VOLUME 47, NO. 3 JUNE 2014

CREIGHTON LAW REVIEW

THE COMPUTER FRAUD AND ABUSE ACT SHOULD NOT APPLY TO THE MISUSE OF INFORMATION ACCESSED WITH PERMISSION

DAVID J. SCHMITT

CREIGHTON UNIVERSITY SCHOOL OF LAW

THE COMPUTER FRAUD AND ABUSE ACT SHOULD NOT APPLY TO THE MISUSE OF INFORMATION ACCESSED WITH PERMISSION

DAVID J. SCHMITT†

I. INTRODUCTION

The Computer Fraud and Abuse Act[1] ("CFAA") makes it unlawful when an individual improperly accesses a protected computer "without authorization" or "exceeds authorized access".[2] The CFAA has been the subject of conflicting and contrary judicial interpretations as to whether it is limited to violations of access restrictions, or whether it applies when an individual misuses computer information that was accessed with permission.[3]

The dispute whether the CFAA applies to misuse has been caused by ambiguous statutory text, which creates uncertainty as to the intent of Congress. The phrase "exceeds authorized access" is defined in 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 to so obtain or alter."[4] The text can be read in two ways. First, it could refer to a user who has permission to access certain files or information on a computer, but instead accesses unauthorized files or information.[5] Second, it could refer to a user who has permission to access information on a computer, but who misuses the information that was accessed with permission.[6]

Despite clear legislative history that the CFAA was intended as an anti-hacking statute, the ambiguous statutory text regarding "exceeds authorized access" has led to a split in the federal courts as to whether the CFAA applies to misuse.[7] Currently the determination of whether the misuse of information accessed with permission violates the CFAA is essentially dependent on the jurisdiction making the de-

† Partner, Lamson, Dugan and Murray, LLP, Omaha, Nebraska. University of Nebraska College of Law (LL.M. Space, Cyber, and Telecommunications Law, 2013); Creighton University School of Law (J.D. *cum laude*, 1989); University of Iowa (B.B.A., 1985).

1. 18 U.S.C. § 1030 (2011).
2. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(1) (2011).
3. *See infra* notes 68-208 and accompanying text.
4. 18 U.S.C. § 1030(e)(6).
5. United States v. Nosal, 676 F.3d 854, 856-57 (9th Cir. 2012) (en banc).
6. *Nosal*, 676 F.3d at 857.
7. *See infra* notes 164-208 and accompanying text.

cision. The same type of conduct has resulted in vastly different consequences depending on which court addressed the CFAA claim.[8] A violation of the CFAA can result in criminal sanctions,[9] and civil liability,[10] so the manner in which it is interpreted has significant implications for those users faced with claims of violations.

Four United States Circuit Courts of Appeals have given a broad interpretation to the scope of the CFAA by finding it applies to the misuse of information the user had permission to access.[11] The United States Courts of Appeals for the First Circuit, Fifth Circuit, Seventh Circuit, and Eleventh Circuit have all adopted this broad approach.[12]

Two Courts of Appeals have interpreted the CFAA narrowly.[13] The United States Courts of Appeals for the Fourth Circuit and Ninth Circuit have held the CFAA is limited to violations of access restrictions, and that its scope does not extend to the misuse of computer information that was accessed with permission.[14] Those courts have placed greater emphasis on the legislative history, the legal doctrine of lenity which requires ambiguous criminal statutes be strictly construed, and policy considerations, such as an unwillingness to transform a large number of individuals into criminals for relatively innocuous violations of computer use policies.

Section II of this Article examines statutory provisions in the CFAA that have been frequently cited in actions alleging misuse of information.[15] Section III reviews the legislative history of the CFAA, which demonstrates it was intended as an anti-hacking statute and therefore arguably was not intended to prohibit the misuse of information accessed with permission.[16]

Section IV examines the split in the United States Courts of Appeals whether the CFAA is limited to violations of access restrictions, or whether it applies when information accessed with permission is misused.[17] It also examines conflicting district court decisions within

---

8. *See infra* notes 65-164 and accompanying text.
9. 18 U.S.C. § 1030(c).
10. 18 U.S.C. § 1030(g).
11. *See infra* notes 68-112 and accompanying text.
12. *See, e.g.,* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).
13. *See infra* notes 145-208 and accompanying text.
14. *See, e.g., Nosal*, 676 F.3d at 854; *WEC Carolina Energy Solutions, L.L.C. v. Miller*, 687 F.3d 199 (4th Cir. 2012).
15. *See infra* notes 29-46 and accompanying text.
16. *See infra* notes 47-64 and accompanying text.
17. *See infra* notes 65-162 and accompanying text.

the Second Circuit, as that court has not specifically decided the issue.[18]

Section V discusses legislation that has recently been proposed to resolve the ambiguity in the CFAA.[19] The proposed legislation strikes the ambiguous definition "exceeds authorized access" from the CFAA and clarifies that the CFAA does not apply to misuse.[20]

Section VI analyzes applicable legal doctrines to interpret the CFAA.[21] The doctrine of lenity requires that ambiguous criminal statutes be interpreted narrowly, and therefore the CFAA should be interpreted narrowly and not apply when information accessed with permission is misused.[22]

Section VII discusses policy considerations and the practical consequences against broadly interpreting the CFAA to apply to misuse.[23] Numerous users who engage in essentially innocuous conduct by violating computer use policies could be subject to criminal liability. A broad interpretation will also place too much discretion in the hands of prosecutors which could lead to inconsistent or discriminatory enforcement, uncertainty, and confusion as to what conduct is criminal under federal law.[24]

Section VIII recognizes the need for immediate resolution of the dispute.[25] The CFAA has significant criminal sanctions, so the dispute about whether the CFAA applies to misuse must be resolved to provide appropriate notice to the public regarding what conduct is criminal under federal law.[26] It can also impose civil liability for damage and loss.[27] Congress should pass legislation clarifying that the CFAA does not apply to misuse. Absent further action by Congress, the United States Supreme Court should grant review and resolve the judicial split in the circuit courts. The Supreme Court should follow the trend created by the recent federal court cases that the CFAA does not apply to misuse, which place greater emphasis on the legislative

18. *See infra* notes 163-208 and accompanying text.

19. *See infra* notes 209-221 and accompanying text.

20. H.R. 2454, 113th Cong. § 2 (2013); S. 1196, 113th Cong. § 2 (2013).

21. *See infra* notes 208-221 and accompanying text.

22. *See infra* notes 222-257 and accompanying text.

23. *See infra* notes 222-263 and accompanying text.

24. *See infra* notes 258-263 and accompanying text.

25. *See infra* notes 258-263 and accompanying text.

26. *See* 18 U.S.C. § 1030(c) (stating offenses may be punished by fine and a term of imprisonment ranging from five to twenty years, depending on the severity of the crime committed).

27. 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief . . .").

history, the legal doctrine of lenity, and policy considerations.[28] An immediate resolution is necessary, particularly given the growing use of computers in society and the workplace.

II. THE CFAA APPLIES WHEN A USER ACCESSES A PROTECTED COMPUTER "WITHOUT AUTHORIZATION" OR "EXCEEDS AUTHORIZED ACCESS"

The CFAA prohibits certain computer related conduct by a user who improperly accesses a protected computer "without authorization" or "exceeds authorized access."[29] The statutory provisions have been subject to significant debate and contrary judicial interpretations as to what activity is prohibited by the CFAA. Ambiguous statutory text has created uncertainty whether Congress intended it apply to the misuse of computer information that was accessed with permission. That uncertainty has led to a judicial split in the United States Courts of Appeals.[30]

The CFAA prohibits improperly obtaining information from "any protected computer".[31] A "protected computer" is defined as follows:

> [T]he term "protected computer" means a computer –
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
> (B) which is *used in or affecting interstate or foreign commerce or communication*, including a computer located outside of the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States . . .[32]

As noted, a "protected computer" includes any computer "used in or affecting interstate or foreign commerce or communication."[33] Under this broad definition, the CFAA has been interpreted to apply to any computer connected to the Internet.

---

28. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) (discussing that some commentators have argued that the failure by Congress requires that the courts limit the CFAA under the constitutional void-for-vagueness doctrine to a narrow interpretation of prohibiting access).

29. 18 U.S.C. § 1030(a)(1)-(a)(7).

30. *See infra* notes 65-208 and accompanying text.

31. 18 U.S.C. § 1030(a)(2)(C).

32. 18 U.S.C. § 1030(e)(2) (italics added).

