Catholic University Law Review

Volume 63
Issue 1 *Fall 2013*

Article 7

4-2014

Finding the Solution in WEC Carolina Energy Solutions: The Computer Fraud and Abuse Act in the Workplace

Emily V. Malone

Finding the Solution in WEC Carolina Energy Solutions: The Computer Fraud and Abuse Act in the Workplace

Cover Page Footnote

J.D. Candidate, May 2014, The Catholic University of America, Columbus School of Law; B.A., 2010, The University of North Carolina at Chapel Hill. The author wishes to thank Professor Carlisle for his invaluable expertise and guidance. The author also wishes to thank her friends and family for their constant love and support. Finally, the author would like to thank her colleagues on the Catholic University Law Review for their time and effort spent working on this Note.

FINDING THE SOLUTION IN WEC CAROLINA ENERGY SOLUTIONS: THE COMPUTER FRAUD AND ABUSE ACT IN THE WORKPLACE

By: Emily V. Malone[+]

Have you ever checked the score of last night's game from your office computer or taken an unauthorized break from work to search online to see if those new boots have gone on sale? Such innocent actions may be federal crimes under the broad interpretations of the Computer Fraud and Abuse Act (CFAA) adopted by three federal circuit courts.[1] Chief Judge Kozinski, of the Ninth Circuit, argued that broadly interpreting the CFAA would

> transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.[2]

[+] J.D. Candidate, May 2014, The Catholic University of America, Columbus School of Law; B.A., 2010, The University of North Carolina at Chapel Hill. The author wishes to thank Professor Carlisle for his invaluable expertise and guidance. The author also wishes to thank her friends and family for their constant love and support. Finally, the author would like to thank her colleagues on the Catholic University Law Review for their time and effort spent working on this Note.

1. *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (concluding that the defendant violated the CFAA by exceeding his authorized access to certain databases when he used the database for personal use); United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010) (finding that the defendant violated the CFAA under an intended-use theory when she used information obtained through her work computer as part of a fraudulent scheme), *cert. denied*, 133 S. Ct. 1237 (2013); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (applying agency theory and concluding that an employer's CFAA-based suit against its former employee for destroying files in breach of his duty of loyalty to the employer should be reinstated).

2. United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (referencing reading the CFAA's language to encompass violations of private computer use policies as grounds for criminal liability).

Congress created the CFAA as an anti-hacking statute to prosecute people who broke into computer systems without authorization.[3] The statute has undergone many changes since its inception in 1986 and now serves as the basis for bringing both criminal charges and civil actions for employee misconduct.[4] In today's technologically-advanced world, courts have broadly interpreted the CFAA's language, which has led to potentially disastrous unintended consequences.[5]

According to the U.S. Census Bureau, only 8.2% of households had personal computers in 1984[6]—the year that Congress enacted the first federal legislation criminalizing certain computer-related activity.[7] Today however, computers are an integral part of everyday American life.[8] As computer use becomes inextricably entwined with household, governmental, and commercial operations, the potential for digital crimes drastically increases and expands in scope, which, in turn, renders CFAA applicability practically boundless.[9]

Recently, the CFAA has been applied in the workplace setting to punish employee wrongdoing involving company computers, databases, and other electronically-stored information.[10] Federal circuit courts disagree over the most

---

3. *See* Pamela Taylor, Comment, *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, 207 (2012); Obie Okuh, Comment, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637, 645–46 (2011) (noting that CFAA was passed in response to concerns over computer-based crimes, which negatively affect commerce).

4. *See infra* Parts I.A.1–3.

5. *See* Taylor, *supra* note 3, at 220–26 (advancing a narrow interpretation of the CFAA and, rejecting broader interpretations as potentially rendering the CFAA unconstitutionally void); Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1548 (2012) (explaining that although the statute, as initially conceived, was "modest," the expansion of the computer industry has allowed the CFAA to "grow[] into a multi-faceted tool with a potentially limitless scope").

