**Florida Law Review**

Volume 66 | Issue 4 Article 7

February 2015

# Misuse of Information Under the Computer Fraud and Abuse Act: On What Side of the Circuit Split Will the Second and Third Circuits Wind Up?

Robert D. Sowell

# MISUSE OF INFORMATION UNDER THE COMPUTER FRAUD AND ABUSE ACT: ON WHAT SIDE OF THE CIRCUIT SPLIT WILL THE SECOND AND THIRD CIRCUITS WIND UP?

Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610 (E.D. Pa. 2013)

JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514 (S.D.N.Y. 2013)

*Robert D. Sowell*[*]

The Computer Fraud and Abuse Act (CFAA) has reached a breaking point. The much-discussed issue is whether the CFAA provides a cause of action against persons who use electronic information in a way that violates a relevant computer-use policy.[1] Four circuit courts of appeals have held that the CFAA provides a cause of action for misuses of information, while two have disagreed.[2] In two undecided circuits, the district courts have favored the latter interpretation.[3] As the Supreme Court recently refused to address the issue,[4] these two undecided circuits will play a pivotal role in determining the direction of the CFAA.

By way of background, in 1984, the Ninety-Eighth Congress enacted the Comprehensive Crime Control Act (CCCA).[5] In § 2102 of the CCCA, Congress included the Counterfeit Access Device and Computer Fraud and Abuse Act, which was codified in § 1030 of Title 18 of the United States Code.[6] Shortly thereafter, Congress substantially amended § 1030 by way of the CFAA.[7] At that time, the CFAA focused primarily on criminalizing computer hacking.[8] Presently, the CFAA provides criminal[9] and civil liability[10] in § 1030(a)(2) for "[w]hoever . . . intentionally accesses a

---

* J.D. 2014, University of Florida Levin College of Law.

1. *See generally* Audra A. Dial & John M. Moye, *The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?*, 64 HASTINGS L.J. 1447, 1451–62 (2013) (discussing the background related to whether the CFAA reaches information misuses); Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, PITT. J. TECH. L. & POL'Y, Fall 2012, at 1, 5–14 (discussing the issue of interpreting the CFAA as well as judicial approaches to resolving that issue); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1572, 1583–87 (2010) (discussing interpretation of the CFAA and its relation to the void for vagueness doctrine).

2. *See infra* notes 13–16 and accompanying text.

3. *See infra* text accompanying notes 92, 106.

4. WEC Carolina Energy Solutions LLC v. Miller, 133 S. Ct. 831, 831 (2013) (denying certiorari).

5. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976.

6. *Id.* § 2102(a), 98 Stat. at 2190–92.

7. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1213–16.

8. *See infra* text accompanying notes 131–32.

9. 18 U.S.C. § 1030(a) (2012) ("Whoever—[listing acts under the CFAA] . . . shall be punished as provided in . . . this section.").

10. *Id.* § 1030(g) (providing a private right of action).

computer without authorization or exceeds authorized access."[11] In § 1030(a)(4), the CFAA reaches "[w]hoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access."[12] These two phrases, "without authorization" and "exceeds authorized access," are the crux of a major circuit split concerning whether the CFAA provides a cause of action against individuals who violate computer-use policies. Adhering to a "broad interpretation,"[13] some circuits have interpreted § 1030 to cover violations of use policies.[14] In contrast, following a "narrow interpretation,"[15] others have held that § 1030 deals only with "access" and does not provide a cause of action for violations of use policies.[16]

In practice, the question is frequently presented as whether an employee, previously given authorization to access an employer's computer, accesses "without authorization" or "exceeds authorized access" if that employee accesses an employer's computer for a wrongful purpose or misuses data after having logged on.[17] Fortunately, the CFAA provides some guidance by defining "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[18] However, the statute fails to define "without authorization."

Recently, two district courts addressed whether the CFAA reaches misuses of information.[19] Notably, neither of the district courts' respective circuit courts of appeals, the Second and Third Circuits, have addressed the issue.[20] An obvious question is whether the Second and Third Circuits will

11. *Id.* § 1030(a)(2).

12. *Id.* § 1030(a)(4). Additionally, § 1030(a)(1) also uses both the "without authorization" and "exceed[s] authorized access" language.

13. *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615–16 (E.D. Pa. 2013) (labeling the competing interpretations as the "broad view" and the "narrow view"); *id. passim* (using the terms "broad interpretation" and "narrow interpretation").

14. *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001).

15. *See* source cited *supra* note 13.

16. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

17. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1632–40 (2003) (discussing the CFAA's application "in the context of employee misconduct" and in cases of breaches of "contracts governing the use of computers").

18. 18 U.S.C. § 1030(e)(6) (2012).

