circuit to weigh in on how to interpret "without authorization" under the CFAA. In a criminal suit brought under the CFAA, the Second Circuit in *United States v. Valle*[100] found that the defendant was not guilty under a narrow definition of "without authorization," despite his distasteful conduct. In *Valle*, the defendant was an NYPD police officer who was also a member of an internet sex fetish community.[101] A criminal suit ensued after the defendant used a police database to obtain personal information about a woman who he and the other members of the internet sex fetish community discussed performing horrific acts on.[102] While there is no question the defendant in this instance used his authorized computer access for personal use, he technically never obtained information he was not entitled to obtain through his employment as a police officer.[103] The court cited *Brekka* in its analysis, finding that the dictionary definition of "authorization" supported the notion that accessing a computer without authorization means accessing a computer without permission to do so at all.[104]

But the court also found that the legislative history also pointed to the understanding that the "exceeds authorized language" portion was intended to cover situations in which a person accessed a computer "for purposes to which such authorization does not extend."[105] The court ultimately concluded, similar to the Fourth Circuit in *Miller*, that given that there were two possible constructions of the statute, the rule of lenity required the court to rule in favor of the defendant.[106] Additionally, and somewhat ironically, the court found that this ruling favored public policy, because the narrow interpretation of "without authorization" would not subject individuals to the risk of criminalizing ordinary behavior, despite the behavior of the police officer defendant in this case being far from ordinary.[107]

Unlike the jurisdictions that interpret the CFAA broadly, the jurisdictions that interpret the CFAA's authorization clauses narrowly find that the distinction between "without authorization" and "exceeds authorized access" is very significant. These courts, while suggesting that company policy or terms of service may fall under the category of "exceeds authorized access" when breached, do not find that these policies or terms are sufficient to determine "authorization" under the CFAA. They further take issue with the potential that interpreting "authorization" broadly may extend criminal liability in too many instances, given the prevalence of computers.

---

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

101 *Id.* at 512.

102 *Id.* at 512–13.

103 *Id.* at 523–24.

104 *Id.* at 524.

105 *Id.* at 525 (emphasis removed) (citing Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat, 1837, 2190 (codified as amended at 18 U.S.C. § 1030)).

106 *Valle*, 807 F.3d at 526.

107 *Id.* at 528.

As this circuit split demonstrates, the courts have had a difficult time in determining what the phrase "without authorization" should entail and how it works together with "exceeds authorized access." Some circuits focus on "exceeds authorized access" to interpret the clause as a broad coverage of computer use that authorizes criminal liability where a user was allowed to access the computer, but did so in a way that exceeded the scope of the access.[108] The more recent trend in the courts, however, has been the narrow approach taken by the Fourth, Ninth, and most recently, the Second Circuits.[109] The narrow approach also has a large coalition of support among the legal community because a broad interpretation has the potential to make the CFAA unconstitutional.[110] Ultimately, the different interpretations need to be reconciled, as the outcome of the two vastly different interpretations leaves inconsistency in the law. Some may find themselves liable for jail time for innocuous computer activity, while others may walk away free from punishment for significant computer breaches and damages.

III. THE CODE-BASED, CONTRACT-BASED, AND AGENCY-BASED APPROACHES

The Second Circuit has somewhat ironically defined "authorization" to be a word "of common usage, without any technical or ambiguous meaning."[111] Black's Law Dictionary defines authorization as "[o]fficial permission to do something" or "[t]he official document granting such permission."[112] In a circular and inconclusive fashion, Black's Law Dictionary further defines "official" as "[a]uthorized or approved by a proper authority."[113] Given the plain meaning and dictionary definition of "authorization," the courts are left with no definitive textual answer to defining "without authorization," and thus have rightly turned to other methods of interpretation.

---

108 *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001).

109 *See, e.g.*, *Valle*, 807 F.3d at 526–27; WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

110 *See* Kerr, *supra* note 35, at 1562 ("The meaning of unauthorized access is remarkably unclear . . . . The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional."); Michael C. Mikulic, Note, *The Unconstitutionality of the Computer Fraud and Abuse Act*, 30 NOTRE DAME J.L., ETHICS & PUB. POL'Y 175, 189 (2016) ("Due to the CFAA's alarming reach under the broad interpretation, the statute must be construed differently.").

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

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

113 *Official*, BLACK'S LAW DICTIONARY (10th ed. 2014).