6. *Computer and Internet Use in the United States*, U.S. CENSUS BUREAU, *available at* http://www.census.gov/hhes/computer/ (last visited Jan. 09, 2014).

7. Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455 (1990); *see also* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 1837, 2190-92 (codified as amended at 18 U.S.C. § 1030 (2006)) [hereinafter the 1984 Act]. The 1984 Act has transformed into what we know today as the CFAA. *See infra* Part I.A.2–3.

8. United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc). The U.S. Census Bureau estimates that 75.6% of households had a computer in 2011, and 71.7% of households accessed the Internet in the same year, whereas in 1984 only 8.2% of households had computer and Internet usage was not even measured. *Computer and Internet Use in the United States*, *supra* note 6.

9. Hernacki, *supra* note 5, at 1548 (arguing that the scope of the CFAA, in the world we live in today, could have drastic effects that were not properly understood during its initial enactment).

10. *See, e.g.*, WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 202, 207 (4th Cir. 2012) (affirming the dismissal of a complaint for failure to state a claim under the CFAA), *cert. dismissed*, 133 S. Ct. 831 (2013); *Nosal*, 676 F.3d at 856; United States v. Rodriguez, 628 F.3d 1258, 1260–62 (11th Cir. 2010); United States v. John, 597 F.3d 263, 269–70 (5th Cir. 2010);

accurate way to interpret the CFAA in this scenario, with each court basing their disparate approaches on each court's interpretation of the CFAA's authorization language.[11] Three theories interpreting this statutory language have emerged: the agency theory,[12] the intended-use theory,[13] and the access means access theory.[14] The agency theory and the intended-use theory both broadly construe the CFAA's authorization language.[15] However, the agency theory bases violations of the CFAA on an employee's breach of loyalty to the company,[16] whereas the intended-use theory bases violations on the employer's computer-use policies.[17] The access means access theory offers the narrowest interpretation of the CFAA because it restricts violations to actual access of company information without authorization.[18]

This Note discusses and endorses the Fourth Circuit's conclusion in *WEC Carolina Energy Solutions LLC v. Miller* that the authorization language of the CFAA should be narrowly interpreted. Part I examines the CFAA, focusing on the authorization language, and traces the development of important amendments to the Act. Part II analyzes the three approaches taken by federal circuit courts: agency theory, intended use theory, and access means access theory. Part III scrutinizes the Fourth Circuit case, *WEC Carolina Energy Solutions*, and argues that it extends the federal appellate courts' trend by adopting the narrow view of the CFAA. *WEC Carolina Energy Solutions* will

---

LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir. 2009); Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

11. *See infra* Part I.B–D (explaining the three approaches taken by various circuits).

12. *See infra* Part I.B. Under agency theory, an employee automatically loses his or her authorized access to a work computer or files by acting in a manner converse to his or her employer's interests because such action terminates the agency relationship between the employer and employee. Taylor, *supra* note 3, at 213.

13. *See infra* Part I.C. The intended-use theory relies on whether an employee knew that his or her actions went beyond the scope of his or her authorized access. *See* Amber L. Leaders, *Gimme a* Brekka*!: Deciphering "Authorization" Under the CFAA and How Employers Can Protect Their Data*, 6 WASH. J. L. TECH. & ARTS 285, 293 (2011).

14. *See infra* Part I.D. The access means access theory has also been termed the plain meaning theory because it looks to the plain meaning of the statutory language and applies the rule of lenity to interpret the meaning of ambiguous terms, such as "authorization." *See* Leaders, *supra* note 13, at 290–92. Under this theory whether or not the employee has "authorization" is defined by the actions of the employer. *See Brekka*, 581 F.3d at 1133. For example, the *Brekka* court stated that an employee has "authorization" to use a computer when "the employer gives the employee permission to use it." *Id.* Under this theory, once the employer gives the employee permission to access the employer's computers, the employee does not violate the CFAA, irrespective of how he later uses the data that he obtains through such access. *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, 552 (2011).

