Loyola of Los Angeles Law Review

Volume 47
Number 3 *Spring 2014*

Article 9

Spring 2014

The Computer Fraud And Abuse Act: As Conflict Rages On, The United States v. Nosal Ruling Provides Employers Clear Guidance

Ryan E. Dosh
J.D. Candidate, May 2014, Loyola Law School, Los Angeles

THE COMPUTER FRAUD AND ABUSE ACT: AS CONFLICT RAGES ON, THE *UNITED STATES V. NOSAL* RULING PROVIDES EMPLOYERS CLEAR GUIDANCE

Ryan E. Dosh∗

I. INTRODUCTION

In 2010, industrial espionage cost U.S. businesses more than $250 billion.[1] While this figure represents all forms of industrial espionage, companies often neglect a class of perpetrators that would be easy to foil: internal employee hackers.[2] It is a common scenario for employees, or soon-to-be-former employees, to download sensitive business information in violation of corporate policy.[3] Over the past several years, employers aware of internal breaches have taken legal action by filing state and federal claims against rogue employees.[4] One weapon in their arsenal is to claim a violation of the Computer Fraud and Abuse Act (CFAA),[5] the United States' most far-reaching computer statute.[6] However, federal courts are greatly conflicted over the scope of the CFAA: whether it only establishes penalties for accessing information or if it is broad enough to include the misuse of information.[7] The Ninth Circuit created a circuit split

∗ J.D., May 2014, Loyola Law School, Los Angeles; B.A. 2011, California Lutheran University. A special thank you to my friends and family, and in particular, to my late father for his unconditional support and guidance.

1. *Insider Data Theft: When Good Employees Go Bad*, SYMANTEC (Dec. 12, 2011), http://www.symantec.com/connect/blogs/insider-data-theft-when-good-employees-go-bad.

2. *Id.*

3. Leslie Paul Machado, *Protecting Against Employee Theft*, HUM. RESOURCES EXECUTIVE ONLINE (July 12, 2010), http://www.hreonline.com/HRE/view/story.jhtml?id=475264808&ss=machado.

4. *See, e.g.*, Petition for Writ of Certiorari at 5, WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (No. 12-158), 2012 WL 5353899.

5. 18 U.S.C. § 1030 (2008).

6. *See id.*; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

7. *See* Petition for Writ of Certiorari, *supra* note 4, at 8–9.

with *United States v. Nosal*,[8] holding that the CFAA only covers the "unauthorized access" of computer information, not its misuse, as the First, Fifth, Seventh, and Eleventh Circuits' broad interpretations of the CFAA have held.[9] Thus, employers are stuck between an employer-friendly interpretation of the CFAA and an employee-friendly interpretation, depending on which jurisdiction they are in.[10]

This Comment explores the federal circuit split over the CFAA's scope and its effect on employers looking to bring CFAA claims against "rogue employees." Part II explores the history of the CFAA, its current posture, and the sections of the statute that are most cited by employers bringing CFAA claims against former employees. Part III analyzes the Ninth Circuit's narrow interpretation of the CFAA in its en banc holding in *United States v. Nosal*. Part IV addresses the widening circuit split over the broad and narrow interpretations of the CFAA, while Part V supports the argument that a narrow interpretation should prevail. Part VI then offers advice for employers hoping to preserve CFAA claims against rogue employees and solutions for protecting sensitive business information. Part VII concludes.

II. CFAA: HISTORY AND CURRENT POSTURE

Congress originally enacted the CFAA in 1984 to protect government computers from unauthorized access and to combat newly emerging, ever-increasing computer crimes.[11] The CFAA was the first federal statute to specifically address computer crimes.[12] Originally a purely criminal statute, the CFAA was limited in scope.[13] The original version "criminalized only important federal interest computer crimes"—those relating to national security secrets, certain financial institutions, and government-owned and -operated computers.[14] However, over the past twenty-eight years Congress has substantially expanded the statute in an attempt to keep

8. 676 F.3d 854 (9th Cir. 2012).

9. *Id.* at 863.

10. *See* Petition for Writ of Certiorari, *supra* note 4, at 6.

11. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2006)).

12. *See* Kerr, *supra* note 6, at 1564.

13. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, *supra* note 11, at 2191.