33. *Id.*

In *United States v. Trotter*,[34] the court stated, "Congress clearly has the power to regulate the [I]nternet, as it does other instrumentalities and channels of interstate commerce."[35] The "Internet is an international network of interconnected computers," and "[a]s both the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality and channel of interstate commerce.'"[36] As such, the CFAA was enacted within Congress's power under the Commerce Clause and is constitutional.[37] Accordingly, the CFAA effectively applies to any computer connected to the Internet.[38]

The CFAA as originally enacted imposed criminal penalties. In 1994, Congress amended the CFAA to provide civil remedies.[39] The CFAA allows persons who suffer damage and loss by violations of the statute to recover compensatory damages and obtain injunctive relief, provided certain conditions are satisfied:

> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses[40] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). . . .[41]

There are several provisions in the CFAA frequently cited in actions alleging misuse of information. The provisions 18 U.S.C. §§ 1030(a)(2), (a)(4), and (a)(5) in particular have been relied on, although they have been subject to contrary judicial interpretations as to whether the CFAA applies when information that was accessed with permission is misused.[42]

---

34. 478 F.3d 918 (8th Cir. 2007).

35. United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (quoting United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004)).

36. *Trotter*, 478 F.3d at 921 (quoting Reno v. ACLU, 521 U.S. 844, 849 (1997); United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006)).

37. *Trotter*, at 921 (adopting the Seventh Circuit's analysis in United States v. Mitra, 405 F.3d 492 (7th Cir. 2005)).

38. *See* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (the court reviewed the CFAA's definition of a "protected computer" as any computer "affected by or involved in interstate commerce" and concluded that "effectively all computers with Internet access" are subject to the CFAA). *Id.* at 859.

39. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 1796 (1994).

40. *See* 18 U.S.C. § 1030(g). The word "subclauses" is in the original text and should arguably be "subclause".

41. 18 U.S.C. § 1030(g). One of the factors in a civil action is the requirement that an aggregate loss of at least $5,000.00 be sustained in a one-year period. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

42. *See infra* notes 43-64 and accompanying text.

Section 1030(a)(2) prohibits obtaining information without authorization, or by exceeding authorized access, from financial institutions, the United States Government, or any protected computer:

> (2) [Whoever] intentionally accesses a computer *without authorization or exceeds authorized access*, and thereby obtains –
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer;
>
> . . . shall be punished as provided in subsection (c) of this section.[43]

Section 1030(a)(4) prohibits engaging in fraudulent activity by accessing a protected computer without authorization, or exceeding authorized access, to obtain anything in value in excess of $5,000:

> (4) [Whoever] knowingly and with intent to defraud, accesses a protected computer *without authorization, or exceeds authorized access*, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
>
> . . . shall be punished as provided in subsection (c) of this section.[44]

Section 1030(a)(5) prohibits causing damage to a protected computer and provides that whoever:

> (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage *without authorization*, to a protected computer;
>
> (B) intentionally accesses a protected computer *without authorization*, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer *without authorization*, and as a result of such conduct, causes damage and loss. [;]
>
> . . . shall be punished as provided in subsection (c) of this section.[45]

---

43. 18 U.S.C. § 1030(a)(2) (emphasis added).
44. 18 U.S.C. § 1030(a)(4) (emphasis added).
45. 18 U.S.C. § 1030(a)(5) (emphasis added).

The confusion as to whether Congress intended the CFAA to prohibit the misuse of information accessed with permission has been caused by the ambiguous phrase "exceeds authorized access." The CFAA does not define the term "access." However, it defines "exceeds authorized access" as follows:

> [T]he term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;[46]

The uncertainty caused by this ambiguous definition has resulted in the CFAA being interpreted in contrary manners, thereby leading to vastly different results for the same type of conduct. A review of the legislative history is accordingly required to determine whether it provides insight as to Congress's intent.

III. LEGISLATIVE HISTORY INDICATES THE CFAA WAS INTENDED AS AN ANTI-HACKING STATUTE

The legislative history demonstrates the CFAA was enacted as an anti-hacking statute. The CFAA originated in 1984 when Congress passed legislation called the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.[47] The statute was enacted to make it a crime to access classified information in a computer without authorization, accessing financial records at financial institutions, or trespassing into government computers.[48] The prohibitions in the 1984 Act applied to whoever "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information . . . ."[49]

The legislative history for the 1984 Act indicates the purpose was to prevent unauthorized access of computers, or computer hacking.[50] The House Report states "Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a

46. 18 U.S.C. § 1030(e)(6).

47. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984) [hereinafter *1984 Act*].

48. 1984 Act, Pub. L. No. 98-4731984 Act § 2102(a), 98 Stat. 1837, 2190-92 (1984). *See also* S. REP. NO. 99-432, at *3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 (discussing the purpose of the 1984 Act).

49. Pub. L. No. 98-473, 98 Stat. 1837, Sec. 2102(a) (Oct. 12, 1984).

50. H.R. REP. 98-894, at *20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706.

gun) in committing the offense."[51] Accordingly, the foregoing history is relatively unambiguous in expressing the purpose the 1984 Act was to prevent improper access. The legislative history continues as follows:

> [I]t prohibits access to a computer to obtain the described data when the perpetrator knows that the access is not authorized or that it is not within the scope of a previous authorization. The provision does not attempt to reach the scope of information incidentally obtained or the use of information that has been obtained legitimately. The provision therefore does not extend to any type or form of computer access that is for a legitimate business purpose. Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected. The provision does not extend to normal and customary business procedures and information usage and so these legitimate practices will not be interrupted or otherwise affected. It imposes criminal sanctions upon "hackers" and other criminals who access computers without authorization.[52]

This history from the House Committee report refers to the concept of "hackers" and is focused at prohibiting improper access to computers.[53] It should be recognized the report states the 1984 Act does not extend to the use of information accessed for legitimate business purposes, so an argument could be made that the statement by the Committee meant the statute was intended to apply to misuse.[54] However, that statement must be viewed in the context of the entire House Committee report, and the report as a whole expresses the intent that the 1984 Act was aimed at hacking.

The CFAA was amended in 1986 to provide additional penalties for fraud and related activity.[55] Congress adopted the phrase "exceeds authorized access" which currently appears in the CFAA. The phrase replaced the language from the 1984 Act "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[56]

The Senate Committee report for the 1986 amendment provides insight as to the intended meaning of the phrase "exceeds authorized access." The Senate Committee discussed the phrase in the context of 18 U.S.C. § 1030(a)(3), which prohibits access to government com-

---

51. *Id.*
52. *Id.* at *21.
53. *Id.*
54. *Id.*
55. S. REP. 99-432, at *1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.
56. *Id.* at *9.

puters "without authorization."[57] It explained the phrase "exceeds authorized access" was purposefully excluded from Section 1030(a)(3) in order to limit that provision to cases aimed at "outsiders" who lacked authorization to access federal computers.[58] Significantly, the Senate Committee stated if the phrase "exceeds authorized access" had been included, it would have applied Section 1030(a)(3) to users who had permission to use government computers, but who viewed data in the computer they were not authorized to access:

> [T]he Committee has declined to criminalize acts in which the offending employee merely "*exceeds authorized access*" to computers in his own department. . . . It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. . . . The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted under this subsection. That danger will be prevented by not including "*exceeds authorized access*" as part of this subsection's offense.[59]

Thus, this legislative history provides insight as to Congress's intended meaning of the phrase "exceeds authorized access." The phrase "exceeds authorized access" addresses improper access to information by individuals who have permission to use a computer, but who view additional information they did not have permission to access, not misuse.[60]

This conclusion is further supported by the Senate Committee statement that it "distinguished between acts of unauthorized access that occur within a department and those that involve trespasses into computers belonging to another department. The former are not covered by subsection (a)(3); the latter are."[61] The Senate Committee envisioned the scenario where an employee was not in any way authorized to use computers in a different government department.[62] It concluded that an "employee who uses his department's computer and, without authorization, forages into data belonging to another de-

57. *Id.* at *8.
58. *Id.* at *10.
59. *Id.* at *7 (emphasis added).
60. *Id.*
61. *Id.*
62. *Id.* at *7-8.

partment, is engaged in conduct directly analogous to an 'outsider' tampering with Government computers."[63]

Accordingly, the legislative history demonstrates Congress intended the CFAA as an anti-hacking statute. It is particularly noteworthy the legislative history from the time the ambiguous phrase "exceeds authorized access" was adopted reflects the provision was intended to address improper access to information by insiders who had permission to use a computer, not misuse. The CFAA was aimed at "outside hackers" who improperly access protected computers, and "inside hackers" who have permission to use protected computers but obtain information beyond the permission that had been granted.[64] If the purpose of the CFAA was to prohibit computer hacking, Congress arguably did not intend it to apply to misuse, particularly given the lack of a clear pronouncement in the legislative history for the same.

IV. FEDERAL COURTS ARE SPLIT ON WHETHER THE CFAA APPLIES WHEN AN INDIVIDUAL MISUSES COMPUTER INFORMATION THAT WAS ACCESSED WITH PERMISSION

Despite seemingly clear legislative history that Congress intended the CFAA as an anti-hacking statute, courts have had difficulty interpreting the CFAA and deciding whether it was intended to apply to individuals who have permission to access computer information but misuse that information. The federal courts are split into two broad groups regarding that issue.