15. *See infra* Parts I.B & C.

16. *See* Taylor, *supra* note 3, at 213–14; *see also infra* Part I.B (discussing how agency theory operates in CFAA cases).

17. *See infra* Part I.C.

18. *See infra* Part I.D.

have a far-reaching impact on future CFAA litigation, as it is the first decision to embrace the narrow approach, since it was laid out by the Ninth Circuit in 2009. Finally, this Note proposes that the *WEC Carolina Energy Solutions* court's narrow approach, which is based on the plain meaning of the statute and the rule of lenity, is supported by congressional intent and will provide for the most effective use of the CFAA in future litigation.

I. INTERPRETATIONS OF THE COMPUTER FRAUD & ABUSE ACT

A. The Evolution of the Computer Fraud & Abuse Act

1. The Beginning: The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

According to hearings before the Subcommittee on Civil and Constitutional Rights of the House of Representatives Committee on the Judiciary, in 1983, twenty-one states had passed legislation criminalizing the misuse of computers.[19] Even though at the time of enactment almost half of the states had existing laws criminalizing computer fraud,[20] Congress enacted the first federal statute that criminalized certain types of computer use,[21] the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act).[22] The 1984 Act was relatively narrow in scope and only governed a few types of activity.[23] The 1984 Act made it a crime to "knowingly access a computer without authorization," or access the computer without authorization to obtain defense or foreign affairs-related information, with the intent to use it to injure the United States or to help a foreign nation;[24] "knowingly access a computer without authorization" or access an authorized computer for unauthorized purposes, to

---

19. *Computer Crime: Hearing Before the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary*, 98th Cong., 2 (1983) (statement of Rep. Bill Nelson).

20. *See id*. Prior to 1984, the types of computer crimes covered by the new legislation were prosecuted under federal statutes originally designed to cover other crimes, such as mail fraud and wire-tapping. *See* 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, 409 & n.18 (2012).

21. Griffith, *supra* note 7, at 455. The threat of computer related crimes such as hacking was magnified by popular culture and movies like the 1983 movie "War Games", in which a teenager hacks into a government computer, gains control of United States nuclear arsenal, and almost causes a nuclear war. *See* Kapitanyan, *supra* note 20, at 410; Okuh, *supra* note 3, at 646. The movie was even mentioned in the 1984 House Report supporting the passage of the legislation. H.R. REP. NO. 98-894, at 10–11 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3895–96 (referencing the movie "War Games" as a means of demonstrating how computers can be used to increase processing power to engage in criminal activity more efficiently).

22. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 1837, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2006)).

23. *See* Griffith, *supra* note 7, at 455.

24. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, ch. 21, sec. 2102(a), 98 Stat. at 2190 (codified as amended at 18 U.S.C. § 1030(a)(1)).

obtain financial information;[25] "knowingly access a [U.S. Government] computer without authorization, or use such access to "use[], modif[y], destroy[], or disclose[] information in, or prevent[] authorized use of, such computer."[26]

Legislators and industry leaders criticized the 1984 Act, charging that the lack of available data regarding computers at the time of its inception made it incomplete, inefficient, and difficult for prosecutors to use effectively.[27] Other commentators argued that the 1984 Act left a large regulatory gap because it did not address harm caused by those who misused authorized access.[28] In response to this negative criticism, Congress passed the Computer Fraud and Abuse Act of 1986 (the 1986 Act).[29]

2. An Attempt to Revise: The Computer Fraud and Abuse Act of 1986

In an attempt to remedy concerns over the liability produced by those with authorized access who cause harm, Congress added the phrase, "exceeds authorized access" to the 1986 Act.[30] This tiny phrase is the root of the problem for courts interpreting, and employers seeking to use, the 1986 Act.[31] In an effort to address federalism concerns, Congress "limit[ed] Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, which is to say, where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature."[32]

Not only did the 1986 Act clarify certain subsections of the 1984 Act, it also prohibited more computer-related acts, such as property theft using a computer as a part of a plan to defraud, intentionally altering or destroying others' data,

---

25. *Id.* at ch. 21, sec. 2102(a), 98 Stat. at 2190–91 (codified as amended at 18 U.S.C. § 1030(a)(2)).