19. *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 614–21 (E.D. Pa. 2013); JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 520–25 (S.D.N.Y. 2013).

20. *Dresser-Rand Co.*, 957 F. Supp. 2d at 616; *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 522.

decide the issue in the near future.[21] Another question is whether the Second and Third Circuits will interpret the CFAA narrowly or broadly. This Comment begins by discussing the relevant facts from each district court case. Next, this Comment delves into the circuit split and focuses on the reasoning behind the competing views. Finally, this Comment discusses the analysis in the district court opinions and explains why the district courts reached the correct result.

In the Second Circuit, the Southern District of New York grappled with the issue in March of 2013.[22] In *JBCHoldings NY, LLC v. Pakter*, a holding company acquired an executive search firm.[23] In doing so, the holding company employed a former owner of the acquired firm, and the former owner signed an employment agreement with the holding company.[24] According to the agreement, the former owner agreed "to help [the holding company] build [its] executive search business."[25] The employment agreement also provided that the former owner, as well as an additional owner of the search firm, would not compete with the holding company.[26]

Approximately six months after the former owner began working for the holding company, management for the holding company discovered personal e-mails of the former owner on a company computer.[27] The e-mails suggested that the former owner was directly competing with the holding company.[28] Specifically, according to the holding company, the former owner and several coconspirators "misappropriated . . . proprietary information, including client lists, and used these to advance their competing business."[29] The holding company theorized that the former owner "obtained this information either by (1) copying it to her personal laptop and sharing it with her co-[conspirators]; (2) lifting it from [the

21. The Second Circuit may, in fact, decide the issue soon. On January 24, 2014, Judge Covello of the District of Connecticut, in the Second Circuit, held that there was no cause of action under the CFAA against a former employee that downloaded confidential information in violation of the employer's computer-use policy. Amphenol Corp. v. Paul, Civil No. 3:12-cv-00543-AVC, 2014 WL 272337, at *8–9 (D. Conn. Jan. 24, 2014). On February 20, 2014, the employer filed a notice of appeal regarding Judge Covello's January 24th order. Notice of Appeal at 1, *Amphenol Corp.*, Civil No. 3:12-cv-00543-AVC (D. Conn. Feb. 20, 2014); *see also* Notice of Appeal at 1, *Amphenol Corp.*, Civil No. 14-547 (2d Cir. Feb. 20, 2014).

22. *See JBCHoldings NY, LLC*, 931 F. Supp. 2d at 520–27; *see also Amphenol Corp.*, 2014 WL 272337, at *8–9 (addressing the issue in January 2014); Targum v. Citrin Cooperman & Co., No. 12 Civ. 6909(SAS), 2013 WL 6087400, at *8 (S.D.N.Y. Nov. 19, 2013) (addressing the issue within the last year); Poller v. Bioscrip, Inc., No. 11 Civ. 1675(JPO), 2013 WL 5354753, at *22 (S.D.N.Y. Sept. 25, 2013 ) (same).

23. *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 518.

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.* at 519.

28. *Id.*

29. *Id.*

holding company's] computers using a flash drive; and/or (3) obtaining it remotely via spyware."[30] The holding company filed a complaint against the former owner and other coconspirators, alleging violations of the Computer Fraud and Abuse Act and the Lanham Act.[31] Thereafter, the former owner, as well as the other coconspirators, moved to dismiss.[32]

More recently, in the Third Circuit, the Eastern District of Pennsylvania addressed the issue in July of 2013.[33] In *Dresser-Rand Co. v. Jones*, two employees worked as managers at a company that "provide[d] technology, product [sic] and services used for developing energy and natural resources."[34] At that time, several company policies governed employee behavior.[35] One, the "Acceptable Use Policy," provided that "[a]ny unauthorized use, disclosure or transmission of [protected] information or content [was] prohibited."[36] The "Internet Access and Usage Policy" defined unauthorized Internet use as "[s]ending, receiving or posting without authorization company-sensitive or privileged information."[37] Each time that an employee logged onto a company computer, the employee was required to acknowledge a "Legal Notice and Acceptable Use Statement" that outlined additional computer-use rules.[38]

During the course of their employment with the plaintiff, the two employees began working for a new employer engaged in a similar business.[39] Before terminating their employment with the first company, the two employees violated computer-use policies when they downloaded company documents onto external hard drives, e-mailed company documents to their new employer, and deleted materials on company-provided computers.[40] Thereafter, the company filed a complaint against the two former employees for, among other claims, violations of the CFAA,[41] and the former employees moved for partial summary judgment as to the CFAA claims.[42]

Without guidance from the Second or Third Circuits, the Southern District of New York and Eastern District of Pennsylvania were left to their own devices in choosing which side of the circuit split to follow. On