Additionally, the phrase "or exceeds authorized access" that follows "without authorization" in the statute provides no clarity on the matter, despite being specifically defined by Congress. Paragraph (e)(6) of the CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[114] This definition does not clarify the ambiguity of what "authorization" is and courts have continued to struggle with the interpretation of the clause, despite the provided definition. For instance, the Fourth Circuit in *Miller* pointed out, "without authorization or exceeds authorized access" leaves the interpretation subject to two plausible interpretations.[115]

Absent a Congressional solution to the ambiguity of the language of the CFAA, scholarly sources and courts have taken it upon themselves to propose their own solutions. As a result, two propositions to defining "without authorization" have made regular appearances.[116] These two approaches, stemming from judicial interpretation, have been labeled the contract-based approach and the code-based approach.[117] Both of these approaches have been criticized in different ways for their incompatibility with various measures of the CFAA and courts have not specifically chosen and implemented either approach across the board.[118]

The contract-based approach to defining "without authorization" leaves the defining to the employer.[119] This approach gives employers the freedom to set the limits of authorization within their employment contracts by stipulating how its employees may or may not use their computers.[120] This approach stems from the decisions and rationale in cases such as *Rodriguez*, where the printing and disbursing of personal information contained in a database violated an employment policy, and *EF Cultural Travel BV*, where the use of the robot scraper was specifically prohibited in the employment contract governing the contracting parties.[121] When a party enters into a contract

---

114 18 U.S.C. § 1030(e)(6) (2012).

115 WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205–06 (4th Cir. 2012).

116 Boyer, *supra* note 9, at 677.

117 *Id.*

118 *Id.* at 678; *see also* United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012) (concluding that "without authorization" does not encompass using login credentials to obtain information). *But see* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001) (concluding that the broad confidentiality agreement between the defendant and his employer prohibiting access to the information obtained dictated "without authorization" under the statute).

119 Gordon, *supra* note 48, at 375.

120 *Id.*; *see also* Boyer, *supra* note 9, at 677 ("In order for access to be unauthorized under this contract understanding of use, 'a user can violate a contractual agreement' by using the system beyond the scope of the contractual right to use such a computer." (quoting Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1596 (2003))).

121 *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); *Explorica, Inc.*, 274 F.3d at 581.

with another party, it follows that the party that breaches the contract should be liable to the other for damages, as was the case in *EF Cultural Travel BV.* However, the criminal conviction and one-year jail sentence that resulted from the decision in *Rodriquez* highlights why allowing an employer to define authorization through a contract-based approach seems to run afoul of the CFAA for several different reasons.[122]

The code-based interpretation of "without authorization" requires a user "to circumvent some type of code restriction in order to gain access to particular information on a computer."[123] In order to violate the CFAA under the code-based approach, a person can only act without authorization or exceed authorized access when he or she takes action to bypass a code (i.e., password protection, technological barrier, etc.) to gain access to information that he or she is aware access to is prohibited.[124] This approach is narrower than the contract-based approach, as under a code-based approach, an individual cannot violate the CFAA merely by breaching an employment policy.[125] Rather, this approach puts the burden on the employer, or more generally, on computer owners, to simply protect their information.[126]

Additionally, a third approach has been proposed, and, although it has been explicitly rejected by numerous courts and legal scholars, it is worth mentioning.[127] This approach has been labeled the "agency-based approach," and is rooted in the Seventh Circuit's determination that an employee's status as an "agent" of his company has implications that are relevant to the CFAA.[128] Under the agency-based approach, an individual's motivations are evaluated to define authorization, and common-law principles of agency are applied.[129] The Second Restatement of Agency provides, "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[130] When applied to the CFAA, this definition implies that authorization would cease upon the creation of the adverse interest, even if explicit

---

122 *See* Kelsey T. Patterson, Note, *Narrowing it Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 513 (2013).

123 *See id.* at 505; *see also* Garrett D. Urban, Comment, *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, 1379–80 (2011).

124 Patterson, *supra* note 122, at 505; *see also* 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, 460 (2009).

125 Patterson, *supra* note 122, at 506.

126 Urban, *supra* note 123, at 1379–80.

127 *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (specifically rejecting the agency-based approach).

128 *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); Ryan H. Niland, *Do Not Read This Article at Work: The CFAA's Vagueness Problem and Recent Legislative Attempts to Correct It*, 15 N.C. J.L. & TECH. ONLINE EDITION 205, 214–15 (2014).

129 Niland, *supra* note 128, at 214–15.

130 RESTATEMENT (SECOND) OF AGENCY § 112 (AM. LAW INST. 1958).

permission to use a specific computer exists.[131] The agency-based approach may arise in instances in which the courts have determined that the defendants have used information from their former employers for the purposes of starting new businesses.[132] For example, in *Citrin*, the defendant deleted information prior to quitting the company to start a competing business.[133] The court made the point that the defendant's "breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access [his] laptop."[134]

The agency-based approach, while purported as a "middle ground" between the code-based and contract-based interpretations, is unpopular for several reasons. Interpreting authorization with an application of agency law as the agency-based approach suggests creates very broad liability. Such broad liability is not only contrary to the established purpose of the CFAA, but it also clearly exceeds "without authorization," no matter how ambiguous the phrase may be.[135] For instance, the agency-based approach leaves open the possibility that an employee can be criminally or civilly liable under the CFAA despite having both login credentials through an active employment, as well as contractual permission to access the information in question. The agency-based approach would therefore appear to neglect the phrase "without authorization" altogether and instead look to "adverse interest," which essentially negates any distinction between the statute's use of "without authorization" and "exceeds authorization."[136] Perhaps it is pertinent in employment situations to evaluate an employee's adverse interest as a factor, but the wide scope of the agency-based approach cannot adequately by itself compensate for the varying interpretations of "without authorization."