26. *Id.* at ch. 21, sec. 2102(a), 98 Stat. at 2191 (codified as amended at 18 U.S.C. § 1030(a)(3)).

27. Griffith, *supra* note 7, at 482–83 ("Computer crime was analogous to the proverbial emperor's clothes: everybody proclaimed it was there, but no one could see it."); *see also* Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 012 ¶ 6 (noting the dearth of data relating to computer crime in 1984).

28. Hernacki, *supra* note 5, at 1549.

29. Pub. L. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030(a) (2006)); *see also* Griffith, *supra* note 7, at 473 (explaining that Congress passed the 1986 Act to address problems with the 1984 Act); Hernaki, *supra* note 5, at 1549 (same).

30. Hernacki, *supra* note 5, at 1549–50 (quoting 18 U.S.C. § 1030 (1988)) (current version at 18 U.S.C. § 1030(a) (2006)).

31. *See id.* at 1550 ("This small phrase would later prove to have widespread interpretive problems."); *see also infra* Part I.A.4.

32. S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482. Additionally, Congress intended in the 1986 Act to strike an "appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses." *Id.*; *see also* Pollaro, *supra* note 27, at ¶ 7 (explaining that Congress acted cautiously, indicating intent to permit states to enact their own computer crime laws).

and password trafficking.[33] According to the U.S. Department of Justice, the current version of the CFAA addresses nine types of computer crimes.[34]

3. Important Amendments: The 1994 & 1996 Amendments to the Computer Fraud and Abuse Act

The CFAA has been amended eight times since 1986, most significantly in 1994 and 1996.[35] In 1994, Congress passed an amendment that provided a private right of action under the CFAA.[36] The CFAA was amended to state, in relevant part, that whoever "suffers damage or loss by reason of a violation . . . may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[37] Employers have used this provision to file civil suits against former employees.[38]

The Economic Espionage Act of 1996 (EEA) also amended the CFAA.[39] The EEA notably expanded the scope of the CFAA's coverage by applying it to all "protected computers," rather than solely to "federal interest" computers, as provided for by the older version of the CFAA.[40] The term "protected computer" includes federal government computers, computers of financial institutions and computers used for interstate or foreign commerce purposes.[41] The EEA expanded the scope of the CFAA by associating it with the breadth of the Commerce Clause.[42]

---

33. Pollaro, *supra* note 27, at ¶ 7; *Prosecuting Computer Crimes*, U.S. DEP'T OF JUSTICE 2, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited Jan. 09, 2014).

34. *Prosecuting Computer Crimes*, *supra* note 33, at 3. The statute criminalizes "Obtaining National Security Information," "Accessing a Computer and Obtaining Information," "Trespassing in a Government Computer," "Accessing a Computer to Defraud & Obtain Value," "Intentionally Damaging by Knowing Transmission," "Recklessly Damaging by Intentional Access," "Negligently Causing Damage & Loss by Intentional Access," "Trafficking in Passwords," and "Extortion Involving Computers." *Id.*

35. Pollaro, *supra* note 27, at ¶ 8 (noting that Congress amended the CFAA in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008 to keep up with evolving computer crime); *see also Prosecuting Computer Crimes*, *supra* note 33, at 2 (same).

36. Hernacki, *supra* note 5, at 1550.

37. 18 U.S.C. § 1030(g) (2006 & Supp. 2012).

38. These civil suits typically stem from actions taken by the employee just before he or she plans to leave his or her current employer and start a competing business, or from actions taken by the employee for other personal benefits. *See infra* Parts I.B–D (discussing various cases in which employers brought civil actions against former employees under the CFAA).

39. Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

40. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1567 (2010); Hernacki, *supra* note 5, at 1550–51.