One group has interpreted the CFAA narrowly by limiting it to individuals who violate computer access restrictions.[65] Generally that group has interpreted the provision prohibiting access to a computer "without authorization" to apply to "outsider hackers," and the provision "exceeds authorized access" to apply to "inside hackers." An inside hacker has permission to access limited information on a computer, but obtains other information on the computer the user did not have permission to access.

The other group has interpreted the CFAA broadly beyond merely prohibiting violations of access restrictions. That group has interpreted "exceeds authorized access" to apply to users who have permis-

63. *Id.* at *8.

64. *Id.*

65. *See, e.g.,* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc); WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ. 9505 (ALC)(DCF), 2013 WL 410873, at *1 (S.D.N.Y. Jan. 30, 2013); JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514 (S.D.N.Y. 2013).

sion to access computer information, but who "misuse" the information obtained with permission.[66]

This section discusses the split in the United States Circuit Courts of Appeals. Four federal circuit courts have interpreted the CFAA broadly: First Circuit, Fifth Circuit, Seventh Circuit, and Eleventh Circuit. Two federal circuit courts have interpreted the CFAA narrowly: Fourth Circuit and Ninth Circuit. This section also discusses conflicting decisions by district courts within the Second Circuit, as the United States Court of Appeals for the Second Circuit has not specifically decided the issue.[67] The decisions by the federal courts have resulted in inconsistent and contrary holdings leading to confusion and uncertainty whether the CFAA prohibits the misuse of information that was accessed with permission.

A. Broad Interpretations by Circuit Courts That the CFAA Applies to Misuse

1. First Circuit

The First Circuit interpreted the CFAA broadly under contract principles to apply to the misuse of computer information. In *EF Cultural Travel BV v. Explorica, Inc.*,[68] the plaintiff was engaged in the business of providing travel services.[69] It brought an action under 18 U.S.C. § 1030(a)(4) against several former employees who left to work for a different company and compete in the same market.[70] Plaintiffs' former vice president of information strategy obtained proprietary information during his employment. A confidentiality agreement required that any proprietary information be maintained in strict confidence and not disclosed to any third party.[71] However, he furnished the information to a computer consultant to create a computer program called a "scraper." The scraper used the plaintiffs' proprietary codes to send more than 30,000 inquiries to the plaintiffs' website and record large volumes of information which could then be used to undercut the plaintiffs' prices.[72]

---

66. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); United States v. John, 597 F.3d 263, 272-73 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263-64 (11th Cir. 2010); Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007); Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *6 (S.D.N.Y. May 18, 2010).

67. *See infra* notes 68-208.

68. 274 F.3d 577 (1st Cir. 2001).

69. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

70. *EF Cultural*, 274 F.3d at 579-80.

71. *Id.* at 582.

72. *Id.* at 579, 582.

The court granted the plaintiff injunctive relief finding the CFAA prohibited such conduct. It relied on the CFAA definition "exceeds authorized access" stating the confidentiality agreement prohibited the disclosure of information contrary to the plaintiffs' interests.[73] Therefore, the transfer of the plaintiffs' proprietary information furnished a sufficient basis for a claim under the CFAA.[74] The court also commented that whatever authorization existed to navigate the plaintiffs' website, the defendants' use of proprietary information to create the scraper program and obtain large volumes of information "exceeded that authorization."[75]

Thus, the First Circuit interpreted the CFAA broadly to apply to misuse. It relied on contract principles to hold the CFAA applies when an employee breaches a confidentiality agreement by misusing information the employee obtained with permission.

2. *Fifth Circuit*

The Fifth Circuit also interpreted the CFAA broadly by holding it applies to violations of computer use policies. In *United States v. John,*[76] the defendant was an account manager at Citigroup and had access to an internal computer system and customer account information.[77] She accessed information from customer accounts and provided it to others to incur fraudulent charges.[78] The defendant was charged, *inter alia*, with exceeding authorized access to a protected computer in violation of 18 U.S.C. § 1030(a)(2). The court stated the issue of whether the CFAA applied depended on the proper interpretation of "exceeds authorized access."[79]

The defendant argued the CFAA did not apply as she was authorized to use Citigroup's computers and view and print customer account information in the course of her official duties.[80] She reasoned the "statute does not prohibit unlawful *use* of material that she was authorized to access through authorized use of a computer. The statute only prohibits using authorized access to obtain information that she is not entitled to obtain or alter information that she is not entitled to alter."[81] The court rejected that argument stating:

---

73. *Id.* at 583.
74. *Id.* at 583, n.16.
75. *Id.* at 583.
76. 597 F.3d 263 (5th Cir. 2010).
77. United States v. John, 597 F.3d 263, 269 (5th Cir. 2010).
78. *John*, 597 F.3d at 269.
79. *Id.* at 270.
80. *Id.* at 271.
81. *Id.*

> The statute at issue prohibits both accessing a computer "without authorization" and "exceed[ing] authorized access" to obtain specified information. The statute does not define "authorized," or "authorization," which is used in the definition of "exceeds authorized access." The question before us 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. We conclude that it may, at least 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.[82]

The court held that, although the defendant was authorized to view and print all of the information she accessed, she could be held criminally liable under the CFAA because providing information to individuals to perpetrate a fraud was not an intended use of Citigroup's computers.[83] The court recognized there could be situations where a defendant may have no reason to know that use of a computer would breach an employer's policy. However, there were no such concerns about applying the CFAA criminal statute in this case given the defendant had "reason to know" she was not authorized to access information in furtherance of a criminally fraudulent scheme.[84]

It is noteworthy the Fifth Circuit indicated there could be some limits on whether the CFAA's criminal penalties apply for misuse.[85] The court stated it agreed with the First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*,[86] that an employment agreement can establish the parameters of authorized access, and the concept that "exceeds authorized access" exists "if the purposes for which access has been given are exceeded."[87] However, the Fifth Circuit stated "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."[88] Thus, the Fifth Circuit indicated the nature of the underlying conduct dictates whether criminal provisions of the CFAA apply. While an employer may obtain civil relief under the CFAA when an employee exceeds authorized access by misusing information in violation of company policy, the Fifth Circuit has created an

82. *Id.* at 271 (alteration in original) (citations omitted).
83. *Id.* at 272.
84. *Id.* at 273.
85. *Id.* at 272.
86. 274 F.3d 577 (1st Cir. 2001).
87. *John*, 597 F.3d at 272.
88. *Id.* In *EF Travel*, the First Circuit held the plaintiff employer stated a civil cause of action under the CFAA when its former employee violated a confidentiality agreement by disclosing plaintiff's proprietary information. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583-84 (1st Cir. 2001).

additional nuance that the criminal provisions only apply when such misuse is criminal in nature.[89]

3. Seventh Circuit

The Seventh Circuit also takes a broad approach that the CFAA applies to misuse of information, although it relies on agency theory. In *International Airport Centers., L.L.C. v. Citrin*,[90] an employee made a decision to quit his employment, but before he quit and notified his employer of the decision, the employee deleted data he collected during his employment from a company issued laptop computer.[91] The employee installed a program designed to permanently delete the data so it could not be recovered as the information would have revealed his improper conduct before he quit.[92]

The employer argued the employee violated 18 U.S.C. § 1030(a)(5)(A)(i),[93] which provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . violates the Act."[94] The court held the employee's installation of a program to delete files and prevent their recovery constituted a "transmission" within the meaning of the statute.[95]

The court also reviewed 18 U.S.C. § 1030(a)(5)(A)(ii),[96] which states that whoever "*intentionally accesses* a protected computer without authorization, and as a result of such conduct, recklessly causes damage" violates the Act.[97] The court held the employee violated that provision stating:

> [H]is authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit [his employer] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation

89. *Id.*

90. 440 F.3d 418 (7th Cir. 2006).

91. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

92. *Int'l Airport Ctrs.*, 440 F.3d at 419.

93. The provision has been amended since the date of this decision, although not in material part for purposes of this article. The text quoted by the court in 18 U.S.C. § 1030(a)(5)(A)(i) currently appears at 18 U.S.C. § 1030(a)(5)(A).

94. *Id.* (*quoting* 18 U.S.C. § 1030(a)(5)(A)(i)).

95. *Id.* at 419-20.

96. The provision has been amended since the date of this decision, although not in material part for purposes of this article. The text quoted by the court in 18 U.S.C. § 1030(a)(5)(A)(ii) currently appears in 18 U.S.C. § 1030(a)(5)(B).

97. *Id.* at 420 (*quoting* 18 U.S.C. § 1030(a)(5)(A)(ii)).