IV. A SHIFTING APPROACH TO DEFINING "WITHOUT AUTHORIZATION" UNDER THE COMPUTER FRAUD AND ABUSE ACT

While the agency-based approach does not seem to offer a comfortable solution to the interpretational dilemma of the CFAA, a combination of the contract-based approach and the code-based approach may serve as the proper solution to the CFAA's ambiguous "without authorization" clause. By employing a shifting interpretation of "authorization" based on these two predominant approaches, courts can apply the CFAA in such a way that would be compatible to both sides of the circuit split until such time Congress

---

131 Urban, *supra* note 126, at 1377.

132 *E.g.*, *Citrin*, 440 F.3d at 419; Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122 (W.D. Wash. 2000).

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

134 *Id.* at 420–21.

135 Urban, *supra* note 126, at 1393.

136 *Id.* at 1393–94.

clarifies the meaning of the statute or the Supreme Court establishes a precedent for the lower courts to follow.

The code-based approach purports to be a solution in the criminal context of the CFAA but falls short in the civil context. The code-based approach stems from the decisions and rationale in cases such as *Brekka* and *Nosal*. In *Brekka*, an employee accessed company emails after his employment was terminated, but the court found he did not act without authorization because he was allowed access to the emails at one point (i.e., during his employment).[137] In *Nosal*, where the defendant accessed confidential information in violation of company policy to obtain and disclose the information to start a competing business, the defendant was not guilty under the CFAA because he used his own login credentials, as authorized at one point by his employer.[138] These two cases, both arising under the CFAA from the Ninth Circuit within three years of each other, demonstrate the circuit's different considerations and reasoning in criminal and civil CFAA suits, despite yielding similar results.[139]

What is significant about these two decisions is how the same court determined in two different ways how "authorization" should be defined. In *Brekka*, the civil suit, the court was quick to distinguish that an employer must maintain some responsibility for determining authorization because "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'"[140] While the court made this distinction, seemingly leaning towards the contract-based approach, the court ultimately decided for the employee.[141] The court grappled with the dictionary definition of "authorization" and found that the definition supported the defendant's argument that he was not liable because he was given authorization to access the company information that he emailed to his personal email account.[142] In this holding, the court made the distinction that an employer should maintain responsibility for deciding authorization in a civil case such as this, ultimately finding for the defendant because the employer never officially rescinded his authorization.[143]

However, in *Nosal*, the defendant was facing criminal charges under the CFAA, and the Ninth Circuit used the code-based approach in a more direct fashion, practically ignoring the "employer defines authorization" rationale predominant in *Brekka*.[144] The circumstances in this case involved an

---

137 LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133–34 (9th Cir. 2009).

138 *See* United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012).

139 *See id.*; *Brekka*, 581 F.3d at 1135.

140 *Brekka*, 581 F.3d at 1133.

141 *Id.*

142 *Id.*

143 *Id.* at 1135.

144 *See* United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc).

employee who left his employer in order to start a competing business of his own.[145] He and a few former colleagues used their login credentials to access confidential company information, explicitly contrary to their former company policy.[146] This time, the Ninth Circuit wasted no time in concluding the code-based approach was more appropriate in this criminal context, by concluding that the legislative intent of the CFAA did not support the contract-based approach.[147] The court was not willing to extend criminal liability to violations of computer use policies in this instance.[148]

What this evaluation of the analyses of the two Ninth Circuit holdings in *Brekka* and *Nosal* intends to highlight is the willingness of a court that has defined "authorization" narrowly through a code-based approach to recognize the merits of the contract-based approach in the civil context. However, just as the court in *Nosal* indicated, the code-based approach used to define "authorization" is appropriately employed when criminal charges arise under the CFAA, but is too narrow in civil cases arising under the same statute. Thus, courts should seek to employ a shifting analysis by applying the code-based approach in criminal suits, and the contract-based approach in civil suits arising under the CFAA.

A. *Contractual Obligations in Civil Law*

The contract-based approach is appropriate under 18 U.S.C. § 1030(g) where the CFAA imposes civil liability for several different reasons. First, there is a basic principle in natural law that one has absolute property rights to the goods that are produced by a combination of his labor and non-appropriated materials.[149] As an extension of that natural right, employers and employees should have the freedom to contract as they desire.[150] To allow oneself the ability to bind his future self is allowing for his autonomy by enlarging the realm of voluntary agreement, and to not allow an individual to bind his future self would take away one's self-determination.[151]

---

145 *Id.* at 856.

146 *Id.*

147 *See id.* (noting that the CFAA was intended by Congress to be an anti-hacking measure).

148 *Id.* at 863.

149 *See* David Bear, *Establishing a Moral Duty to Obey the Law Through a Jurisprudence of Law and Economics*, 34 FLA. ST. U. L. REV. 491, 504 (2007).

150 *See id.* at 505 ("Freedom to contract holds that an individual may freely and voluntarily enter into a contract, that a contract shall not be held void, and that a contract shall be enforced." (emphasis removed)).