14. Kerr, *supra* note 6, at 1561; *see also* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, *supra* note 11, at 2191.

pace with the rapidly changing computerized world.[15] The statute's scope now includes nearly every computer in the United States and millions of computers abroad.[16]

The first significant amendment occurred in 1994, when Congress added a private cause of action to the statute.[17] In turn, the 1994 amendment gave any private party the right to "maintain a civil action against . . . violator[s]" of the CFAA.[18] Later, in 1996, Congress expanded the CFAA's scope again, by introducing the term "protected computer."[19] The CFAA's authority then extended to any computer used by the government, by financial institutions, or in interstate commerce or communication.[20] Again, in 2001, Congress extended the scope of the CFAA to include international computers.[21] Most recently, a 2008 amendment expanded the definition of protected computers once again. The definition now includes any computer used by a financial institution, by the United States government, or by any computer used in *or affecting* foreign and interstate commerce and communications.[22] As one author argued, "the CFAA [is] one of the most far-reaching criminal laws in the United States Code,"[23] due to our increasing dependency on an internet-connected, computerized world.

As a result of the statute's evolution and broad definitions, private parties, especially employers, are bringing an increasing number of CFAA claims in federal court.[24] The statute permits a "private party who suffers damage or loss by reason of a violation of 'the statute'" to bring a federal civil cause of action against the violator.[25] Assuming the plaintiff can show damages of at least

15. Kerr, *supra* note 6, at 1563.

16. *Id.* at 1561.

17. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit.XXIX, 108 Stat. 2097.

18. *Id.* at 2098.

19. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3492.

20. Kerr, *supra* note 6, at 1567–68.

21. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 382–84 (2001) (codified in scattered sections of 18 U.S.C. and 50 U.S.C.).

22. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 207, 122 Stat. 3560, 3563 (codified at 18 U.S.C. § 1030(e)(2)(B)).

23. *See* Kerr, *supra* note 6, at 1561.

24. Richard Raysman & Peter Brown, *'Unauthorized Access' and the Computer Fraud and Abuse Act*, N.Y. L.J. (Oct. 12, 2010), http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202473140814.

25. *Id.*

$5,000 within any one-year period, a CFAA claim may be brought in federal courts, which gain federal question jurisdiction under the statute.[26] Most claims brought under the statute are for unauthorized access to a computer or for access beyond the user's authorization level.[27]

Thus, employers most frequently claim a CFAA violation under Section 1030(a)(2)[28], against employees who "intentionally [access] a computer without authorization or [exceed] authorized access, and thereby [obtain] . . . information from any protected computer,"[29] and Section 1030(a)(4), against those who "knowingly and with intent to defraud, [access] a protected computer without authorization, or [exceed] authorized access, and by means of such conduct [further] the intended fraud and [obtain] anything of value."[30] The statute defines "exceeding authorized access" as "access[ing] a computer with authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[31] However, the statute fails to define "without authorization."[32] Therefore, the statute's broad definition of a "protected computer," in conjunction with the lack of a clear statutory definition for "authorization," has left federal courts split as to the scope and meaning of the CFAA.[33]

As federal courts continue to dispute the legislative intent behind the CFAA and the statute's scope, Congress continues to propose legislation that is equally conflicted.[34] What is certain is Congress' original intent to create a single statute to cover the field of computer crime "rather than identify[] and amend[] every potentially applicable statute affected by advances in computer technology."[35] However, that does little to resolve a widening circuit

26. 18 U.S.C. § 1030(c)(4)(i)(I) (2006).

27. *See* Machado, *supra* note 3.

28. *See* LINDA K. STEVENS & JESI J. CARLSON, THE CFAA: NEW REMEDIES FOR EMPLOYEE COMPUTER ABUSE 2 (2008), *available at* http://www.schiffhardin.com/binary/stevens_carlson_ibj_0308.pdf.

29. 18 U.S.C. § 1030(a)(2) (2008).

30. *Id.* § 1030(a)(4).

31. *Id.* § 1030 (e)(6).

32. *See id.* § 1030.

33. *See* Petition for Writ of Certiorari, *supra* note 4.

34. Erin Fuchs, *The Law Used To Target Aaron Swartz Doesn't Make Sense Anymore*, BUS. INSIDER (Jan. 20, 2013), http://www.businessinsider.com/computer-fraud-and-abuse-act-reform-2013-1.