30. *Id.*
31. *Id.*
32. *Id.* at 519–20.
33. *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 614–21 (E.D. Pa. 2013).
34. *Id.* at 611.
35. *Id.* at 612.
36. *Id.* (second alteration in original)
37. *Id.* (alteration in original).
38. *Id.* A "Code of Conduct" also covered "conflicts of interest, competition and fair dealing, confidentiality, privacy, protection and proper use of company assets, and other topics." *Id.*
39. *Id.* at 611.
40. *Id.* at 611–12.
41. *Id.* at 611.
42. *Id.* at 611–12.

one side, the First, Fifth, Seventh, and Eleventh Circuits have adhered to the broad interpretation and have held that violations of a computer-use policy can provide a basis for a CFAA cause of action.[43] These decisions approach the issue in two ways: a contract-based theory or an agency-based theory.[44]

The First, Fifth, and Eleventh Circuits employ the contract-based theory whereby the breach of the policy itself triggers CFAA liability.[45] In *United States v. Rodriguez*, the Social Security Administration (SSA) maintained electronic databases that included sensitive personal information such as social security numbers, addresses, dates of birth, and annual income.[46] The SSA established computer-use policies prohibiting an employee from accessing the database for nonbusiness reasons.[47] When an SSA employee accessed the personal information of seventeen individuals for personal reasons, the employee was charged with violating the CFAA.[48] The Eleventh Circuit determined that, according to the policy, the employee's authorization to access varied depending on his purpose.[49] Following a cursory analysis, the court held that, by violating the SSA's computer-use policies, the employee "exceeded his authorized access" in violation of the CFAA.[50]

Similarly, the Fifth Circuit interpreted the statute broadly and held that a bank employee "exceed[ed] authorized access" when she provided a relative with confidential customer account information in violation of the bank's computer-use policies.[51] The First Circuit, reviewing a motion for preliminary injunction, held that a company would "likely prove that"[52] a former employee "exceed[ed] authorized access"[53] by accessing the company's website in a way that violated a confidentiality agreement between the company and former employee.[54]

---

43. *See supra* note 14.

44. *See* Goldman, *supra* note 1, at 5–9.

45. *See* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010); United States v. John, 597 F.3d 263, 271–73 (5th Cir. 2010); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001).

46. *Rodriguez*, 628 F.3d at 1260.

47. *Id.*

48. *Id.* at 1260, 1262.

49. *Id.* at 1263.

50. *Id.* at 1263, 1265.

51. United States v. John, 597 F.3d 263, 272–73 (5th Cir. 2010).

52. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).

53. *Id.* at 581 (alteration in original) (internal quotation marks omitted).

54. *Id.* at 581–83. In *EF Cultural Travel*, the former employee signed a confidentiality agreement with the company providing that the "[e]mployee agree[d] to maintain in strict confidence and not to disclose to any third party . . . any Confidential or Proprietary Information." *Id.* at 582. In conjunction with a third party, the former employee used that confidential information to develop a computer program to extract proprietary pricing information from the company's website. *Id.* at 579. The former employee would then use the extracted data to undercut the

In contrast, the Seventh Circuit employs an agency-law theory to justify a broad interpretation.[55] In *International Airport Centers, L.L.C. v. Citrin*, an employee decided to terminate his employment.[56] Before returning a company-issued laptop, the employee deleted all the data in the laptop and installed a "secure-erasure program" to prevent the data from being recovered.[57] Judge Richard Posner determined that the employee accessed the laptop "without authorization" after acquiring an interest adverse to the company.[58] According to this theory, the agency relationship between the principal-employer and agent-employee was the basis for the employee's authorization to access the laptop.[59] The employee breached his fiduciary duty to the company by resolving to quit and destroying the files within the laptop.[60] That breach resulted in a termination of the agency relationship.[61] Thereafter, the employee accessed the laptop without authorization by using it after the agency relationship had ended.[62]

On the other side of the circuit split, the Fourth and Ninth Circuits interpret the CFAA narrowly and hold that violations of computer-use policies do not provide a basis for a CFAA cause of action.[63] In this camp, the Fourth Circuit recently affirmed a decision from the District of South Carolina that granted a Rule 12(b)(6) motion to dismiss for failure to state a claim under the CFAA.[64] In *WEC Carolina Energy Solutions LLC v. Miller*, a company provided an employee with a laptop, cell phone, and authorization to access "the company's intranet and computer servers."[65] According to the company, the employee, while working for the company, violated company policies by "download[ing] confidential and proprietary

company's price scheme. *Id.* at 580. According to the court, the former employee likely "exceeded authorized access" "by providing proprietary information and know-how to [the third party] to create the [computer program]." *Id.* at 583. In sum, "[t]he website was open to the public, so he was authorized to use it, but he exceeded his authorization by using confidential information to obtain better access than other members of the public." Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (discussing the holding in *EF Cultural Travel*).