41. 18 U.S.C. § 1030(e)(2).

42. Hernacki, *supra* note 5, at 1553 (explaining that the specific language used by Congress in defining what constitutes a protected computer expands the CFAA's scope to include every computer used to perform "economic . . . activities that substantially affect commerce"); Kerr, *supra* note 40, at 1568 (internal citations omitted) ("Because every computer connected to the Internet is used in interstate commerce or communication, it seems that every computer connected to the Internet is a 'protected computer' covered by 18 U.S.C. § 1030."); *see also* Pollaro, *supra*

4. A Tiny Phrase that Causes a Huge Problem: The Computer Fraud and Abuse Act's Authorization Statute

Many offenses under the current version of the CFAA require an offender to act "without authorization" or in a manner that "exceeds authorized access."[43] The phrase "without authorization" is not defined in the CFAA, but the CFAA explains that an offender "exceeds authorized access" when he or she "access[es] a computer with authorization and . . . use[s] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[44] According to the CFAA's legislative history, Congress drafted the language "exceeds authorized access" with the belief that it would most likely be applied to insiders who already had some degree of access to the computer.[45] In contrast, Congress anticipated that the "without authorization" language would be used to cover outsiders with no degree of access to the computer.[46]

Courts have developed different approaches for interpreting this authorization language in the context of the workplace when the offender is an inside employee charged with misusing or misappropriating information.[47] Consider the following scenario: an employee downloads confidential company information with the intent to use that information in a presentation made on behalf of the company's competitor. The company has given the employee explicit authorization to access the confidential information but the employee uses it in a malicious manner that was not anticipated by the company when it granted authorization.[48] Whether the employee's actions fall within the scope of the CFAA depends on how the court interprets the CFAA's authorization language; interpretations vary among the circuits.[49] Some circuits would

---

note 27, at ¶ 8 (explaining that defining protected computers in relation to interstate commerce substantially broadened the CFAA's scope).

43. 18 U.S.C. § 1030(a) (2006 & Supp. 2012).

44. *Id.* § 1030(e)(6).

45. Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 174 (2011).

46. *Id.*

47. *See infra* Parts I.B–D (detailing the three approaches applied by various federal circuit courts).

48. These are roughly the facts of the most recent case to address the scope and meaning of the authorization statute of the CFAA. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201–02 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013). The court's holding and reasoning are explained in greater detail later in this Note. *See infra* Part II.

49. *See infra* Parts I.B–D.

consider the employee's actions within the CFAA's scope,[50] while others would hold that the CFAA does not apply.[51]

B. CFAA Authorization: Agency Theory

The Seventh Circuit was the first federal appellate court to officially rule on the CFAA authorization language.[52] In *International Airport Centers LLC v. Citrin*, an employee of International Airport Centers LLC (IAC), Citrin, was issued an official company laptop to use for work purposes.[53] Citrin decided to leave IAC to start his own business, in breach of his employment contract.[54] In anticipation of quitting, he downloaded a program onto the company laptop that permanently deleted not only his files, but also any evidence that he had engaged in improper activity before quitting.[55]

IAC filed a civil suit against Citrin alleging that he violated 18 U.S.C. § 1030(a)(5)(A)(ii), a provision of the CFAA that prohibits knowingly transmitting information without authorization that causes damage to a protected computer.[56] The court, using the agency theory rationale, held that IAC had a valid claim against Citrin under the CFAA because an employee's access authorization ends when the employee breaches his or her duty of loyalty to the employer.[57]

In defining the scope of the CFAA's authorization statute, the court relied on agency theory to develop a broad interpretation of the CFAA.[58] Under agency

---

50. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010) (affirming the defendant's conviction under the CFAA based on the intended-use theory); United States v. John, 597 F.3d 263, 269, 273 (5th Cir. 2010) (affirming the defendant's conviction under the CFAA based on the intended-use theory), *cert. denied*, 133 S. Ct. 1237 (2013); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (reinstating an employer's suit under the CFAA against a former employee based on the agency theory).