35. S. REP. NO. 104-357, at 5 (1996).

split, nor does it help employers looking to "rein in rogue employees."[36]

III. *UNITED STATES V. NOSAL*

In *Nosal*, the Ninth Circuit narrowly construed the CFAA's term "exceeds authorized access" to not cover unauthorized disclosure or fraudulent use of information, even if covered as prohibited conduct by a company's computer-use agreement.[37] Instead, the *Nosal* court stated that the CFAA only covers claims as to a computer's access and not the misuse of information obtained by such access.[38] There, the defendant, David Nosal, resigned from a major executive search firm, Korn/Ferry, after over eight years of service.[39] As part of his departure from the firm, Nosal received $25,000 monthly compensation and two lump sums of money in exchange for signing a one-year non-compete agreement.[40] However, Nosal left the firm intending to start his own business with the help of current Korn/Ferry employees.[41] Nosal convinced two employees to download company information from a confidential database and transfer the information to him.[42] The employees maintained valid credentials granting them access to the information, but violated an employee policy that forbade disclosing confidential information.[43] The government charged Nosal with violating the CFAA by aiding the employees in "exceeding authorized access" under Section 1030(a)(4).[44] Nosal then challenged the CFAA claims, stating that the statute only targets "hackers, not individuals who access a computer with authorization but then misuse the information they obtain by means of such access."[45]

The *Nosal* majority found the purpose of the statute was to "punish hacking" and not the misappropriation of trade secrets.[46] The

36. WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012).
37. United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).
38. *Id.*
39. *Id.* at 856.
40. Brief for the United States at 3, United States v. Nosal, 642 F.3d 781 (9th Cir. 2010) (No. 10-10038), *aff'd en banc* 676 F.3d 854 (9th Cir. 2012), .
41. *Nosal*, 676 F.3d at 856.
42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.* at 863.

court reasoned that the CFAA's text "limited violations of restrictions on *access* to information, and not restrictions on its *use*."[47] The court found that the CFAA's principal purpose was to target hackers, not to "allow private parties to manipulate their computer-use agreements and personnel policies so as to turn [employment] relationships into ones policed by the criminal law."[48] Considerably concerned with expanding the scope of a criminal statute, the majority determined that the CFAA was not intended to criminalize minor computer misuses in the workplace.[49]

The dissent in *Nosal* found that the statute's purpose was to prevent the stealing of valuable information, regardless of who was the culprit.[50] Significantly, however, the dissent acknowledged that this contested portion of the statute might be unconstitutionally vague.[51] The *Nosal* court's holding created a clear circuit split between the narrow interpretation penned by Judge Kozinski and the broad interpretation taken by several other federal circuits.[52]

IV. JUDICIAL INTERPRETATION: WIDENING CIRCUIT SPLIT

A widening circuit split has evolved over the interpretation of the CFAA's terms "without authorization" and "exceeds authorized access."[53] The Fourth Circuit recently complicated the circuit split by aligning with the Ninth Circuit's narrow interpretation of the CFAA in *Nosal*, in contrast with the First, Fifth, Seventh, and Eleventh Circuits' broad interpretation.[54] The conflict particularly revolves around employer-employee relationships and confidential database misuse.[55] The meaning of the term "authorized" (or, put another way, "without or exceeds authorization") sits at the core of the disagreement.[56]

---

47. *Id.* at 864.
48. *Id.* at 860.
49. *Id.*
50. *Id.* at 865.
51. *Id.* at 866.
52. *See* Petition for Writ of Certiorari, *supra* note 4, at 6.
53. *Id.*
54. *Id.*
55. *See* Ryan Patrick Murray, *Myspace-ing Is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act*, 29 LOY. L.A. ENT. L. REV. 475, 480–81 (2009).
56. *See* Paul J. Larkin, Jr., United States v. Nosal*: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIR. REV. 257, 270–71 (2012).