55. *See Citrin*, 440 F.3d at 420–21. The Seventh Circuit is the only circuit court of appeals that has employed this theory, and both the Ninth and Fourth Circuits expressly rejected the agency-based theory. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc).

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

57. *Id.*

58. *Id.* at 420–21.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

64. *WEC Carolina Energy Solutions LLC*, 687 F.3d at 201.

65. *Id.* at 202.

information to a personal computer" and then using the information to successfully procure projects for a subsequent employer.[66]

Reviewing the district court's dismissal of the company's CFAA claims, the Fourth Circuit narrowed the issue to whether an employee that violates a computer-use policy accesses "without authorization" or "exceeds authorized access."[67] The unanimous panel held that an employee "accesses a computer 'without authorization' when he gains admission to a computer without approval."[68] In contrast, "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."[69] Applying the rule of lenity,[70] the court construed the CFAA narrowly and held that the CFAA only addresses "individuals who *access* computers without authorization or who obtain or alter information beyond the bounds of their authorized access."[71]

The Fourth Circuit relied heavily on borrowed reasoning from the Ninth Circuit's en banc decision in *United States v. Nosal*.[72] In *Nosal*, a former employee solicited a company's current employees to use "their log-in credentials to download source lists, names and contact information from a confidential database on the company's computer, and then transfer[] that information to" the former employee.[73] Because that conduct violated the company's computer-use policies, the government charged the former employee with violating the CFAA.[74] The former employee moved to dismiss, and the district court granted the motion.[75]

---

66. *Id.* (internal quotation marks omitted). Additionally, the company alleged that the employee "downloaded a substantial number of [the company's] confidential documents and emailed them to his personal e-mail address." *Id.* (internal quotation marks omitted).

67. *Id.* at 203.

68. *Id.* at 204. Specifically, the court defined "'authorization' as [a] 'formal warrant, or sanction.'" *Id.* (citing THE OXFORD ENGLISH DICTIONARY 798 (2d ed. 1989)). Accordingly, "an employee is *authorized* to access a computer when his employer approves or sanctions his admission to that computer." *Id.* (emphasis added).

69. *Id.*

70. *Id.* at 205–06. The rule of lenity requires that ambiguous criminal statutes be strictly construed in favor of the criminal defendant. United States v. Lanier, 520 U.S. 259, 266 (1997). Where a statute has both criminal and civil applications, the rule of lenity applies in the civil context as well. Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004).

71. *WEC Carolina Energy Solutions LLC*, 687 F.3d at 207 (emphasis added).

72. *Id.* at 203, 205.

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

74. *Id.* Specifically, the government charged the former employee with aiding and abetting the current employees in "'exceed[ing their] authorized access' with intent to defraud." *Id.* (alteration in original).

75. *Id.* After initially denying the motion to dismiss, the district court granted the motion on reconsideration, following the Ninth Circuit's decision in *LVRC Holdings LLC v. Brekka*. *Id.* Decided in 2009, *Brekka* is a precursor to *Nosal*. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009). In *Brekka*, the Ninth Circuit held that there is no cause of action under the CFAA against an individual for sending personal e-mails containing company documents in violation of

The initial panel reversed.[76] However, on rehearing en banc, the Ninth Circuit affirmed the district court.[77] To begin, the court looked to the legislative history to determine that "without authorization" refers to traditional "*outside* hackers," while "exceeds authorized access" covers "*inside* hackers."[78] Accordingly, inside hackers are "individuals whose initial access to a computer is authorized but who [thereafter] access unauthorized information or files."[79] The court also posited several extreme examples that would follow from a broad interpretation.[80] One example was where a company's computer-use policy prohibits using a company computer for personal use, an employee could call a family member from a work phone but could be criminally prosecuted if the employee instead sends an e-mail.[81] Therefore, the en banc court interpreted the statute narrowly and held that the CFAA does not reach violations of computer-use policies.[82]

Both Judge Paul Engelmayer of the Southern District of New York and Judge Anita Brody of the Eastern District of Pennsylvania were persuaded by the reasoning of the Fourth and Ninth Circuits.[83] In *JBCHoldings NY, LLC*, the company's CFAA cause of action hinged on a violation of an employment agreement between the company and the former owner of the acquired executive search firm.[84] Judge Engelmayer determined that the issue was "whether an employee acts 'without authorization' or 'exceeds authorized access' when that employee is authorized in the first instance to access certain information, but then uses that information for an improper purpose."[85] Stated narrowly, the issue was "whether an employee's *misuse* of an employer's information violates the CFAA where that information

---

the company's computer-use policy. *Id.* at 1135. The decision largely focused on the "without authorization" language and held that that language does not reach an individual's misuse of information. *Id.* at 1132–35.