151 *See* CHARLES FRIED, CONTRACT AS PROMISE 8, 16, 20–21 (2d ed. 2015) (arguing that the state must enforce contracts because it is good behavior to honor one's promise).

This philosophical principle has been further established by the Supreme Court and followed by state courts, as the courts have taken the position that a party's freedom to contract should be given effect between the parties, unless a public policy takes precedence.[152] Many other courts have recognized that freedom to contract is a qualified right protected by the Fifth and Fourteenth Amendments to the United States Constitution.[153] It follows that an employee's signature on a contract or company policy represents an understanding of one's behavior and willingness to bind one's future self.[154] In such instances, an ordinary employee could reasonably expect that a breach of an employment contract would lead to liability to his employer in a legal setting.[155] In jurisdictions that interpret the CFAA broadly, the contract-based approach may be significant to delineate the scope of the employee's authorization regarding the computer system.[156]

However, if the contract-based approach was used as an exclusive remedy to defining "authorization" throughout the entirety of the CFAA, employers could include prohibitions regarding computers and access in their employment contracts that use overtly broad and general language.[157] This is because it would be a very difficult task for an employer to consider and express every possible scenario within the confines of its contract of the ways in which employees are not authorized regarding the use of its computers.[158] The contract-based approach could potentially create a situation where employers broadly define "without authorization" while drafting their policies in such a way that leaves employees accessing information against employer policy for mild digressions from routine job duties.[159] It is not feasible for every employee to possess the wherewithal or desire to negotiate alterations

---

152 *See, e.g.*, Broaddus v. Broaddus, 130 S.E. 794, 799 (Va. 1925) ("Freedom to contract is one of the liberties of every *sui juris* citizen which the law very carefully safeguards."); Green v. Safeco Life Ins., 727 N.E.2d 393, 397 (Ill. App. Ct. 2000).

153 *See, e.g.*, Manhattan Bldgs., Inc. v. Hurley, 643 P.2d 87, 95 (Kan. 1982).

154 Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 117 (2013).

155 *Id.*

156 Peter J.G. Toren, *Computer Fraud and Abuse Act*, 9 LANDSLIDE 42, 46 (2017) ("The agreement should very clearly state that the employee's access of the computer system is limited by the employee's employment responsibilities, and any use of the computer system that is inconsistent with this understanding or contrary to the interests of the employer is without authorization.").

157 Gordon, *supra* note 48, at 375.

158 *Id.*

159 Patterson, *supra* note 122, at 525 (arguing that the contract-based approach creates an avenue through which "clever employers" could implement the CFAA in areas like "employee frolics" and "Terms of Service"); Urban, *supra* note 123, at 1399 ("Any actions, such as reading e-mail, checking college basketball scores, or simply being inefficient, could be contractually defined as a violation of the statute.").

to employment agreements,[160] and employers (or their attorneys) draft their contracts in order to protect their own interests.[161]

If the contract-based approach was applied across the board, such mild digressions from routine job duties resulting in a breach of a private employment contract could invoke unwarranted criminal liability under the CFAA. Many federal and state legislatures and courts have placed varying limits on the enforceability of employment contracts to protect employees and employers alike.[162] To give just one example, most states and courts have asserted general rules for noncompete agreements in the employment context, often requiring noncompete agreements be reasonably restrictive in geographic scope, practice area, or duration, or some variation thereof.[163] But unlike noncompete agreements, the contract-based approach to the CFAA has no inherent limits on the enforceability of employment contracts. Without any limits on the employment contracts, criminal liability and federal jurisdiction could arise under any contractually defined circumstances with no regard for reasonableness or scope.[164] If the contract-based approach was employed in the criminal context of the CFAA, it would therefore run afoul of the traditionally legislative and court-sought balance of protections between employers and employees.

The CFAA has strong deterrence effects, given the possibility of felony charges and jail time resulting from its violation.[165] Many criticize the CFAA for creating punishment that exceeds the scope of what was intended by the statute, especially in the civil context.[166] This was a strong sentiment that followed the indictment of young college student, Aaron Swartz, in *United States v. Swartz*.[167] In this case, Swartz was indicted for downloading electronically archived materials from JSTOR (against JSTOR's user policy)

---

160 *See* John F. Hyland, *Drafting Practical & Enforceable Employment Agreements: The Process and the Substance*, 2014 WL 4785368 at *2 ("[I]ndividuals often have a reluctance to push for what they need in an agreement for fear that it will create the wrong impression.").

161 *See* Wayne N. Outten, *Negotiating Employment Agreements: An Employee's Lawyer's Perspective*, AM. BAR ASS'N, at 2 ("Invariably, the employment agreement will be drafted by the employer's counsel, typically using a model that the lawyer has used for other employers (if the lawyer is an outside counsel) or has used for other employees of the employer. In any event, that document is rarely balanced or sufficiently protective of the employee's interests.").