51. *See, e.g.*, *WEC Carolina Energy Solutions LLC*, 687 F.3d at 201, 203 (affirming the dismissal of the employer's CFAA claim against a former employee under the narrow access means access theory); United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc) (affirming the district court's dismissal of several CFAA charges under a plain language reading of the statute because the defendant's accomplices had permission to access the company data base at issue); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1128–29 (9th Cir. 2009) (affirming the district court's grant of summary judgment to a former employee in a CFAA action brought by his employer under a plain language reading of the statute because the employee had authorization to use the computer in question at the time the alleged violation occurred).

52. Pollaro, *supra* note 27, at ¶ 12; *see also Citrin*, 440 F.3d at 418–19.

53. *Citrin*, 440 F.3d at 419. Citrin worked in the real estate side of the business and assisted in locating and acquiring desirable properties for the company. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.* at 420–21.

58. *See id.* An "agency relationship" is defined as "the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act." RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006).

theory, "[u]nless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[59] The *Citrin* court held that Citrin breached his duty of loyalty to IAC when he decided to quit his job in violation of his employment contract and to destroy files belonging to IAC on his company computer.[60] Once the breach of loyalty occurred, it terminated the agency relationship and, with it, Citrin's authority to access the computer and its files.[61] The agency theory interpretation, adopted by the Seventh Circuit, broadly construes the CFAA's authorization language because it goes beyond the language of the statute to consider external issues such as agency relationships.[62]

C. CFAA Authorization: Intended Use Theory

Like the agency theory, the intended use theory also broadly construes the CFAA, granting employers the ability to pursue civil action against employees for a broad range of activities under the CFAA.[63] This theory, adopted by both the Fifth and Eleventh Circuits, focuses on whether the employee misuses information in a way that the employer had not intended, rather than the employee's unauthorized access to information.[64]

In *United States v. John*, the Fifth Circuit affirmed John's conviction for seven counts of criminal activity, including violation of Sections 1030(a)(2)(A) and (C) of the CFAA, which prohibit "exceed[ing] authorized access" to obtain information from a protected computer.[65] John was working as an account manager for Citigroup when she accessed confidential customer account information and provided that information to her half-brother as part of a scheme

---

59. RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

60. *Citrin*, 440 F.3d at 420. Citrin's actions were significant because, as an agent of his employer, he had "a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship." RESTATEMENT (THIRD) OF AGENCY § 8.01.

61. *Citrin*, 440 F.3d at 420–21.

62. *Id.* at 419–21.

63. *See* Leaders, *supra* note 13, at 293 (explaining that the Fifth Circuit's interpretation of the CFAA's authorization language in *John*, adopting the intended-use theory, is broader than interpretations of the same language by other courts).

64. *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010), *cert. denied*, 133 S. Ct. 1237 (2013). Although the Eleventh Circuit did not use the words "intended-use theory," the court applied similar reasoning to reach its holding as the Fifth Circuit used in *John*. Compare *Rodriguez*, 628 F.3d at 1263 (explaining that the employee exceeded the scope of his authorized access and thus violated the CFAA by accessing victim's personal records for non-business reasons), *with John*, 597 F.3d at 270–72 (holding that an employee had exceeded her authorized access where the employee knew she was accessing information on a computer for an illegal purpose); *see also* Leaders, *supra* note 13, at 292–94 (2011) (providing an overview of how the intended-use theory played a role in the holdings of both the *John* and *Rodriguez* cases).