> of the duty of loyalty that *agency law* imposes on an employee.[98]

The court relied on principles of agency law in finding the employee violated the CFAA once he decided to terminate the employment relationship. At that point, the employee breached his duty of loyalty to his employer and with it any authority to access the computer:

> [The employee's] breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as [the employer's] agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship. "Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship." . . . "Unless otherwise agreed, the authority of the 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."[99]

Accordingly, the Seventh Circuit adopted a broad interpretation to apply the CFAA to misuse. It relies on agency law to determine the point at which authorized access to a computer terminates. This will require an inquiry into the intent and state of mind of the individual accessing the computer, as the court finds the authority of the agent to access is terminated once the agent makes a decision and acquires an interest adverse to the agent's duty of loyalty to the employer.[100] At that point, improper actions by the employee will violate the CFAA, even though the employer is unaware of the same.

4. Eleventh Circuit

The United States Court of Appeals for the Eleventh Circuit has also adopted a broad interpretation of the CFAA to hold it applies when a computer use policy is violated. In *United States v. Rodriguez*,[101] the defendant worked at the Social Security Administration and had access to government computer databases containing sensitive personal information.[102] A policy prohibited employees from accessing information from the computer databases for non-business reasons.[103] The defendant was charged with violating 18 U.S.C.

---

98. *Id.* at 420 (emphasis added).
99. *Id.* at 420-21 (citation omitted) (quoting State v. DiGiulio, 172 Ariz. 156, 160, 835 P.2d 488, 492 (Ariz. Ct. App. 1992)).
100. *Id.*
101. 628 F.3d 1258 (11th Cir. 2010).
102. United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010).
103. *Rodriguez*, 628 F.3d at 1260.

§ 1030(a)(2)(B) after he accessed information of individuals for his own personal reasons, such as looking at their income and obtaining dates of birth and addresses to send birthday gifts.[104] The defendant argued he did not violate the statute because he did not exceed his authorized access as he only accessed databases he was authorized to use as a representative of the Social Security Administration.[105]

The court reviewed the definition of "exceeds authorized access" and concluded "the plain language of the Act forecloses any argument that [the defendant] did not exceed his authorized access."[106] It rejected the defendant's argument that the CFAA did not apply because he was authorized to use the database. It reasoned the Social Security Administration's policy limited the use of its databases to business reasons, and the defendant's access of the information was not in furtherance of his job duties.[107] The court also rejected the defendant's argument that he could not be convicted under the CFAA because his use of the information was not criminal. It stated the defendant's actual use of the information "is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access."[108] The fact he "did not use the information to defraud anyone or gain financially is irrelevant."[109]

Thus, the Eleventh Circuit adopted a broad approach that the CFAA applies when an employer's use policy is violated. It is noteworthy the Eleventh Circuit takes an even broader approach to the type of penalties that may apply under the CFAA for misuse than the Fifth Circuit. The Fifth Circuit in *United States v. John*[110] stated it would not impose criminal penalties under the CFAA if the misuse did not constitute criminal conduct.[111] The Eleventh Circuit, however, stated that criminal sanctions under the CFAA can be imposed for a violation of a computer use policy, even though such use was not criminal in nature.[112]

---

104. *Id.* at 1260-62.

105. *Id.* at 1263.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.* at 1264.

110. 597 F.3d 263 (5th Cir. 2010).

111. *See* United States v. John, 597 F.3d 263, 272-73 (5th Cir. 2010) (stating that the student in United States v. Phillips, 477 F.3d 215 (5th Cir. 2007), was authorized to see and print the information that she accessed, while John's use of the Citigroup computer system to engage in fraud in *John* was not part of the intended use for the system); *see also* discussion of United States v. John, *supra* notes 65-110.

112. *See Rodriguez*, 628 F.3d at 1263.

B. Narrow Interpretations by Circuit Courts That The CFAA Does Not Apply to Misuse

In contrast to the cases from the First Circuit, Fifth Circuit, Seventh Circuit, and Eleventh Circuit, two recent federal circuit court decisions from the Fifth Circuit and Ninth Circuit interpreted the CFAA narrowly. The recent circuit court cases place greater emphasis on the legislative history, the legal doctrine of lenity requiring ambiguous criminal statutes be narrowly construed, and the practical consequences against applying the CFAA to misuse. The current trend in the circuit courts as revealed by these two recent decisions is that the CFAA does not apply when an individual misuses information that was obtained with permission.

1. Ninth Circuit

The Ninth Circuit interpreted the CFAA narrowly and held it does not apply to violations of employer use restrictions. In *United States v. Nosal*,[113] the defendant left his employment to start a competing business and convinced others still working for his former employer to download confidential computer information. The employees were authorized to access the database, but a company policy prohibited the disclosure of confidential information.[114] The defendant was charged with criminally violating 18 U.S.C. § 1030(a)(4) for aiding and abetting the employees in "exceed[ing their] authorized access" with the intent to defraud.[115] The defendant sought to dismiss the charges on the basis the CFAA only targets hackers and not individuals who access computers with authorization, but misuse the information obtained from such access.[116]

The court reviewed the CFAA's definition of "exceeds authorized access"[117] stating the language could be read in either of two ways. First, it could refer to someone who is authorized to access certain files or data on a computer, but instead accesses unauthorized files or data, which is commonly referred to as "hacking."[118] Second, it could refer to someone who has unrestricted access to information on a computer, but is limited in the manner the information can be put to use.[119]

In support of its argument that the CFAA applies to misuse, the government argued the word "so" in the definition of "exceeds author-

113. 676 F.3d 854 (9th Cir. 2012).
114. United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).
115. *Nosal*, 676 F.3d at 856 (alteration in original).
116. *Id.*
117. 18 U.S.C. § 1030(e)(6).
118. *Nosal*, 676 F.3d at 856-57.
119. *Id.* at 857.

ized access" should be interpreted to mean "in that manner."[120] Thus, the government reasoned that by replacing the word "so" with the phrase "in that manner," the definition could instead be read as "accesser is not entitled to 'in that manner' obtain or alter" to support its argument that the CFAA applies to misuse.[121] The court rejected the government's argument that a different meaning should be applied a word. Rather, the court stated the word "so" has meaning "even if it doesn't refer to use restrictions," or "Congress could just as well have included 'so' as a connector or for emphasis."[122] However, despite the court's statement, the court nevertheless commented on an alternative interpretation for the word "entitled" in the definition "accesser is not *entitled* so to obtain or alter."[123] It stated a "sensible reading of 'entitled' is as a synonym for 'authorized.'"[124] Under that interpretation, "exceeds authorized access" would refer to information on a computer that a person is not authorized to access.[125]

The court adopted the narrow approach and held the CFAA only applies to access restrictions and not use restrictions.[126] It reasoned Congress enacted the CFAA primarily to address computer hacking and the problem of an offender intentionally trespassing into computer files.[127] It stated both prohibitions of access "without authorization" and "exceeds authorized access" can be read to apply to hackers:

> "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.[128]

The court also reasoned that interpreting the CFAA broadly to prohibit misuse of information could "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute."[129] The CFAA extends to any "protected computer."[130] "Because 'protected computer' is defined as a computer affected by or involved in

120. *Id.*
121. *Id.*
122. *Id.* at 858.
123. *Id.* at 857.
124. *Id.*
125. *Id.*
126. *Id.* at 863-64.
127. *Id.* at 858 (quoting S. Rep. No. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)).
128. *Id.* at 858.
129. *Id.* at 857.
130. *Id.* at 859.

interstate commerce—effectively all computers connected with Internet access—[a broad interpretation] of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime."[131] "[M]illions of unsuspecting individuals would find that they are engaging in criminal conduct."[132] Basing criminal liability on violations of computer use policies could render otherwise innocuous behavior into violations of federal law simply because a computer is involved.[133] The court also relied on the doctrine of lenity stating it is a long-standing principle that ambiguous criminal statutes must be construed narrowly.[134] The court therefore held the CFAA's provision of "exceeds authorized access" is limited to violations of restrictions on "access" to information, and not restrictions on its "use."[135]

Accordingly, the Ninth Circuit adopted a narrow approach by limiting the CFAA to access violations and not misuse. A portion of the Ninth Circuit's opinion could be subject to potential criticism. On the one hand it rejected the argument that the word "so" should be read in a different manner.[136] On the other hand, the court commented that the word "entitled" in the definition of "exceeds authorized access" could be read as a synonym for the word "authorized."[137] Applying different meanings to words is contrary to established principles of statutory construction that all words must be given their plain and ordinary meaning and effect. In *Gustafson v. Alloyd Co., Inc.*,[138] the Supreme Court interpreted a statutory definition stating it "must be read in its entirety" and that the "Court will avoid a reading which renders some words altogether redundant."[139] Where the language of a statute is plain, "the sole function of the courts is to enforce it according to its terms."[140] Here, Congress certainly understood the

131. *Id.* at 859 (citing 18 U.S.C. § 1030(e)(2)(B)).

132. *Id.* at 859.

133. *Id.* at 860.

134. *Id.* at 862-63 (citing United States v. Santos, 553 U.S. 507, 514 (2008)).

135. *Id.* at 863-64.

136. *Id.* at 858.

137. *Id.* at 857.