A. Broad Interpretation: Employee Liability

The First,[57] Fifth,[58] Seventh,[59] and Eleventh[60] Circuits adopted a broad interpretation of the CFAA, which holds employees who are authorized to access a computer liable for using that access to steal or damage company data in violation of a computer-use policy.[61] The circuits that adopted a broad interpretation rely on one of two modes of analysis when defining the "without authorization" and "exceeds authorized access" language.[62] The first approach is based on a common law agency theory, and the second approach is based on mere violation of a computer use agreement and rooted in contract theory.[63] Under the broad interpretation, both modes of reasoning are employer-friendly and determine that "without authorization" and "exceeds authorized access" extend to misuse of information, rather than just the access to it.[64]

In *International Airport Centers, L.L.C. v. Citrin*,[65] the Seventh Circuit held that "an employee's authorization to access his employer's computer terminates when the employee uses the computer contrary to the employer's interests, thereby breaching his duty of loyalty to his employer" and violating the CFAA.[66] Citrin decided to start his own company, but before resigning, engaged in improper conduct by taking his employer's marketing data for corporate mergers and permanently deleted the employer's only copy of the files.[67] Applying an agency theory, the court reasoned that when Citrin breached his duty of loyalty, his authorization to access the employer's data terminated.[68] Therefore, Citrin had accessed the computer "without authorization," in violation of the CFAA.[69]

The First, Fifth, and Eleventh Circuits all recognize that an

57. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
58. United States v. John, 597 F.3d 263 (5th Cir. 2010).
59. Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).
60. United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).
61. Petition for Writ of Certiorari, *supra* note 4, at 8.
62. *Id.*
63. *See id.* at 10.
64. Pamela Taylor, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 203 (2012).
65. 440 F.3d 418 (7th Cir. 2006).
66. *Id.* at 420–21; *see* Petition for Writ of Certiorari, *supra* note 4, at 7.
67. Complaint at 4, Int'l Airport Centers LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (No. 03C 8104).
68. *Citrin*, 440 F.3d at 420–21.
69. *Id.*

employee's authority to access information is properly defined by a company's computer usage policy, and that violating such a policy can serve as a basis for holding an employee liable under the CFAA.[70] These circuits reason that "an employee 'exceeds authorized access' by violating employer-imposed restrictions on the purpose for which computer-stored information may be obtained."[71]

In *EF Cultural Travel BV v. Explorica, Inc.*,[72] the First Circuit held that an employment agreement can establish the parameters of "authorized" access.[73] There, as part of an employment agreement, the employee signed a broad confidentiality agreement that he violated when he attempted to "mine" his former employer's website.[74] The Fifth Circuit's holding in *United States v. John*[75] takes the First Circuit's reasoning a step further. There, the court summarized the First Circuit, stating that "an employment agreement can establish the parameters of 'authorized' access" and thus determined that "the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'"[76] The employee in *John* used her valid credentials to access company information, removed highly sensitive and confidential information, and ultimately used it to perpetrate fraud.[77] The Fifth Circuit found the employee accessed the information in violation of her employer's employee policies, and knew the purpose for accessing the information was not "authorized."[78] Thus, the employee was found to be in violation of the CFAA.[79] Lastly, in *United States v. Rodriguez*,[80] the Eleventh Circuit held that an employee exceeded authorized access when he violated the employer's policy by obtaining information for a non-business purpose.[81] Although the defendant did not use the information to further another crime, the court found a violation of the CFAA.[82]

70. Petition for Writ of Certiorari, *supra* note 4, at 9.
71. *Id.* at 9–10.
72. 274 F.3d 577 (1st Cir. 2001).
73. *Id.* at 581–82.
74. *Id.* at 582–83.
75. 597 F.3d 263 (5th Cir. 2010).
76. *Id.* at 272.
77. *Id.* at 271–72.
78. *Id.*
79. *Id.*
80. 628 F.3d 1258 (11th Cir. 2010).
81. *Id.* at 1265.
82. *Id.* at 1260.

The First, Fifth, Seventh, and Eleventh Circuits' broad definitions of "without authorization" and "exceeds authorized access" provide employers federal recourse against an employee for the misuse of electronic data.[83] Therefore, in these circuits, *any* violation of a company's computer-use policy invites civil *and* criminal liability to employees.[84]

B. Narrow Interpretation: Employers Beware

In *United States v. Nosal*, the Ninth Circuit held that the CFAA does not cover employee-hackers or insiders who take data from their employers and use it in an anticompetitive manner after leaving the company.[85] Three months later, the Fourth Circuit agreed with the Ninth Circuit in *WEC Carolina Energy Solutions LLC v. Miller*,[86] holding that the CFAA is not violated when a former employee who received authorization to obtain or alter data when he or she was employed later misuses that information.[87] The Fourth Circuit found that the CFAA prohibits only hacking and does not extend to misuse.[88]