65. *John*, 597 F.3d at 269–70. But only two of the seven were in violation of the CFAA. *Id.* at 269–70.

to allow him to make fraudulent charges.[66] John admitted to being aware of Citigroup's explicit employee policies prohibiting the misuse of customer information.[67] The court applied the intended-use theory and concluded that, "[a]ccess 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."[68] Additionally, the court emphasized John's prior notice and knowledge of company policies as indicators of John's actual knowledge of the intended purpose for his access.[69] This case highlights two practical aspects of CFAA jurisprudence. First, *John* illustrates criminal charges may be brought against an employee under the CFAA.[70] Second, the case demonstrates the private right of action available to employers victimized by employee behavior.[71]

In *United States v. Rodriguez*, the Eleventh Circuit also examined the scope of the CFAA's authorization language in the context of a criminal case.[72] The court upheld Rodriguez's conviction for violating Section 1030 (a)(2)(B) of the CFAA.[73] Rodriguez worked at the Social Security Administration (SSA) and was given explicit access to various databases to use as part of his duties.[74] Rodriguez used one of these databases for his personal use to retrieve information about women who he found romantically desirable.[75] Rodriguez knew that the SSA had a strict policy against using the database information for non-business reasons.[76]

---

66. *Id.* at 269. The information obtained included computer printouts containing account numbers and copies of scanned personal checks. *Id.*

67. *Id.* at 272.

68. *Id.*

69. *Id.* at 272 (highlighting that Citigroup's official policy prohibiting the misuse of confidential customer account information was reiterated in meetings that John attended).

70. *Id.* at 270–72.

71. *See id*. at 269–70; 18 U.S.C. § 1030(g) (2006).

72. United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

73. *Id.* Section § 1030 (a)(2)(B) of the CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any department or agency of the United States." 18 U.S.C. § 1030 (a)(2)(B) (2006 & Supp. 2012).

74. *Rodriguez*, 628 F.3d at 1260. The SSA databases that Rodriguez was given access to contained personal information, including addresses, dates of birth, and social security numbers. *Id.*

75. Hernacki, *supra* note 5, at 1557. Rodriguez used the personal information to call women, send them flowers and letters at their homes, and obtain their birth dates. *Rodriguez*, 628 F.3d at 1260–63. In almost all of the cases, the victims had not disclosed their addresses, phone numbers, or date of birth to the defendant and were concerned to discover that he possessed this information. *Id.*

76. *Rodriguez*, 628 F.3d at 1263. The SSA policy "prohibits an employee from obtaining information from its databases without a business reason." *Id.* at 1260. All of the SSA's TeleService employees, including Rodriguez, were made aware of this policy "through mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily." *Id.* The court also noted that SAA required employees to acknowledge receipt of the policies in writing annually and warned employees that criminal penalties could be imposed for

The court held that Rodriguez was criminally liable under the CFAA and, using the intended-use analysis, found a company's computer use policies could be used to define authorized access within the meaning of the CFAA and thereby specify the scope of actions violating the statute.[77] When Rodriguez accessed the information for non-business reasons, he effectively exceeded his authorized access in violation of the SSA's policy.[78]

D. CFAA Authorization: Access Means Access/Plain Meaning Theory

The third theory federal appellate courts have used to determine the scope of the CFAA's authorization language is the plain meaning theory. This approach was originally adopted by the Ninth Circuit[79] and, more recently, by the Fourth Circuit.[80]

In *LVRC Holdings LLC v. Brekka*, the Ninth Circuit addressed the CFAA's authorization language in the context of a civil case in which an employer, LVRC Holdings LLC (LVRC), sued a former employee, Brekka, for violating Sections 1030(a)(2) and (4) of the CFAA.[81] Both sections of the CFAA impose liability only when the employee acts without authorization or in a manner that exceeds his or her authorization.[82] Brekka was hired to work as an administrator for a rehab clinic.[83] His duties included overseeing the company's online marketing efforts.[84] Brekka was given a company computer and full access to LVRC's website via an administrative log-in.[85] LVRC did not establish company policies for the use of company documents by employees, nor did they have a written employment agreement with Brekka.[86] Brekka left LVRC's

---

violations. *Id.* Rodriguez refused to sign the forms acknowledging the SSA's policies, "ask[ing] a supervisor rhetorically, 'Why give the government rope to hang me?'" *Id.*

77. *Id.* at 1263 ("Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness purpose."); Tuma, *supra* note 45, at 180 (noting that the *Rodriguez* court applied intended-use theory reasoning to reach its conclusion).