162 *See generally* 104 AM. JUR. 3D *Proof of Facts* 3d § 3 (2008); Paul S. Chan & John K. Rubiner, *Access Denied*, 28 L.A. LAW. 22, 25 (2006); Urban, *supra* note 123, at 1396.

163 *See generally* Chan & Rubiner, *supra* note 162, at 25.

164 Urban, *supra* note 123, at 1399 (arguing that if courts attempt to draw limits on contractual terms without clear guidance from Congress, confusion would result and employees would be exposed to too much risk).

165 *See* 18 U.S.C. § 1030(c) (2012).

166 *See* Curtiss, *supra* note 37, at 1843.

167 *See id.* at 1832 ("After Swartz's death, there was an outpouring of calls to reform the CFAA."); *see also id.* at 1833 (noting that legislators also tried to reform the CFAA with the introduction of a bill that "sought to resolve the circuit split, prevent a breach of contract from becoming a criminal violation, and bring greater proportionality to CFAA penalties").

through an MIT network, and charged under the CFAA for accessing the information "without authorization," despite having login credentials to JSTOR and access to the files for educational purposes.[168] Before the case was decided, Swartz committed suicide while facing the potential felony charges under the CFAA, and many blamed the drastic potential legal consequences for his untimely death.[169]

The impact of a felony conviction has more consequences for an individual than the mere label of a "felon." Felony convictions can result in the loss of the right to vote, future job limitations, the right to own a firearm, and an unwavering social stigma.[170] By allowing an employer to define "authorization" broadly and following the contract-based approach under the CFAA in a criminal suit, a court would not only be condemning an individual to the status of "felon," but the conviction could result in life-long impacts such as the ones just listed. Employing the code-based approach in a criminal setting makes it so that a mere breach of a broadly-worded contract cannot render an employee a felon, and maybe had Swartz not been facing a criminal conviction under the CFAA for a breach of contract in the form of a user agreement, the trajectory of his life would have been different.

Additionally, allowing employers to broadly define "authorization" through the contract-based approach could further open the door for criminal penalties beyond the scope of legislative intent. As previously explained in Part I, prior to the addition of the civil sections of the CFAA, the scienter requirement in the original CFAA was altered from "knowingly" to "intentionally" so as to avoid a criminal conviction for one who knowingly but inadvertently accesses a computer file or data without authorization.[171] This amendment points to a legislative desire to limit criminal penalties unless there was specific intent to access unauthorized information.[172] Employing the code-based approach in criminal cases would mean determining that a person, whether an employee or a third party, intentionally took action to bypass a code to gain access to information.[173] This approach would satisfy the scienter requirement and therefore supports the legislative intent of the criminal sections of the statute.

---

168 *See id.* at 1831.

169 *See id.* at 1832.

170 *See id.* at 1843.

171 S. REP. NO. 99-432, at 5–6 (1986); *see also* Hong, *supra* note 19, at 293 ("[U]nder the 1986 Act, even if a person does not intend to damage the computer system, liability will attach if the person intended to access the computer system.").

172 *See* S. REP. NO. 99-432, at 5–6; *see also* Gordon, *supra* note 48, at 370 ("The Senate report accompanying the original 1986 act . . . strongly supports a narrower code-based approach. . . . to make sure that any party prosecuted under the CFAA was deserving of criminal liability." (footnote omitted)).

173 *See* Patterson, *supra* note 122, at 505.

B. *Legislative Intent and History*

The legislative history of the statute further supports the notion that "authorization" should be defined by a code-based approach in the criminal context. At the outset of the CFAA's formation, Congress intended to create a statute that made it a felony to access a governmental computer to gain information related to United States foreign relations.[174] The statute was intended first and foremost to target external hackers in the name of protecting national security.[175] The original statute only included the phrase "without authorization," and it was not until later amendments that Congress added "or exceeds authorized access."[176] The original intent of the statute seemingly supports the code-based approach because the statute was created to address concerns of outside hackers breaking into government computers to access information to distribute to other foreign states. It did not address instances in which private employees breached a private employment contract, because such instances would not affect government computers, nor national security.

Furthermore Congress sought to ensure that federal employees would not be prosecuted for acts of computer access of computers they were meant to have access to, because that "did not rise to the level of criminal conduct."[177] This is further exemplified by the fact that the original statute did not include a section providing for civil liability.[178] The code-based approach is therefore supported in the criminal context because it falls in line with the original 1984 version of the statute, which included only the criminal framework.

It wasn't until 1986 that Congress broadened the statute to include the phrase "or exceeds authorized access" to accompany "without authorization," and then the 1990s that Congress changed federal computers to all "protected computers" affecting commerce and added a private cause of action to allow for a civil remedy for employers.[179] Much of the reasoning behind these amendments stemmed from concerns that the federal government's jurisdiction would have extended too broadly over computer related crimes that would be better handled by the private sector, and that jail terms did not adequately provide redress to private employers.[180] Additionally, the Senate Committee Report described the addition of "exceeds authorized access" in terms of trespassing into a computer system of files, explaining that

---

174 Baker, *supra* note 11, at 64.

175 *Id.*

176 *See* Counterfeit Access Device and Computer Fraud and Abuse Act § 2102(a); Baker, *supra* note 11, at 64.