76. United States v. Nosal, 642 F.3d 781, 789 (9th Cir. 2011), *rev'd*, 676 F.3d 854 (9th Cir. 2012) (en banc). The initial panel construed the term "so" within the definition of "exceeds authorized access" to mean "in that manner." *Id.* at 785–86. In that sense, the CFAA would define "'exceeds authorized access'" to mean "'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 [*in that manner*] to obtain or alter.'" *Id.* at 785 (quoting 18 U.S.C. § 1030(e)(6) (2012)). According to the panel, by qualifying the *way* in which an individual accesses a computer, the CFAA reaches violations of computer-use policies. *Id.* at 786.

77. *Nosal*, 676 F.3d at 864.

78. *Id.* at 858.

79. *Id.*

80. *Id.* at 860.

81. *Id.* As another example, an employee could surreptitiously read a newspaper at work but would risk criminal sanctions if the employee instead visited a news website. *Id.*

82. *Id.* at 863–64.

83. *See* JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 522–23 (S.D.N.Y. 2013); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 616–18 (E.D. Pa. 2013).

84. *See supra* text accompanying notes 22–32.

85. *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 521.

was obtained from a computer to which the employee was permitted access."[86]

After briefly outlining the circuit split, the court noted that, even within the Southern District of New York, interpretations of the CFAA varied.[87] As to the text, the court distinguished between access and use.[88] In that vein, the court concluded that authorization to access cannot vary depending on one's purpose.[89] Rather, should an individual violate a policy after having permissibly accessed a computer, that conduct would simply be a misuse of that information.[90] Summarily stated, "[a]n employee acts 'without authorization' when he accesses a computer without permission to do so; an employee 'exceeds authorized access' when he has permission to access certain information on a computer, but accesses other information as to which he lacks permission."[91] Therefore, consistent with the narrow interpretation, the court held that the CFAA does not cover violations of computer-use policies.[92]

While the court explicitly refused to declare the statute ambiguous, it did note that even if the statute were ambiguous, the rule of lenity would necessitate the same narrow construction.[93] To be sure, "if Congress seeks to make a federal crime out of an employee's misuse of his work computer, it is required to say so clearly."[94]

Addressing the motion to dismiss, the court turned to the amended complaint.[95] According to the allegations therein, the former owner

86. *Id.*

87. *Id.* at 522. Specifically, the court cited four decisions interpreting the CFAA narrowly. *Id.* (citing Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ. 9505(ALC)(DCF), 2013 WL 410873, at *7 (S.D.N.Y. Jan. 30, 2013); United States v. Aleynikov, 737 F. Supp. 2d 173, 190–94 (S.D.N.Y. 2010); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 384–86 (S.D.N.Y. 2010); Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 383–84 (S.D.N.Y. 2010)). In contrast, the court cited three other decisions within the Southern District of New York interpreting the CFAA broadly. *Id.* (citing Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *6–7 (S.D.N.Y. May 18, 2010); Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252–53 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004)).

88. *Id.* at 522–23.

89. *Id.* at 523. According to the court, to allow "authorization" to vary depending on one's purpose would impose a subjective element into the CFAA that was not intended by the enacting Congress. *Id.*

90. *Id.*

91. *Id.*

92. *Id.* at 523, 525 (concluding that the CFAA does not address "the circumstance where an employee has permission to access certain information and then uses that information for an improper purpose" and that Congress did not intend the CFAA to expand federal jurisdiction over such acts).

93. *Id.* at 524.

94. *Id.*

95. *Id.* at 525.

acquired the holding company's "client lists and other proprietary information and used that information to set up a competing enterprise," in violation of the holding company's "electronic media policy."[96] Applying a narrow interpretation, the court noted that the amended complaint did not allege that the former owner "lacked the authority to access th[e] information."[97] Accordingly, the holding company failed to state a claim upon which relief could be granted.[98] Specifically, "such misuse does not state a claim under the CFAA, because an employee does not 'exceed[] authorized access' or act 'without authorization' when she misuses information to which she otherwise had access."[99]

In *Dresser-Rand Co.*, the company's CFAA claim centered on two employees' violations of several computer-use polices.[100] Judge Brody began her analysis with a discussion of the legislative history of the CFAA.[101] Particularly, the court cited a pre-CFAA committee report that discussed § 1030 as addressing "breaking and entering" or trespass-type crimes.[102] Notably, that type of conduct has little to do with misuse; it has everything to do with access or hacking. Aside from the legislative history, the court narrowed its focus to whether the two employees "exceed[ed] authorized access" when they violated the company's computer-use policies.[103] As to the text, the court relied almost exclusively on the Fourth and Ninth Circuits in reasoning that the plain meaning of the CFAA and the rule of lenity[104] necessitate a narrow interpretation.[105] The court then rejected the opposing case law as "wrap[ping] the *intent* of the employees and *use* of the information into the CFAA despite the fact that the statute narrowly governs access, not use."[106]