Similar to the Ninth Circuit in *Nosal*, the Fourth Circuit in *WEC* adopted a narrow reading of the CFAA and held that the statute applies "only when an individual accesses a computer without permission or obtains and alters information on a computer beyond that which he is authorized to access."[89] There, a WEC employee took computer data in violation of corporate policy, resigned and started working for a competitor, and then used WEC's data to pitch a project to a customer.[90] The court reasoned that the CFAA's "without authorization" and "exceeds authorized access" language means that one cannot gain admission to a computer without approval or gain access to information outside the scope of approved

83. *See* Robert B. Milligan, *Computer Fraud and Abuse Act Circuit Split Remain Unresolved: United States Supreme Court Challenge Dismissed*, TRADING SECRETS (Jan. 7, 2013), http://www.tradesecretslaw.com/2013/01/articles/computer-fraud/computer-fraud-and-abuse-act-circuit-remains-unresolved/.

84. *See id.*

85. United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

86. 687 F.3d 199 (4th Cir. 2012).

87. *Id.* at 207.

88. *Id.* at 206.

89. *Id.*

90. *Id.* at 202.

access.[91] As a result, the court declined to extend the CFAA's scope to include the improper use of information that was *validly* accessed by the employee.[92] As the CFAA is a criminal and civil statute, the Fourth Circuit was concerned with extending the statute's reach to employees who simply failed to comply with a company's computer-use policies.[93]

The Ninth and Fourth Circuits' narrow interpretation of the CFAA holds that the statute prevents only hacking, or unauthorized access to a computer, and does not prohibit the misuse of such information.[94] The courts were concerned with extending a criminal statute to include any computer-use agreement violations, however trivial.[95] Thus, employers are limited in what claims can be brought against "rogue employees."[96]

V. CLEAR STANDARD: NARROW INTERPRETATION

The narrow interpretation of the CFAA articulated in *Nosal*, and recently supported by the Fourth Circuit, reserves the CFAA's principal purpose as an anti-hacking statute, not an expansive misappropriation statute.[97] Focusing on the plain language of the statute, and considering the "rule of lenity" and the goal of preventing suspected but not yet proven unauthorized access, a narrow interpretation is grounded in a sound analysis.[98] Additionally, employers prevented from bringing CFAA claims are not without recourse, as other legal remedies exist for misuse grievances.[99] As such, "without authorization" and "exceeds authorized access" should be construed narrowly, either by the Supreme Court or by Congress.

The *Nosal* court construed a limited definition of the terms "without authorization" and "exceeds authorized access."[100] Ultimately, the term "authorize," as used in "without authorization" or "exceeds authorized access," requires interpretation. The

91. *Id.* at 204.
92. *Id.* (emphasis added).
93. *Id.* at 205.
94. *See id.* at 207; United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).
95. *WEC*, 687 F.3d at 207.
96. *Id.*
97. *See Nosal*, 676 F.3d at 857.
98. *See id.* at 863.
99. *See WEC*, 687 F.3d at 207 n.4.
100. *See Nosal*, 676 F.3d at 863.

dictionary defines *authorize* as, "to grant official permission for or approval."[101] *Authorize*, then, must be read in conjunction with the meaning of *access*: "to gain admission to."[102] Therefore, an employer gives an employee permission to gain admission to a company computer when an employer "authorizes" the employee's "access." Thus, accessing a computer "without authorization" means to gain admission to it without permission.[103] Similarly, an employee "exceeds authorized access" by using her approved admission to the computer to obtain or alter information that falls outside the bounds of her approved access.[104] Both of these phrases deal with setting boundaries and exceeding them. The statute fails to mention misuse, and instead clearly addresses just the access of information.[105] Specifically, as the *WEC* court held, neither term extends "to the improper *use* of information validly accessed."[106] Instead, it is limited solely to the access.

In contrast, circuits applying the broad interpretation of the CFAA define "authorizes," in terms of state-law principals governing agency relationships.[107] Therefore, employer authorization hinges on whether an employee is acting in the best interest of the employer or, conversely, in violation of an employment agreement.[108] Thus, employment agreements and computer-use agreements drafted by employers arbitrarily determine when an employee either "exceeds authorized access" or uses a computer "without authorization," by being without authority at certain moments.[109]

Accordingly, employees are constantly accessing a computer without authorization and then potentially misusing information.[110]

101. RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2nd ed. 2001); WEBSTER'S THIRD INTERNATIONAL DICTIONARY 146 (2002).

102. RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2nd ed. 2001).

103. *See WEC*, 687 F.3d at 206.

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

105. *See id.*

106. *WEC*, 687 F.3d at 204.

107. *See* Larkin, *supra* note 56, at 272–273.

108. Matthew Kapitanyan, *Beyond Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 405, 423 (Winter 2012).

109. *See* Brief for Electronic Frontier Foundation as Amicus Curiae Supporting the Appellee and Urging Affirmance at 1617, United States v. Nosal, 642 F.3d 781 (No. 10-10038), 2010 WL 6191781.

110. Brian Zemil, *Federal Circuits Split on Computer Fraud and Abuse Act*, LITIGATION

Throughout a normal workday, employees can be found violating employee computer-use agreements, simply through routine behavior.[111] Employees perform personal, non-work related activities on corporate computers, from sending personal emails, to checking sports scores, to filling in the occasional sudoku.[112] What then qualifies as a breach of the agreement, resulting in a CFAA violation? The standard is arbitrary. If Congress wanted the statute to capture those who misuse information they are otherwise entitled to access, it would have done so clearly.[113] The *Nosal* court rightly held that it was implausible to think Congress intended to make a criminal law so expansive.[114] Instead, even if they have not settled on the narrow interpretation, the courts should read an ambiguous statute, as opposing viewpoints indicate, strictly.[115]

The narrow interpretation complies with the settled principle that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity."[116] The Supreme Court has held that a statute with both civil and criminal applications must be construed strictly.[117] Statutory interpretation applied for criminal prosecution will also be applied in a civil action.[118] If there is any doubt as to Congress' intentions, "the lowest common denominator must govern."[119] Therefore, if ambiguity exists, as it does, a narrow interpretation should prevail. A broad interpretation could make felons out of millions of unsuspecting people.[120] The CFAA could criminalize millions of employees for ordinary online behavior without being on notice of what conduct is criminally punishable.[121]

Furthermore, employees will be subject to the employer's

NEWS (Apr. 14, 2010), http://www.abanet.org/litigation/litigationnews/top_stories/041410-federal-circuit-computer-fraud-abuse.html.

111. *See Nosal*, 676 F.3d at 860.

112. *Id.*

113. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellee's Petition for Rehearing En Banc at 9–10, *Nosal*, 676 F.3d 854 (No. 10-10038), 2011 WL 2617475.

114. *See Nosal*, 676 F.3d at 862–63.

115. *See* Clark v. Martinez, 543 U.S. 371, 380 (2004).

116. *Nosal*, 676 F.3d at 863.

117. *Clark*, 543 U.S. at 380–81.

118. *See* Larkin, *supra* note 56, at 279.

119. *Clark*, 543 U.S. at 380.

120. *See* Larkin, *supra* note 56, at 270.

121. Brief of Amicus Curiae Electronic Frontier Foundation Supporting the Appellee and Urging Affirmance, *supra* note 109, at 17.

definition of a criminal statute. Allowing a broad interpretation of "authorize" delegates to a private party the power to define a federal criminal statute.[122] As the *Nosal* court observed, simply performing any personal, non-work-related activity serves to violate computer-use agreements.[123] Additionally, allowing the employer to define the criminal statute by defining "unauthorized access" in the computer use agreement leaves employees inadequately notified of what conduct is criminally punishable at any given time.[124] Employee agreements and computer-use policies, which are privately created, frequently go unread and may be altered without notice.[125] While minor misuse is far from stealing, a broad interpretation leaves the CFAA open to arbitrary enforcement and subject to violation by millions of employees on a daily basis.[126]

A narrow interpretation not only provides a clearer standard, but also is "in accord with the initial spirit and purpose of the CFAA."[127] As the court in *Nosal* found, "If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer-use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose."[128] Instead, the purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation.[129] Thus, the United States Supreme Court or Congress must take action to narrow private interpretation of the CFAA's scope.

VI. EMPLOYERS: IMPLEMENT PROTECTION

While a circuit split and uncertainty of the CFAA's scope continue to rage on, employers need to take protective steps in preserving their company data and potential CFAA claims.[130] Employers, especially in the Fourth and Ninth Circuits, need to take

122. *See* Murray, *supra* note 55, at 486.