177 Griffith, *supra* note 17, at 477.

178 *See* Baker, *supra* note 11, at 71.

179 *See supra* Part I.

180 *See* S. REP. NO. 99-432, at 4 (1986); Baker, *supra* note 11, at 71.

the goal was not to hold liable those who "inadvertently 'stumble into' someone else's computer file or computer data."[181]

In broadening the statute, Congress sought not to change its meaning, but rather to extend its jurisdictional scope to address these concerns.[182] Because the intent of the statute seems to support a code-based approach, the legislative history further demonstrates that the approach to defining "without authorization" was not intended to take a different form than the original intent. Therefore, the criminal sections of the statute as they have existed throughout history and as they exist today do not support a contract-based approach in defining "without authorization."

C. *Constitutional Concerns and Rules of Statutory Interpretation*

Commentators have expressed concerns that the contract-based approach to defining authorization would cause some statutory interpretation issues, such as violating the "void for vagueness doctrine" rooted in the Due Process Clause.[183] Employing the contract-based approach in only cases brought under the CFAA in a civil suit, and not a criminal suit, would also solve the violation of the "void for vagueness doctrine" the CFAA proposes. The principle underlying the void for vagueness doctrine is that "no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed."[184] In applying the void for vagueness doctrine, courts have implemented a fair notice test to examine whether a law is "so vague and standard-less that it leaves the public uncertain as to the conduct prohibits."[185] Courts and legal scholars have criticized the CFAA for violating due process because it "fails to provide a person of ordinary intelligence fair notice of what is prohibited," and as such, is a criminal statute that should be found void for vagueness.[186]

The CFAA does not give "fair notice" of what "without authorization" means, which is evidenced by the current circuit split.[187] If a law's language is vague to lawyers and judges, then surely a reasonable person could not be

---

181 *See* S. REP. NO. 99-432, at 6.

182 *See id.* at 5–6.

183 *See, e.g.*, Mikulic, *supra* note 110, at 190.

184 United States v. Harriss, 347 U.S. 612, 617 (1954); Mikulic, *supra* note 110, at 190 ("It makes no sense under any theory of punishment to chastise a person who violates a statute that gives no fair explanation of what behavior is criminal.").

185 *See* Kerr, *supra* note 35, at 1573 (arguing that the fair-notice standard implies that the public knows the legal precedent for a statute's terms) (quoting Giaccio v. Pennsylvania, 382 U.S. 399, 402 (1966)).

186 *See, e.g.*, *id.* at 1577 ("[C]ourts must reject interpretations of unauthorized access that criminalize routine Internet use or that punish common use of computers."); Mikulic, *supra* note 110, at 189 (quoting United States v. Williams, 553 U.S. 285, 305 (2008)).

187 *See* Mikulic, *supra* note 110, at 194.

expected to define "without authorization."[188] Critics of the CFAA have argued that not only is the plain meaning of the statute vague, but also it does not directly inform a reader "that a violation of a contract will result in criminal penalties."[189]

Employing the code-based approach in criminal cases brought under the CFAA would not violate the void for vagueness doctrine because the approach narrowly limits culpability. If a user circumvents a code or password, the user is seemingly aware that he or she is doing so, and in so doing is acting contrary to the statute. Employing the code-based approach in criminal cases brought under the CFAA does not result in a "fair notice" problem.[190] A user would have fair notice by confronting and overcoming a code-based limitation in order to use the system and obtain or disseminate information.[191] In the context of a federal criminal statute, the law should require clarity, and the code-based restrictions would alert a user that he is acting contrary to the law, whereas the contract-based restriction may not provide such clear notice, especially in instances where a lengthy and likely unread "terms of service" (such as the one Google used to prohibit minors from using its services up to 2012) is breached.[192]

The contract-based approach would not remedy the unconstitutionality of the CFAA in the sections where it imposes criminal penalties through its vague language because ordinary men and women presume a contract breach does not result in criminal prosecution.[193] However, ordinary men and women could expect a contract breach to result in civil liability under not only state law, but also under the CFAA, where for instance, an employee is aware of what conduct is or is not authorized.[194] Where an employer has defined "authorization" within the scope of a contract, presumably its employees have read the contract and have knowledge of what that authorization includes or does not include.

Take, for example, the case of *United States v. Drew*,[195] where Lori Drew was prosecuted under the CFAA for exceeding the access of the MySpace terms of service, after she created a false account and personified a teenage boy in an effort to learn information about her neighbor.[196] An interpretation of "unauthorized access" that includes all terms-of-service violations would render the statute unconstitutional for vagueness, because

---

188 *See id.*

189 *See id.* at 194–95.

190 Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1475–76 (2016).

191 *Id.*

192 *Id.*

193 Mikulic, *supra* note 110, at 194–95; *see also* United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012).

194 Mikulic, *supra* note 110, at 195 & n.164.

195 259 F.R.D. 449 (C.D. Cal. 2009).