138. 513 U.S. 561 (1995).

139. Gustafson v. Alloyd Co., Inc., 513 U.S. 561, 574 (1995).

140. United States v. Ron Pair Enters., 489 U.S. 235, 241 (1989) (citing Caminetti v. United States, 242 U.S. 470, 485 (1917)). It is a cardinal cannon of statutory construction that "courts must presume that a legislature says in a statute what it means and means in a statute what it says." Connecticut Nat'l Bank v. Germain, 503 U.S. 249, 253-54 (1992) (citations omitted). It is also a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." National Ass'n of Homebuilders v. Defenders of Wildlife, 551 U.S. 644, 666 (2007) (quoting FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 132 (2000)).

word "authorized" as it is used throughout the CFAA.[141] Therefore, the fact Congress did not use the word "authorized" and instead used the word "entitled" in the definition of "exceeds authorized access" is a distinction with significance.[142]

In any event, the Ninth Circuit did not reach its decision by applying different meanings to the statutory text. Rather, it adopted a narrow approach relying on the doctrine of lenity due to the ambiguity in the text. It also relied on the legislative history and the practical effect a broad interpretation would have as it could transform innocuous violations of computer use policies into federal crimes.[143] The Ninth Circuit interpreted the CFAA narrowly to maintain its focus on the issue of hacking rather than "turning it into a sweeping Internet-policing mandate."[144]

2. *Fourth Circuit*

The Fourth Circuit also adopted a narrow interpretation to hold that misuse of computer information the user has permission to access does not violate the CFAA. In *WEC Carolina Energy Solutions LLC v. Miller*,[145] the plaintiff argued a former employee violated the CFAA by downloading proprietary information from its computer system before resigning from employment, e-mailing the information to his personal e-mail address, and providing the information to a competitor.[146] The employer had provided the employee with a computer and access to the proprietary information, but issued a policy "that prohibited using the information without authorization or downloading it to a personal computer."[147]

The employer filed a civil action under the CFAA seeking to recover its damage and loss.[148] The employer argued violations of 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), and (a)(5)(B)-(C), all of which require accessing a computer "without authorization" or "exceeding authorized access."[149] The court discussed the legislative history of the

141. In Dep't of Revenue of Oregon v. ACF Indus., Inc., 510 U.S. 332 (1994), the Court stated it is an established rule of statutory construction that "identical words used in different parts of the same act are intended to have the same meaning." *Id.* at 342 (quoting Sorenson v. Secretary of Treasury, 475 U.S. 851, 860 (1986) (additional quotations omitted)).

142. 18 U.S.C. § 1030(e)(6).

143. *Nosal*, 676 F.3d at 854, 860.

144. *Id.* at 858.

145. 687 F.3d 199 (4th Cir. 2012).

146. WEC Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

147. *WEC Energy*, 687 F.3d at 202.

148. *Id.* at 201, n.1. The court also noted there are additional requirements to maintain a civil cause of action, one of which is an aggregate loss of at least $5,000 in value during any one-year period. *Id.*

149. *Id.* at 203.

CFAA stating it "remains primarily a criminal statute designed to combat hacking."[150] However, a private party who suffers damage or loss by reason of a violation of CFAA may also bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief."[151]

The employee sought to dismiss the CFAA claim arguing the employer's policies only regulated the "use" of the information and not access, and because the employee had permissible access, the employee asserted the employer could not establish a violation of the CFAA.[152] The court stated the issue was the scope of the terms "without authorization" and "exceeds authorized access" and "whether these terms extend to violations of policies regarding the *use* of a computer or information on a computer to which a defendant otherwise has access."[153]

The court stated that to analyze the issue, the first step with regard to statutory interpretation is to review the plain language of the statute.[154] Terms of a statute must be given their "ordinary, contemporary, common meaning" absent some indication by Congress to the contrary.[155] The court considered the fact that the CFAA has both civil and criminal applications and stated its interpretation of the statute would apply uniformly in both contexts.[156] Because the CFAA has a criminal application, it was required to follow "the canon of strict construction of criminal statutes, or rule of lenity."[157] A criminal statute must be construed strictly to avoid interpretations that are not "clearly warranted by the text" in order to provide fair warning what is prohibited by law.[158] The rule of lenity requires that Congress speak in clear and definite language before the court can impose the harsher alternative of two alternative readings.[159]

The court concluded "we adopt a narrow reading of the terms 'without authorization' and 'exceeds authorized access' and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."[160] It stated:

---

150. *Id.* at 201.
151. *Id.* (citing 18 U.S.C. § 1030(g)).
152. *Id.* at 202.
153. *Id.* at 203 (emphasis added).
154. *Id.*
155. *Id.*
156. *Id.* at 204.
157. *Id.* at 204 (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)).
158. *Id.* at 204 (citing Crandon v. United States, 494 U.S. 152, 160 (1990)).
159. *Id.* at 206.
160. *Id.*

> [W]e nevertheless conclude based on the "ordinary, contemporary, common meaning," . . . of "authorization," that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer "without authorization" when he gains admission to a computer without approval. . . . Similarly, we conclude that an employee "exceeds authorized access" when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access. . . . Notably, neither of these definitions extends to the improper *use* of information validly assessed.[161]

The court also reasoned it was "unwilling to transform a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy," noting there are other remedies for those grievances.[162] Thus, it held that because the employee did not access the computer without authorization or exceed authorized access, the employer failed to state a claim under the CFAA.[163]

The recent Fourth Circuit and Ninth Circuit cases rely on much of the same rationale. Both courts reason that because the CFAA has criminal penalties, the doctrine of lenity requires the statute be construed narrowly. Additionally, the legislative history demonstrates the CFAA was originally intended to target hackers. The courts also considered the practical consequences against imposing criminal liability for violations of computer use policies. Thus, the trend from those recent decisions is to limit the CFAA to violations of access restrictions and not misuse.

C. District Courts Within the Second Circuit Have Rendered Contrary Decisions Whether the CFAA Applies to Misuse

The United States Court of Appeals for the Second Circuit has not specifically decided the issue whether the CFAA applies to misuse. District courts within the Second Circuit have interpreted the CFAA in a contrary manner. Much like the trend with the recent circuit court decisions, the recent district court cases hold the CFAA does not apply to misuse. Like the circuit courts, many recent district court

161. *Id.* at 204 (citations omitted).

162. *Id.* at 207 (citing United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc)). It noted the plaintiff alleged nine state-law causes of action that could potentially provide relief, including tortious interference with contractual relations, conversion, civil conspiracy, and misappropriation of trade secrets. *Id.* at 207, n.4.

163. *Id.* at 207.

cases within the Second Circuit place greater emphasis on the legislative history, the legal doctrine of lenity, and the practical consequences against extending the CFAA to misuse.

For example, in *Advanced Aerofoil Technologies, AG v. Todaro*,[164] the plaintiff filed an action against former employees alleging they misused confidential and proprietary information obtained during their employment to create a company in direct competition with the plaintiff.[165] Plaintiff alleged the defendants violated 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(A)-(C) arguing that the defendants' use of the computer, after they decided to resign, constituted unauthorized access.[166] Plaintiff reasoned that, in reality, they were no longer employees, even though the employer did not yet know about their resignations and had not terminated their access to the computer systems.[167]

The court stated it was adopting a "narrow reading" of the CFAA and not expanding it to situations where an employee takes confidential information, using authorization given by the employer, and misuses the information.[168] It reasoned the legislative history as a whole indicated the CFAA was intended to prohibit improper access of a computer and not misuse.[169] It also noted the CFAA is primarily a criminal statute and that the rule of lenity required it be read narrowly and any ambiguity resolved in favor of the defendants.[170] Because there were no allegations that the plaintiff had revoked the defendants' unlimited access to its systems, the plaintiff failed to state a claim under the CFAA.[171]

Other recent district court decisions in the Second Circuit have taken the same approach to narrowly interpret the CFAA. In *JBCHoldings NY, LLC v. Pakter*,[172] the plaintiff filed an action alleging the defendants violated 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4) and 1030(a)(5)(C).[173] The court stated that in order to violate the provisions, a defendant must have acted "without authorization" or by "exceeding authorized access."[174] There is "no doubt that the CFAA applies to an 'outside' hacker who remotely enters a computer system

164. No. 11 Civ. 9505 (ALC)(DCF), 2013 WL 410873, at *1 (S.D.N.Y. Jan. 30, 2013).
165. Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ. 9505 (ALC)(DCF), 2013 WL 410873, at *1 (S.D.N.Y. Jan. 30, 2013).
166. *Advanced Aerofoil Techs.*, No. 11 Civ. 9505 (ALC)(DCF), 2013 WL 410873, at *5.
167. *Id.*
168. *Id.* at *7.
169. *Id.*
170. *Id.*
171. *Id.* at *7-8.
172. 931 F. Supp. 2d 514 (S.D.N.Y. 2013).
173. JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 517 (S.D.N.Y. 2013).
174. *JBCHoldings*, 931 F. Supp. 2d at 517.