Applying the narrow interpretation, the court noted that the company had provided the two employees with "user names and passwords to

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.* (alteration in original). The court did note that the amended complaint included allegations that "someone . . . placed a flash memory drive on [the holding company's] computer servers . . . in an effort to surreptitiously rip information from the drives." *Id.* at 525–26 (ellipsis in original) (internal quotation marks omitted). Had those allegations been pleaded with the requisite specificity, then those allegations may have sufficed to state a claim under the CFAA. *Id.*

100. Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 611–12 (E.D. Pa. 2013).

101. *Id.* 613–14.

102. *Id.* at 613 (citing H.R. REP. NO. 98-894, at 20 (1984) (internal quotation marks omitted)).

103. *Id.* at 615 (alteration in original) (internal quotation marks omitted).

104. Generally, before the rule of lenity applies, the court must declare that the statute is ambiguous. LINDA D. JELLUM & DAVID CHARLES HRICIK, MODERN STATUTORY INTERPRETATION 151 (2d ed. 2009) (noting that the rule of lenity "is generally applied only when the statute at issue is both penal in nature *and ambiguous*" (emphasis added to last word)); *see also id.* at 476–77 (discussing the relationship between ambiguity and the rule of lenity).

105. *Dresser-Rand Co.*, 957 F. Supp. 2d at 615–19.

106. *Id.* at 619 (emphasis added).

access" the company's network and database.[107] Additionally, the company provided the employees with laptops.[108] According to the court, if the employees "were authorized to access their work laptops and to download files from them, they cannot be liable under the CFAA even if they subsequently misused those documents to compete against" the company.[109] For that reason, even though the employees used the company's information for competitive purposes, the court granted the employees' motion for partial summary judgment on the company's CFAA claims.[110] Consequently, relief for the company would have to come in the form of a non-CFAA cause of action.[111]

Today, a major question surrounding the CFAA is whether the Southern District of New York and the Eastern District of Pennsylvania reached the correct result. The interpretation adopted by *JBCHoldings*, that the text of the CFAA unambiguously favors a narrow interpretation, appears unfairly dismissive.[112] In fact, the existence of the circuit split suggests otherwise. Regarding *Dresser-Rand Co.*, by relying mostly on case law, it is unclear whether the text, legislative history, or both require a narrow interpretation.[113] As to both cases, a better approach would be to recognize the ambiguity and apply the rule of lenity, as well as consult the legislative history, to reach the same conclusion. Under either approach, the CFAA does not provide a cause of action for violations of a computer-use policy.

Beginning with the text, as noted above, the CFAA provides a cause of action against individuals who access "without authorization" or "exceed[] authorized access."[114] Statutory text may be deemed "ambiguous" if "two or more reasonable people disagree as to its meaning."[115] Because reasonable minds can differ as to the meaning of "without authorization" and "exceeds authorized access," those phrases are ambiguous.

As to the "without authorization" language, the crux of that phrase lies in the definition of "authorization." Authorization can be defined as "the state of being authorized,"[116] and "authorize" can mean "to endorse,

107. *Id.* at 620.

108. *Id.*

109. *Id.*

110. *Id.* at 621.

111. *Id.*

112. *See supra* text accompanying notes 93–94.

113. *See supra* notes 101–06 and accompanying text.

114. *See supra* text accompanying notes 11–12.

115. JELLUM & HRICIK, *supra* note 104, at 94 ("Most courts state that statutes are ambiguous when two or more reasonable people disagree as to its meaning."). *But cf.* Chickasaw Nation v. United States, 534 U.S. 84, 94 (2001) (emphasis added) (defining ambiguity as where a "statute is '*fairly capable*' of two interpretations"); Mayor of Lansing v. Mich. Pub. Serv. Comm'n, 680 N.W.2d 840, 847 (Mich. 2004) ("[A] provision of the law is ambiguous only if it 'irreconcilably conflict[s]' with another provision or when it is *equally susceptible* to more than a single meaning." (second emphasis added) (citation omitted)).

116. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 146 (1993).

empower, justify, or permit by . . . some recognized or proper authority."[117] Under the broad interpretation of the CFAA, one may argue that "authorization" to access can vary depending on the accesser's purpose.[118] Under that approach, an employer may authorize an employee to access the employer's database for business purposes; however, that same employer may deny authorization to access for personal purposes. In contrast, under a narrow reading of the CFAA, one may argue that "authorization" to access must be unqualified, and any violation of a policy after having accessed under the employer's authorization is merely a misuse of information and not a violation of the CFAA.[119] Here, an employee who receives a username and password is presumptively authorized to access the employer's database; however, if that employee then impermissibly downloads or misappropriates employer information, that employee merely misuses the information. Regardless, "authorization" is at least capable of two reasonable interpretations,[120] and therefore the term is ambiguous.[121]

As to the "exceeds authorized access" language, the question is more difficult. The CFAA defines the phrase in § 1030(e)(6) as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[122] Under a broad interpretation of the CFAA, one may argue that impermissible "obtain[ing] or alter[ing]" is equivalent to misuse.[123] In contrast, under a narrow interpretation, the definition of "exceeds authorized access" only covers "insider hacking,"[124] wherein an individual, after having permissibly accessed a database, "accesses other information as to which he lacks permission."[125] In this sense, "entitled" would be

117. *Id.*; *see also* United States v. Aleynikov, 737 F. Supp. 2d 173, 191 (S.D.N.Y. 2010) (discussing several dictionary definitions of "authorize").

118. *See supra* text accompanying note 49; *see also* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) ("Access to a computer and data that can be obtained from that access may be exceeded if the *purposes* for which access has been given are exceeded." (emphasis added)).

119. *See supra* text accompanying notes 85–86, 89–90.

120. *Cf. supra* note 115 (discussing competing standards for determining ambiguity).

121. *But see* JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 524 (S.D.N.Y. 2013) (refusing to declare the CFAA ambiguous).

122. 18 U.S.C. § 1030(e)(6) (2012).

123. One could also argue that the term "so" should be construed to mean "in that manner." *See* United States v. Nosal, 642 F.3d 781, 785–86 (9th Cir. 2011), *rev'd*, 676 F.3d 854 (9th Cir. 2012) (en banc). In that vein, "exceeds authorized access" would refer to the way in which information is "obtain[ed] or alter[ed]" which speaks to using (not accessing) information. *Id.*

124. *See supra* text accompanying note 79.

125. *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 523. For example, an employee, with a username and password, would "exceed[] authorized access" if that employee, after permissibly accessing the employer's network, hacked into another employee's e-mail account or into a password-protected folder.

synonymous with "authorized,"[126] and "*entitled* so to obtain or alter" may simply refer to whether an individual is permitted to access the information.[127] However, again, both interpretations seem reasonable, and the statute is therefore ambiguous.

Declaring the CFAA ambiguous is a critical determination in interpreting the statute narrowly. For one, the rule of lenity will apply, requiring courts to strictly construe the CFAA in favor of the defendant.[128] Significantly, the rule of lenity will apply even in civil applications of the CFAA.[129] Additionally, because the statute is ambiguous, courts will more readily consult the legislative history,[130] and the legislative history seems to conclusively favor a narrow interpretation.

Looking back to the Counterfeit Access Device and Computer Fraud Abuse Act of 1984, wherein 18 U.S.C. § 1030 was originally enacted, the House Judiciary Committee expressed its concern for "so-called 'hackers' who have been able to access (trespass into) both private and public systems."[131] In all, the report from House Judiciary Committee mentioned some derivation of the word "hack" seven times.[132] The Committee was especially blunt in stating that "[i]t is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere *use* of a computer."[133]

Just two years later, Congress enacted the CFAA.[134] Here, Congress established the "exceeds authorized access" language.[135] By including "exceeds authorized access" in § 1030(a) and defining that phrase in § 1030(e)(6), Congress removed the prior language from § 1030(a) that covered individuals who "having accessed a computer with authorization, use[] the opportunity such access provides for purposes to which such

126. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (en banc) ("An equally or more sensible reading of 'entitled' is as a synonym for 'authorized.'").

127. *JBCHoldings NY, LLC*, 931 F. Supp. at 523 ("[A]n employee 'exceeds authorized access' when he has permission to access certain information on a computer, but accesses other information as to which he lacks permission.").

128. *See supra* notes 70–71, 104, 114 and accompanying text.

129. *See supra* note 70.

130. *See* Mayor of Lansing v. Mich. Pub. Serv. Comm'n, 680 N.W.2d 840, 846 (Mich. 2004) ("A finding of ambiguity, of course, enables an appellate judge to bypass traditional approaches to interpretation and . . . engage in a largely subjective and perambulatory reading of 'legislative history.'"); *cf.* Martin H. Redish & Matthew B. Arnould, *Judicial Review, Constitutional Interpretation, and the Democratic Dilemma: Proposing a "Controlled Activism" Alternative*, 64 FLA. L. REV. 1485, 1525 (2012) (noting the plain meaning rule "dictates that when words are linguistically *unambiguous*, an interpreter may *not* resort to external sources to contradict the inexorable implications of that unambiguous meaning" (emphasis added)).