196 *See id.* at 452.

terms of service are broad and lengthy, few people actually read them, and people often do not treat them as if they are entering into a contract.[197] The court in *Drew* found that it was unclear whether an intentional breach of a website's terms of service would comprise intent to access a site without authorization or in excess of authorization, warning that "if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution."[198] A contract, such as the terms of service of a social media platform, does not provide fair notice and the void for vagueness doctrine would still apply. Thus, the contract-based approach does not provide for a remedy in criminal actions under the CFAA because it does not satisfy the void for vagueness doctrine in cases where terms of service are involved.

Another statutory interpretation criticism of the CFAA is that it imposes criminal penalties on an individual by way of an impermissible private delegation of lawmaking power, which is in violation of the private nondelegation principle.[199] Justice Samuel Alito once acknowledged:

> When citizens cannot readily identify the source of legislation or regulation that affects their lives, Government officials can wield power without owning up to the consequences. One way the Government can regulate without accountability is by passing off a Government operation as an independent private concern.[200]

While the Supreme Court uses the term "delegation" in a variety of contexts, the concept is applicable to the CFAA in the form of the private nondelegation principle. This doctrine, based on separation of powers principles, supports the premise that Congress may not constitutionally delegate its legislative power to a private party.[201] Critics of the contract-based approach argue that through its application, the private nondelegation doctrine would be violated by allowing the writers of a contract or terms of service the ability to define crimes, a job that is reserved to Congress through the Constitution.[202] However, by only allowing the contract-based approach to apply in the civil context, employers would only be defining when they can personally recover through damages caused to their own protected computers. Thus, the writers of the contracts would not be able to define "without authorization"

---

197 *See* Kerr, *supra* note 35, at 1582 (arguing that most internet users violate terms of service regularly, scrolling through them assumingly without impact).

198 *Drew*, 259 F.R.D. at 467.

199 *See* Mikulic, *supra* note 110, at 196 ("Congress gave the power to delineate a criminal sanction to private parties.").

200 Dep't of Transp. v. Ass'n of Am. R.Rs., 135 S. Ct. 1225, 1234 (2015) (Alito, J., concurring).

201 *See* Loving v. United States, 517 U.S. 748, 758 (1996); Touby v. United States, 500 U.S. 160, 165 (1991).

202 Mikulic, *supra* note 110, at 198; James M. Rice, *The Private Nondelegation Doctrine: Preventing the Delegation of Regulatory Authority to Private Parties and International Organizations*, CALIF. L. REV., 539, 547 (2017).

in the criminal context of the statutes, thereby avoiding a violation of the private nondelegation doctrine.

The ramifications of delegating the power to define a criminal statute to an employer under the CFAA could be considerably detrimental. Such ramifications are easily highlighted in the Eleventh Circuit's criminal conviction of the defendant in *United States v. Rodriguez*. When the defendant in that case obtained personal information for his own personal use by accessing a database of his employer's, he was handed a criminal conviction because the employment policy in place allowed obtaining personal information in the database only for business purposes.[203] As most employment policies universally prohibit accessing information for any use other than business purposes, it is difficult to fathom that an employee could be facing criminal charges for using a computer for personal reasons during the work-day, especially given the prevalence of computers and the frequent diversions from purely work-related activities employees engage in. In *Rodriguez*, the court allowed the defendant's employer to define "authorization," violating the private nondelegation principle.[204] As a result, not only was the defendant criminally convicted, but also the court ultimately ended up concluding that his one-year jail sentence was a reasonable punishment under the terms of the CFAA.[205] The consequences of allowing an employer to define access under criminal charges of the CFAA could therefore leave an employee subject to incarceration for any small violation of company policy.

The jurisdictions that have defined "authorization" in cases brought under the CFAA and ultimately employed the code-based approach rationale in criminal suits found that the rule of lenity supported their interpretation.[206] In *Valle*, where the Second Circuit was faced with a criminal case involving a police officer accessing a database to obtain personal information about a woman to relay to other members of an online sex fetish community, the court did not convict the police officer under the CFAA.[207] In this case, the defendant had the login credentials and the authorization through his employment to access the database, but department policy forbade the use of the database for searches unrelated to job activity.[208] The court found that the plain meaning of the statute was ambiguous, and further went on to conclude that the legislative history also rendered support for both the contract-based approach and the code-based approach in defining authorization under the statute.[209] The court concluded: "Where, as here, ordinary tools of legislative

---

203 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

204 *See id.* at 1263–64.

205 *See id.* at 1264–65.

206 *See, e.g.*, United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012).

207 *Valle*, 807 F.3d at 528.

208 *Id.* at 512–513.