without authority to do so."[175] However, it noted the federal circuit courts have been divided "whether an employee's *misuse* of an employer's information violates the CFAA where that information was obtained from a computer to which the employee was permitted access."[176]

The court relied on the Fourth Circuit and Ninth Circuit decisions in *WEC Carolina Energy Solutions LLC v. Miller*[177] and *United States v. Nosal*[178] stating it found the narrow approach more persuasive.[179] It therefore held an employee who has been granted access to a computer does not "exceed authorized access" by misusing that access, either through a breach of the duty of loyalty to the employer or by violating terms of use.[180] In support of its decision, the court relied on the "plain language" of the statute stating the language addressed access and did not refer to misuse or misappropriation of information.[181] It also reasoned that interpreting the statute to rely "on the employee's *purpose* in making use of his permitted access to the information . . . would effectively add to the statute a subjective intent requirement that Congress did not impose."[182] The court stated that, while it did not find the statute ambiguous, the doctrine of lenity "requires ambiguous criminal statutes be interpreted in favor of the defendants subjected to them."[183] As such, if Congress intended "to make a federal crime out of an employee's misuse of his work computer, it is required to say so clearly."[184]

The court also considered practical consequences against applying the CFAA to misuse given it could have an effect on millions of ordinary citizens. For example, an employee who looked at Facebook or checked a sporting event score in violation of an employer's use policy could be subject to immediate cessation of his agency and violate the CFAA under a broad interpretation.[185] It would "create a federal cause of action for incidents and injuries traditionally governed by state contract and tort laws."[186]

---

175. *Id.* at 521.
176. *Id.*
177. 687 F.3d 199 (4th Cir. 2012).
178. 676 F.3d 854 (9th Cir. 2012).
179. *BCHoldings*, 931 F. Supp. 2d at 522.
180. *Id.* at 522-23.
181. *Id.* at 523.
182. *Id.*
183. *Id.* (quoting United States v. Santos, 505 U.S. 507, 514 (2008)).
184. *Id.* at 524 (citing United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc)).
185. *Id.* at 525 (quoting WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)).
186. *Id.* (citing United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc)).

In contrast to the foregoing recent district court decisions, earlier district court decisions in the Second Circuit have taken a broad approach to apply the CFAA to misuse. In *Marketing Technology Solutions, Inc. v. Medizine LLC,*[187] the plaintiff argued its former employee violated 18 U.S.C. §§ 1030(a)(2)(C) and 1030(a)(4) by transferring its computer electronic files and trade secrets to a competitor during his employment.[188] The employee sought to dismiss the claims arguing the plaintiff could not prove he accessed the employer's computer "without authorization or in excess of authorization, because of the broad access [he] had as an employee."[189] The court denied the employee's motion to dismiss based on the fact the employment agreement contained a confidentiality provision. It relied on *EF Cultural Travel BV v. Explorica, Inc.*,[190] wherein the First Circuit Court of Appeals held that misuse of information in violation of a confidentiality agreement stated a claim under the CFAA.[191] Accordingly, the district court held the employee's access to the computers "exceeded his authorized use" and stated a claim under the CFAA.[192]

The district court in *Calyon v. Mizuho Sec. USA, Inc.*[193] also adopted a broad approach in interpreting the CFAA.[194] In that case, an employer brought an action against former employees alleging they violated 18 U.S.C. §§ 1030(a)(4) and 1030(a)(5)(A)(i) by copying proprietary information from the employer's computer system and emailing it to their personal accounts and a competitor during their employment in violation of internal email policies.[195] The court interpreted the CFAA broadly to apply to misuse, which it stated was based on the "plain language" of the statue:

> [T]he *plain language* of the statute seems to contemplate that, whatever else, "without access" and "exceeds authorized access" would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer.[196]

187. No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *1 (S.D.N.Y. May 18, 2010).

188. Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *1 (S.D.N.Y. May 18, 2010).

189. *Mktg. Tech. Solutions*, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *7.

190. 274 F.3d 577 (1st Cir. 2001).

191. *Mktg. Tech. Solutions*, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *7.

192. *Id.* at *7 (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-84 (1st Cir. 2001)).

193. No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007).

194. Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007).

195. *Calyon*, No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1.

196. *Id.* at *1 (emphasis added).

In denying a motion to dismiss, the court reasoned the employees did not have authorization to access the computer system to take proprietary documents to give to a competitor, and therefore the employer stated a claim under the CFAA.[197]

While the district court in *Calyon* stated it was adopting a broad approach based on the "plain language" of the statute, another district court in the Second Circuit held the plain language supported a narrow interpretation. In *Orbit One Commc'ns, Inc. v. Numerex Corp.*,[198] the plaintiff brought an action against former employees alleging they violated 18 U.S.C. §§ 1030(a)(4) and 1030(a)(5)(A)(iii) by intentionally accessing computer systems and downloading confidential and proprietary information in the course of their employment.[199] The court found the "plain language" of the CFAA supported a narrow reading and did not apply, even where the employees misused or misappropriated information after they left given the employer had granted them unlimited access.[200] It stated:

> The *plain language* of the CFAA supports a narrow reading. The CFAA expressly prohibits improper "access" of computer information. It does not prohibit misuse or misappropriation. Although the statute does not define "access without authorization," it provides that the phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled [sic][201] to obtain or alter." Thus, reading the phrases "access without authorization" and "exceeds authorized access" to encompass an employee's misuse or misappropriation of information to which the employee freely was given access and which the employee lawfully obtained would depart from the plain meaning of the statute.[202]

The court stated the statute as a whole indicated Congressional intent to prohibit access to computers without authorization, rather than address an employee's misuse of information the employee was entitled to access.[203] It considered the CFAA's definition of "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[204] It also considered the CFAA's definition of "loss" as "a reasonable cost to any victim, including the cost of re-

197. *Id.*
198. 692 F. Supp. 2d 373 (S.D.N.Y. 2010).
199. Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 384 (S.D.N.Y. 2010).
200. *Orbit One*, 692 F. Supp. 2d at 385.
201. The court omitted the word "so" from the definition "exceeds authorized access" contained in the CFAA. *See* 18 U.S.C. § 1030(e)(6).
202. *Orbit One*, 692 F. Supp. 2d at 385 (emphasis added).
203. *Id.*
204. *Id.* (quoting 18 U.S.C. § 1030(e)(8)).

sponding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[205] The court stated those definitions are consistent with the CFAA's "prohibition of computer hacking, which compromises the integrity and availability of data and may cause an interruption of computer service," and are inconsistent with a broader interpretation that the CFAA applies to misuse.[206]

Finally, the court stated it was guided by the rule of lenity to interpret the CFAA, which is "primarily a criminal statute," to resolve an ambiguity that it is only to apply to conduct clearly covered.[207] The court dismissed the CFAA claim concluding it would be "imprudent to interpret the CFAA, in a manner inconsistent with its plain meaning, to transform the common law civil tort of misappropriation of confidential information into a criminal offense."[208]

As demonstrated, district courts within the Second Circuit have rendered conflicting and contrary interpretations as to the scope of the CFAA, with earlier cases adopting a broad approach to apply it to misuse, and recent cases narrowly interpreting it to only apply to violations of access restrictions. The recent district court decisions within the Second Circuit are developing a trend similar to the recent decisions of the circuit courts that the CFAA does not apply to misuse. The recent decisions place greater emphasis on the legislative history, the legal doctrine of lenity, and the practical consequences to apply a narrow interpretation.

V. LEGISLATION HAS BEEN PROPOSED TO RESOLVE THE AMBIGUITY IN THE CFAA REGARDING "EXCEEDS AUTHORIZED ACCESS"

As noted, there is a split in the United States Circuit Courts of Appeals regarding the scope of the CFAA and whether it applies to misuse. The uncertainty regarding Congressional intent has, in particular, been caused by the phrase "exceeds authorized access."