123. United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012).

124. Brief of Amicus Curiae Electronic Frontier Foundation Supporting the Appellee and Urging Affirmance, *supra* note 109, at 15–16.

125. *Id.* at 16.

126. *See Nosal*, 676 F.3d at 863.

127. Greg Pollaro, iBrief, *Disloyal Computer Use and The Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, 23 (2010).

128. *Nosal*, 676 F.3d at 857.

129. *Id.*

130. *See* Milligan, *supra* note 83.

the necessary steps of establishing strict access guidelines and multiple levels of password protection.[131] While a narrow interpretation restricts employers' claims under the CFAA, understanding the Circuits' holdings allows for employers to position themselves to potentially preserve their federal claims, and to better protect their data.[132]

The first step is to establish strict access guidelines for employees.[133] While the Ninth and Fourth Circuits held that computer-use agreements do not define when an employee lacks authorization or exceeds authorized access, establishing clear access guidelines can only help the company in a practical sense and potentially strengthen CFAA claims.[134] Clarifying what access is permissible gives employees a better understanding of what constitutes a violation, and helps a company establish a framework for implementing protective measures.[135] With data theft steadily on the rise, rewriting access guidelines will force employers to address the access issue and devise protective measures that effectively prioritize different types of information.[136] Additionally, those jurisdictions that have not followed a narrow interpretation of the CFAA will have further ammunition in maintaining a CFAA claim.[137]

Once companies set more detailed access guidelines, they can implement more restrictive access with the use of multiple levels of passwords.[138] This extensive password-protection approach has been termed a "code-based" restriction by Professor Orin Kerr.[139] Under this approach, employers assign detailed clearance levels for employees on a strict need-to-know basis.[140] Employees will then only be able to access data necessary for particular responsibilities, limiting the risk of rogue employees retrieving confidential company

131. Taylor, *supra* note 64, at 226.

132. *See id.*

133. *See* Machado, *supra* note 3.

134. *See id.*; Taylor, *supra* note 64, at 227.

135. Carolyn M. Plump, *Can the Computer Fraud and Abuse Act Help Protect Your Business Data?*, LEGAL INTELLIGENCER (Dec. 9, 2009), http:www.law.com/jsp/pa/PubArticlePA.jsp?id=1202436184535.

136. *See* Machado, *supra* note 3; *Insider Data*, *supra* note 1.

137. *See* Machado, *supra* note 3.

138. *See* David Rosen, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access,"* 27 BERKELEY TECH. L.J. 737, 760 (2012).

139. Kerr, *supra* note 6, at 1572.

140. *See id.*

data.[141] Limited access allows employers to better monitor sensitive business information.[142] Furthermore, it will be clear when an employee accesses information "without authorization" or "exceeds authorized access."[143]

The ultimate goal is to curtail the ease of internal "hacking" and to protect sensitive business information.[144] Even though a narrow interpretation of the CFAA limits employers' federal judicial remedies, implementing restrictive-access measures strengthens data protection, possibly CFAA claims, and if nothing else, state law claims.[145]

VII. CONCLUSION

The Supreme Court recently dismissed a petition for Writ of Certiorari intended to address the circuit split, leaving CFAA's scope dependent on which federal court reviews the claim.[146] Additionally, contradictory legislation proposed in Congress fails to clarify the CFAA's scope.[147] Thus, the circuit split has no end in sight. The First, Fifth, Seventh and Eleventh Circuits broadly interpret the CFAA; the Fourth and Ninth Circuits interpret it narrowly. Yet, in terms of employer-employee relationships, a narrow interpretation should prevail and employers should prepare for a Supreme Court ruling confirming the Ninth Circuit's approach. The Ninth Circuit's holding in *United States v. Nosal* is grounded in sound judicial analysis and sets clear guidelines. Even though the conflict and widening circuit split rages on, employers need to take steps to protect sensitive business information in anticipation of a narrow ruling.

141. *See* Rosen, *supra* note 138, at 761.
142. *See* Larkin, *supra* note 56, at 283–84.
143. *See id.*; Rosen, *supra* note 138, at 760–61.
144. Machado, *supra* note 3.
145. *See* Milligan, *supra* note 83.
146. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012), *cert. denied*, 133 S. Ct. 831 (2013).
147. Milligan, *supra* note 83.