209 *Id.* at 526.

construction fail to establish that the Government's position is unambiguously correct, we are required by the rule of lenity to adopt the interpretation that favors the defendant."[210]

Where a statute imposing criminal liability is subject to more than one reasonable interpretation, courts use the common law rule of lenity to construe any statutory ambiguity in favor of the criminal defendant.[211] Employing this doctrine, the court in *Valle* concluded that the best solution is to construe criminal statutes narrowly, making the code-based approach to defining without authorization the most appropriate interpretation in the criminal context.[212] As the Second Circuit's decision demonstrates, the code-based approach is more properly employed in the criminal setting because the rule of lenity in criminal suits supports it.[213] However, the rule of lenity is not applicable in cases brought under the CFAA in the civil context because such instances would not give rise to the "criminaliz[ation] . . . of millions of ordinary computer users," as was the most significant concern expressed in the Second Circuit's holding in *Valle*.[214]

The court in *Valle* further concluded that their decision was supported by public policy, fearing that the public obviously would be surprised to find that any breach of company policy or contract might leave them susceptible to criminal punishment.[215] By considering the rule of lenity and public policy together, the court justified its finding in favor of the defendant. Despite the offensive facts surrounding the defendant's blatant disregard for his department policy and the dangerous use of private personal information, the decision of the court to employ the narrow code-based approach in defining "authorization" was the least offensive reading of the ambiguous phrase of the statute where significant criminal penalties were in play.

To summarize the above points, courts should seek to employ the contract-based approach where actions are brought under the civil section of the CFAA and the code-based approach for criminal actions brought by the federal government against an individual. The contract-based approach is supported by natural law and the freedom to contract, and as such it follows that, where there is a willingness to bind oneself, civil liability for breach of a binding promise is an appropriate result. However, the contract-based approach should not be employed in criminal cases under the CFAA, specifically in the employment context, because digressions from routine job duties could result in criminal liability. Letting contracts that criminalize such digressions run unchecked violates the balance between employees and employers that the courts seek to maintain. Furthermore, the CFAA has the capacity to label an employee a felon, with all the limitations that come with

---

210 *Id.*

211 Zachary Price, *The Rule of Lenity as a Rule of Structure*, 72 FORDHAM L. REV. 885, 885 (2004).

212 *Valle*, 807 F.3d at 528.

213 *Id.*

214 *Id.* at 527.

215 *Id.* at 528.

the label, under its criminal sections for mere terms of service or user agreements violations under the contract-based approach. In order to avoid significant consequences for minor breaches, the contract-based approach must not be employed in such instances.

The legislative history of the CFAA further supports that the original statute was created for criminal purposes, as evidenced by the amendments to the scienter element of the statute. Employing the code-based approach in the criminal setting supports legislative intent and preserves the original meaning of the statute, while employing the contract-based approach to only the newer civil sections of the CFAA does not offend the original purpose of the statute.

Lastly, employing the code-based approach in lawsuits brought under the criminal sections of the CFAA satisfies the common principles employed only in criminal suits: the void for vagueness doctrine, the private nondelegation doctrine, and the rule of lenity. Whereas the contract-based approach fails to account for these principles in the criminal setting due to its broad interpretation of an ambiguous phrase, the code-based approach's narrower reading satisfies these principles and further promotes public policy and constitutional values. As such, the courts should seek to employ a shifting interpretation to "unauthorized access" under the CFAA, depending on whether the lawsuit is brought in the criminal or civil setting.

CONCLUSION

The Computer Fraud and Abuse Act was originally created when computers were first beginning to surface and were not readily accessible to every individual. The statute was intended to prevent hackers from fraudulently accessing federal computers and using hacked information to dispel trade secrets. Over time, Congress made several amendments to the statute, which resulted in a much broader function of the CFAA. While the legislative amendments were intended to cover the spread of technology and the result of computers being readily accessible, Congress did not remedy the language of the statute to clearly delineate the purpose of the phrase "without authorization." As a result, some courts have translated the phrase broadly, extending criminal and civil liability in situations where individuals accessed a protected computer in a way that was the intended purpose of the access. Other courts have interpreted the phrase narrowly, finding that criminal and civil liability cannot extend where any type of access has been warranted. Without a Supreme Court precedent or amendment to guide the interpretations of the lower courts, the results have been inconsistent and jurisdictionally dependent.

The courts and legal community have weighed in on which approach is more favored, with the more recent and supported trend favoring the narrow approach. As a result, two significant theories to defining "without authorization" have been the main subject of attention: the code-based approach and

the contract-based approach. While both of these approaches have considerable merit, criticism has extended to both for various reasons involving overreaching unconstitutional consequences. Therefore, courts should employ a shifting standard.

The shifting standard would seek to employ the contract-based approach under the CFAA in cases arising under civil suits in the employment or website terms of service violations context, as doing so would not yield unconstitutional results nor violate the language of the CFAA. However, the contract-based approach is simply too broad to be applied in the criminal context of the CFAA, and thus courts should seek to employ the code-based approach in such instances. The code-based approach—the narrowest approach—should be employed in the criminal context so as not to impose criminal liability resulting in felonies and imprisonment in instances where "without authorization" has not been defined by the legislative body. This solution of employing a shifting approach would not only uphold the purpose of the CFAA in protecting information stored electronically and relationships between providers and users or employers and employees, but also would not unconstitutionally impose criminal liability on those individuals who merely engage in electronic access readily available in this modern technological era.