Members of the Senate and House of Representatives recently proposed legislation to amend the CFAA and resolve the ambiguity regarding the phrase "exceeds authorized access." The bills have been referred to as "Aaron's Law Act of 2013" in recognition of Aaron Swartz, a late activist and hacker who was being prosecuted under the

205. *Id.* (quoting 18 U.S.C. § 1030(e)(11)).
206. *Id.* at 386.
207. *Id.*
208. *Id.*

CFAA at the time of his suicide.[209] According to a press release on July 19, 2011 by the United States Department of Justice, the government indicted Mr. Swartz for accessing the Massachusetts Institute of Technology's network without authorization.[210] The government reported that Mr. Swartz downloaded scientific journals and academic work from a not-for-profit archive in order to distribute them to the public through file sharing websites.[211] Mr. Swartz faced up to 35 years in prison and a fine up to $1,000,000.[212] The government filed a dismissal of the action on January 14, 2013, following Mr. Swartz's death on January 11, 2013.[213]

A bill sponsored by Representative Zoe Lofgren (D-CA) was introduced to the House of Representatives on June 20, 2013, as "Aaron's Law Act of 2013."[214] The bill is summarized as: "A bill to amend title 18, United States Code, to provide for clarification as to the meaning of access without authorization, and for other purposes."[215] The bill was referred to the House Committee on the Judiciary on June 20, 2013.[216]

Senator Ron Wyden (D-OR) sponsored a bill to the Senate on June 20, 2013, containing the same substantive text as the House bill. The summary of the Senate bill states: "A bill to amend title 18, United States Code, to provide for clarification as to the meaning of access without authorization, and for other purposes."[217] On June 20, 2013, the bill was referred to the Senate Committee on the Judiciary.[218]

Both the Senate bill and House bill strike the definition of "exceeds authorized access"[219] from the CFAA and substitute a new definition of "access without authorization." The bills provide in relevant part:

> Sec. 2. CLARIFYING THAT 'ACCESS WITHOUT AUTHORIZATION' UNDER 18 U.S.C. 1030 MEANS CIRCUMVEN-

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

210. Press Release, United States Department of Justice, U.S. Attorney's Office, District of Massachusetts, Alleged Hacker Charged With Stealing Over Four Million Documents From MIT Network (July 19, 2011), *available at* http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html.

211. *Id.*

212. *Id.*

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

214. H.R. 2454, 113th Cong. § 1 (2013).

215. *Id.*

216. 159 CONG. REC. H3988 (June 20, 2013).

217. S. 1196, 113th Cong. (2013).

218. 159 CONG. REC. S4792-02 (June 20, 2013).

219. 18 U.S.C. § 1030(e)(6).

> TION OF TECHNOLOGICAL BARRIERS IN ORDER TO GAIN AUTHORIZED ACCESS.
> IN GENERAL. – Section 1030(e)(6) of title 18, United States Code, is amended by –
> striking 'exceeds authorized access' and all that follows; and inserting the following: 'access without authorization' means –
> '(A) to obtain information on a protected computer;
> '(B) that the accesser lacks authorization to obtain; and
> '(C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information;'.[220]

The proposed legislation should resolve the current dispute as to the scope of the CFAA. It deletes the ambiguous definition "exceeds authorized access" which has been the source of confusion and contrary judicial interpretations whether the CFAA applies to the misuse. Instead, the proposed legislation substitutes the definitional phrase "access without authorization" and adds the requirement that the user must have knowingly circumvented technological or physical measures that were designed to prevent access to the information.[221] Thus, the legislation should sufficiently clarify that the CFAA applies to violations of access restrictions and not misuse, given the requirement that measures designed to prevent unauthorized individuals from obtaining the information must be circumvented.

VI. LEGAL DOCTRINES REQUIRE THE CFAA BE INTERPRETED NARROWLY AND NOT APPLY TO MISUSE

The split in the United States Circuit Courts of Appeals has resulted in conflicting applications of the statute.[222] Currently, the determination of whether misuse violates the CFAA is essentially dependent on the jurisdiction where the conduct occurred or claim accrued. The same conduct has resulted in vastly different consequences depending on which court decides the CFAA claim.[223]

The judicial split is due to ambiguous text in the CFAA, which has lead to confusion as to Congressional intent.[224] Given the CFAA has significant criminal applications, its scope must be clarified to provide appropriate notice to the public regarding what conduct is criminal

220. H.R. 2454, 113th Cong. (2013); S1196, 113th Cong. (2013).
221. *Id.*
222. *See supra* notes 65-208 and accompanying text.
223. *See supra* notes 65-208 and accompanying text.
224. *See supra* notes 258-263 and accompanying text.

under federal law. The ambiguity in the CFAA should be resolved by further legislation. In the event Congress fails to amend the CFAA, the United States Supreme Court should grant review to resolve the split in the circuit courts.[225] In the event of a judicial resolution, the split should be resolved by holding the CFAA is limited to violations of access restrictions and not misuse.

The legislative history indicates the CFAA was intended as an anti-hacking statute.[226] Congress responded to the threat of individuals hacking into computer systems by enacting legislation to provide criminal penalties against those who engaged in such improper access.[227] The CFAA was subsequently amended and the provision "exceeds authorized access" was added.[228] The legislative history from that time indicates the provision was intended to address conduct by individuals who had permission to use computers, but who accessed additional information beyond the permission they were granted.[229] In other words, it was intended to address unauthorized access by insiders, not misuse. Thus, the legislative history supports judicially interpreting the CFAA narrowly to only apply to violations of access restrictions and not misuse. This is why the recent decisions by the Fourth Circuit and Ninth Circuit have interpreted the CFAA narrowly as they relied more heavily on the legislative history.[230]

The legal doctrine of lenity also requires a narrow judicial interpretation of the CFAA.[231] The CFAA is primarily a criminal statute. Both the criminal and civil provisions must be read consistently and in the same manner, as it would be improper to construe the scope of the CFAA differently depending on whether criminal penalties or civil remedies were being sought.[232] Therefore, the CFAA as a whole must be interpreted narrowly. It is a long standing principle of jurisprudence that when language in a criminal statute is susceptible to two alternative meanings, it must be interpreted in a narrow fashion to

225. Other commentators have noted, given the split in the circuit courts, "[t]he stage is set for an appeal to the Supreme Court on the scope of the CFAA as it relates to employee-hackers and what is the meaning of 'authorized access' in the phrase 'exceeds authorized access.'" Robert C. Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, But Illegal in Miami, Dallas, Chicago, and Boston*, 87 FLA. BAR J. 36 (2013).

226. Pub. L. No. 98-473, 98 Stat. 1837, Sec. 2102(a) (Oct. 12, 1984). *See also* S. REP. NO. 99-432, at *3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 (discussing the purpose of the 1984 Act).

227. H.R. REP. 98-894, at *20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706.

228. *See* S. REP. NO. 99-432, at *9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2486.

229. *Id.*

230. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc); WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

231. *WEC Carolina Energy*, 687 F.3d at 204 (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)).

232. *WEC Carolina Energy*, 687 F.3d at 204.

avoid imposing the harsher penalty absent clear Congressional intent to the contrary.[233] The definition "exceeds authorized access" in the CFAA has been interpreted in contrary manners by different courts. The fact different courts have stated their respective contrary interpretations were based on the same "plain language" highlights the inherent ambiguity of the language.[234]

Under the doctrine of lenity, before the CFAA can be extended to persons who misuse computer information, Congress must first be compelled to speak in a clear manner announcing its intention to criminalize such conduct.[235] While Congress would have the right to enact legislation making it a federal crime to misuse computer information, the judicial branch should not interpret the CFAA in that manner absent a clear pronouncement from Congress.[236] Criminal statutes must be construed narrowly "so that Congress will not unintentionally turn ordinary citizens into criminals."[237]

The recent trend in the federal circuit courts, as exemplified by the Fourth Circuit and Ninth Circuit, places more emphasis on lenity, whereas the earlier decisions from the First Circuit, Fifth Circuit, Seventh Circuit and Eleventh Circuit did not.[238] The Supreme Court should follow the recent trend and resolve the judicial split by holding the CFAA does not apply to misuse.

VII. POLICY CONSIDERATIONS SUPPORT LIMITING THE CFAA TO VIOLATIONS OF ACCESS RESTRICTIONS

There are policy considerations against interpreting the CFAA broadly to apply to misuse. The CFAA applies to a "protected computer," which has been interpreted as any computer connected to the Internet.[239] Therefore, the CFAA can apply to essentially everyone who uses a computer in modern society.

Courts have noted the practical consequences against extending the CFAA to misuse as it could subject countless users who engage in

233. *Id.* at 206.

234. *Compare* Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. 2007) (stating it was adopting a broad approach based on the "plain language" of the CFAA), *with* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 384 (S.D.N.Y. 2010) (stating it was adopting a narrow approach based on the "plain language" of the CFAA).

235. *WEC Carolina Energy*, 687 F.3d at 204.

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

237. *Id.* at 863.

238. *Compare* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc); WEC Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012), *with* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

239. *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).

essentially innocuous conduct to criminal sanctions and civil liability.[240] For example, it could apply to individuals who violate terms of service, such as lying about one's age on a social networking Internet website.[241] Another common scenario is where an employer provides a computer with Internet access to its employee with a policy that the computer only be used for business purposes. If the employee uses the computer to access the Internet to look at the score of a baseball game, or check the price of a product at a retail store, neither of which are for business purposes, the employee will have violated the employer's use policy and could face criminal sanctions under the CFAA.[242] It is difficult to image Congress intended the CFAA to apply to such innocuous conduct absent a clear pronouncement for the same.