131. H.R. REP. NO. 98-894, at 10 (1984).

132. *Id.* at 10–11, 21.

133. *Id.* at 20 (emphasis added).

134. *See supra* note 7.

135. *See supra* text accompanying notes 11–12.

authorization does not extend."[136] In its report, the Senate Judiciary Committee illustrated its understanding of "exceeds authorized access."[137] The Committee noted that an employee might "exceed[] authorized access" if "while authorized to use a particular computer in one department, [he] briefly exceeds his authorized access and peruses data belonging to [a] department that he is not supposed to look at."[138] The Committee referred to the "exceeds authorized access" language as covering "insider cases,"[139] much like the Ninth Circuit referred to "insider hacking."[140]

It should be noted that the report from the Senate Judiciary Committee accompanying the 1996 amendment hints that misuses of information may be covered by the CFAA. Specifically, in discussing the penalties for violating § 1030(a)(2)(C), the report mentions that the CFAA covers "misusing information," as well as theft-related issues.[141] Without more, theft of information seems like a misuse issue, not an access issue. But, the Committee clarified that "[t]he crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information."[142] Therefore, the CFAA does not cover the actual offense; rather, it covers the unauthorized access that precedes the offense.[143]

Pending legislation also seeks to narrow the reach of the CFAA by removing the "exceeds authorized access" language and defining "access without authorization" to include only access, and not use.[144] This proposed amendment could indicate that Congress understands the current language to be broad; therefore, Congress wishes to alter the plain meaning. In contrast, the amendment could indicate that Congress understands the text to be narrow; however, Congress nonetheless wishes

136. *See* S. REP. NO. 99-432, at 9 (1986).

137. *See id.* at 7. Here, the Committee was discussing whether to include the "exceeds authorized access" language in § 1030(a)(3). *Id.* While the Committee ultimately decided to exclude that language from (a)(3), *id.*, "exceeds authorized access" can be found in §§ 1030(a)(1), (a)(2), and (a)(4).

138. *Id.*

139. *Id.* at 7–8 (internal quotation marks omitted).

140. *See supra* text accompanying note 78–79.

141. S. REP. NO. 104-357, at 7–8 (1996).

142. *Id.*

143. These statements are found in a broader discussion of what is meant by "obtaining information" within the definition of "exceeds authorized access." *Id.* The Committee noted that "obtain[]" only includes "mere observation." *Id.* at 7 (quoting S. REP. NO. 99-432 at 6–7 (1986)). In that sense, "obtain" is akin to "access," i.e., an individual "obtains" a file by merely accessing that file.

144. *See* Aaron's Law Act of 2013, S. 1196, 113th Cong. § 2; Aaron's Law Act of 2013, H.R. 2454, 113th Cong. § 2; *see also* Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (Mar. 5, 2014, 9:30 PM), http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/ (discussing CFAA's flaws and whether Aaron's Law will improve the CFAA).

to add clarity to combat prosecutorial abuse. While the pending legislation provides little guidance on that point, the weight of the legislative history indicates that the CFAA prohibits only unauthorized access, not unauthorized use.[145]

Thus, the Southern District of New York in *JBCHoldings NY, LLC* and the Eastern District of Pennsylvania in *Dresser-Rand Co.* correctly interpreted the CFAA narrowly. Whereas these two decisions reach the correct result, each court's rationale leaves something to be desired. In addressing whether the CFAA provides a cause of action for misuses of information, a better method would be to declare the statute ambiguous. Because the CFAA is ambiguous, courts will more readily consult the legislative history that favors a narrow interpretation. Where that much is unclear, the rule of lenity will require that courts interpret the CFAA narrowly in favor of a criminal or civil defendant.

Therefore, when the issue inevitably reaches the Second and Third Circuits, those courts should interpret the CFAA narrowly and hold that there is no cause of action under the CFAA for misusing electronic information. Additionally, in light of a recent trend favoring a narrow interpretation,[146] the Second and Third Circuits will likely follow suit. Soon enough, in both New York and Philadelphia, there will be no cause of action under the CFAA for violating a computer-use policy.

145. *See supra* text accompanying notes 78–79, 82, 101–02.

146. *See* Thomas E. Booms, Note, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 565–67 (2011) (discussing the trend favoring a narrow interpretation in both the Second and Third Circuits); *see also supra* notes 20–21 and accompanying text (noting that neither the Second nor Third Circuit has addressed whether the narrow interpretation should control at the appellate level and that the Second Circuit may soon address the issue).