Consider even a scenario where an employee clearly misuses computer information, but the level of misconduct does not rise to a level that has historically been considered criminal in nature. Assume an employee has permission to access a report created by a co-worker on the employer's computer, but the employee misuses the report by plagiarizing it as the employee's own work in violation of company policy. Such conduct would certainly subject the employee to repercussion by the employer. However, if the CFAA applies to misuse, it could also transform that employee into a federal criminal for misusing information the employee had permission to access on the employer's computer. In fact, such conduct would be rendered criminal under federal law simply because the information came from a computer rather than from a file cabinet. While Congress could criminalize such actions, there are policy considerations against turning countless individuals into criminals under federal law for that type of conduct.[243]

There are also policy considerations against extending the CFAA to misuse and making the determination of whether conduct is criminal dependent on an employer's use policy, particularly when the policy is not uniformly enforced.[244] Consider the example where an employer has a written policy stating files from its computer system are not to be downloaded without permission. However, an employee downloads a file to a personal laptop computer to work at home, but fails to request permission because the employee was confused whether a policy existed as the employer never consistently enforced the policy. The concern of extending the CFAA to misuse and giving

240. WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012); JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 525 (S.D.N.Y. 2013).

241. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

242. *See WEC Carolina Energy*, 687 F.3d at 206; JBCHoldings, 931 F. Supp. 2d at 525.

243. *Nosal*, 676 F.3d at 859.

244. *See, e.g., WEC Carolina Energy*, 687 F.3d at 206; *Nosal*, 676 F.3d at 859.

the employer unlimited discretion when to enforce the written use policy becomes apparent.[245] An employer could decide to discriminately enforce its written policy by selectively targeting certain employees and threatening, for example, to request a prosecutor file criminal charges unless the employee resigned or agreed to other sanctions. The concern is highlighted by the fact employer use policies are typically non-negotiable with the terms and enforcement being dictated by the employer. Limiting the CFAA to violations of access restrictions should avoid such problems given there will likely be little confusion about whether a individual has permission to access computer information.

Interpreting the CFAA in a narrow manner will not deprive a computer owner from seeking relief against individuals who misuse information.[246] There are various federal statutes and common law doctrines that provide remedies against individuals who misuse information, including providing for damages or injunctive relief. Common law doctrines can include misappropriation of trade secrets, breach of contract, and tort remedies.[247] Federal legislation currently exists to protect against the misappropriation of information, such as the Federal Copyright Act,[248] Theft of Trade Secrets Act,[249] and Stored Communications Act.[250]

However, even though other remedies are available, some claimants may prefer that they be permitted to file actions under the CFAA for misuse because criminal penalties and damage recovery can be significant. Criminal sanctions can include imprisonment up to five, ten or twenty years depending on the type and level of conduct.[251] Civil remedies can include injunctive relief and the recovery of damages and loss.[252] The CFAA broadly defines "loss" as "any reasonable cost to the victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred

245. *See, e.g., Nosal*, 676 F.3d at 860 (the court reasoned private parties could manipulate personnel and computer-use policies to turn relationships "into ones policed by the criminal law", and that "[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.").

246. *See, e.g., Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010).

247. *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010).

248. 17 U.S.C. § 501, *et seq*.

249. 18 U.S.C. § 1832.

250. 18 U.S.C. § 2701, *et seq*.

251. *See* 18 U.S.C. § 1030(c).

252. 18 U.S.C. § 1030(g).

because of interruption of service".[253] Therefore, the monetary recovery could potentially be greater under the CFAA as damages can include the cost of responding to the offense and conducting a damage assessment.[254] Nevertheless, while the CFAA may provide relief beyond the remedies available in other types of actions, it is not a sufficient basis to extend the CFAA to misuse. Rather, it is better to leave actions arising from information misuse to other laws specifically tailored to that type of misconduct.

There are also policy considerations against placing too much discretion in the hands of a prosecutor if the CFAA were extended to misuse. The Ninth Circuit in *Nosal* said "we shouldn't have to live at the mercy of our local prosecutor."[255] Courts have rejected arguments by the government that it wouldn't prosecute minor violations of statutes as a basis to interpret statutes broadly, reasoning giving such power to a prosecutor could invite "discriminatory and arbitrary enforcement."[256] At a minimum, individuals should have notice as to what conduct is criminal, and the fact the government may or may not prosecute such conduct creates too much uncertainty, inconsistency, and confusion requiring that the CFAA be narrowly interpreted.[257]

In light of the foregoing policy considerations, the CFAA should be limited to violations of access restrictions. There are practical consequences against extending the CFAA to misuse and it should accordingly be limited to an anti-hacking statute focused on improper access.

VIII. CONGRESS SHOULD AMEND THE CFAA, AND ABSENT FURTHER CONGRESSIONAL ACTION, THE SUPREME COURT SHOULD RESOLVE THE JUDICIAL SPLIT HOLDING THE CFAA DOES NOT APPLY TO MISUSE

There is an immediate need for Congress to pass legislation clarifying that the CFAA does not apply to misuse. While Congress certainly has the right to criminalize the misuse of computer information accessed with permission, members of Congress should have an opportunity to first fully debate the issue as to whether they want to

253. 18 U.S.C. §1030(e)(11).

254. *Id.*

255. *Nosal*, 676 F.3d at 862. In United States v. Stevens, 559 U.S. 460 (2010), the Court stated, "We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly." *Id.* at 480.

256. *Nosal*, 676 F.3d at 862 (citing United States v. Kozminski, 487 U.S. 931 (1988)).

257. Some legal commentators have recognized the problem that a broad scope of the CFAA will lead to arbitrary and discriminatory enforcement and difficulty for people to understand what conduct the statute forbids. *See* Timothy P. O'Toole, *Digital Defense: Meeting the Challenges That the Computer Fraud And Abuse Act Poses*, 37 THE CHAMPION 44 (2013).

criminalize such conduct, particularly given the foregoing policy considerations and practical consequences against a broad application.[258]

As previously noted, bills were introduced in both the House of Representatives and Senate on June 20, 2013 to amend the CFAA.[259] The proposed legislation would delete the ambiguous definition "exceeds authorized access" and substitute the phrase "access without authorization" while adding the requirement that technological barriers be circumvented in order to gain authorized access.[260] The legislation will therefore clarify that the CFAA applies to violations of access restrictions and not misuse.[261]

Absent further action by Congress, the United States Supreme Court should grant review to resolve the current judicial split. The circuit courts have reached contrary and opposing interpretations.[262] Therefore, the determination of whether information misuse violates the CFAA is essentially dependent on the court deciding the issue. This judicial split has created confusion and uncertainty in the public as to what conduct is criminal, and review by the United States Supreme Court is necessary to resolve that dispute.

The Supreme Court should resolve the dispute following the trend that has been created by the recent federal court cases that interpret the CFAA narrowly.[263] The recent federal court cases have placed greater emphasis on the legislative history, the legal doctrine of lenity, and the practical consequences against applying the CFAA to misuse. The practical consequences against a broad interpretation are becoming more apparent as the use of computers with Internet access is growing, thereby subjecting many more individuals to the CFAA's provisions. Perhaps the federal courts are coming to the realization that broadly interpreting the CFAA will have practical consequences far beyond what Congress could have intended, given that extending the CFAA to prohibit misuse will transform numerous individuals into federal criminals from essentially innocuous conduct. Therefore, in light of the policy considerations, the legislative history, and the legal doctrine of lenity, the Supreme Court should resolve the judicial split

258. *See supra* notes 258-263 and accompanying text.
259. H.R. 2454, 113th Cong. (2013); S1196, 113th Cong. (2013).
260. *Id.*
261. *Id.*
262. *See supra* notes 258-263 and accompanying text.
263. The two circuit court cases and three district court cases discussed herein which interpreted the CFAA narrowly were decided in 2013, 2012 and 2010. *See supra* notes 112-208 and accompanying text. The four circuit court cases and two district court cases discussed herein which interpreted the CFAA broadly to apply to misuse were decided in 2010, 2007, 2006 and 2001. *See supra* notes 65-112, 187-197 and accompanying text. While there are additional district court cases addressing the CFAA, the cases discussed herein are illustrative of the trend developing with district court decisions in the Second Circuit.

by holding the CFAA does not apply to the misuse of information that was accessed from a computer with permission.

IX. CONCLUSION

The CFAA was an attempt by Congress to criminalize the problem of computer hacking and the improper access of computer information. However, the statutory text in the CFAA regarding "exceeds authorized access" is ambiguous and has lead to confusion by the federal courts regarding Congressional intent, which has resulted in conflicting and contrary interpretations regarding its scope. A split exists in the United States Circuit Courts of Appeals as to whether the CFAA prohibits the misuse of information that was accessed with permission. There is an immediate need for Congress to amend the CFAA to eliminate that ambiguity and resolve the dispute. Absent further action by Congress, the United States Supreme Court should grant review to resolve the split in the federal circuit courts. The Supreme Court should follow the trend that has developed by the recent federal court decisions which place greater emphasis on the legislative history, the legal doctrine of lenity, and policy considerations to limit the CFAA to violations of access restrictions and not misuse.