78. *Rodriguez*, 628 F.3d at 1263.

79. *See* United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

80. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203–04 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013).

81. *Brekka*, 581 F.3d at 1129. Section 1030 (a)(2) prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2) (2006 & Supp. 2012). Section 1030 (a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value." 18 U.S.C. § 1030(a)(4).

82. *See* 18 U.S.C. § 1030(a)(2); 18 U.S.C. § 1030(a)(4).

83. *Brekka*, 581 F.3d at 1129.

84. *Id.*

85. *Id.*

86. *Id.*

employ;[87] but before quitting, Brekka emailed confidential company documents to his personal computer with the intent to use the information to start his own competing business.[88] LVRC sued Brekka, arguing that, pursuant to the agency theory adopted by the *Citrin* court, LVRC could bring an action against Brekka under the CFAA.[89]

The Ninth Circuit rejected LVRC's argument, stating that the CFAA is primarily a criminal statute and should not be interpreted in a "surprising" manner that is inconsistent with the statutory language.[90] Instead, the court relied on the statutory construction cannon of plain meaning, stating that the CFAA should be interpreted according to the ordinary meaning of its words unless the terms are otherwise defined.[91] The court referenced the dictionary definition of "authorization"[92] to explain that the plain meaning of the statute does not support the agency theory approach because the CFAA does not indicate that an employee's authorization terminates when he or she uses the computer in a manner contrary to the employer's interest.[93]

The court also used the plain meaning of the statute to rebut the intended use theory, reasoning that, "[t]he definition of the term 'exceeds authorized access' . . . implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer."[94] The court noted that the plain language of the CFAA does not explicitly reject the access means access theory, and furthermore, that the legislative history of the CFAA does not support a broad interpretation of the authorizing language.[95] The court also explained that the rule of lenity supports

---

87. *Id.* at 1129–30 (noting that Brekka left after negotiation efforts regarding giving him an ownership interest in the company failed).

88. *Id.* (stating that the documents Brekka sent included, "a financial statement for the company, LVRC's marketing budget, admissions reports for patients . . . . [and] a master admissions report, which included the names of past and current patients of the rehab clinic").

89. *Id.* at 1130, 1133–34. LVRC tried to bring an additional claim against Brekka after the company discovered that someone accessed files using Brekka's assigned password after Brekka was fired. *Id.* at 1136–37. However, the district court dismissed the claim due to a lack of evidence establishing that Brekka was the responsible party. *Id.*

90. *Id.* at 1134.

91. *Id.* at 1132 (quoting Perrin v. United States, 444 U.S. 37, 42 (1979)).

92. *Id.* at 1133 (quoting RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY 139 (2001)) (noting that authorization is defined as "permission or power granted by an authority").

93. *Id.* ("It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'").

94. *Id.* at 1135.

95. *Id.* The CFAA's legislative history "shows that the statute was intended to apply only to crimes of computer misuse and not to crimes incidentally involving the use of a computer" and is thus analogous to "'breaking and entering'" rather than mere facilitation." Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 238 (2010) (quoting H.R. REP. NO. 98-894, at 32 (1984)). Scholars have explained that the CFAA was meant to be a stop-gap measure targeted at gaps in traditional crime laws, which were improperly structured to handle new computer-misuse

a narrow interpretation of the CFAA's language.[96] The rule of lenity specifies that when a criminal statute is ambiguous, it must be construed in a manner most favorable to the defendant.[97] Similarly, the court noted that "[t]he Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants."[98]

The court ultimately concluded that LVRC did not have a valid claim against Brekka under the CFAA.[99] The court held that Brekka's actions did not exceed his authorized access because his actions fell within the computer usage allowed by his company and because the CFAA is concerned with access, not what is done with that access.[100] The court concluded that a person acts without authorization under the CFAA only "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway."[101]

The Ninth Circuit had another opportunity to address the scope of the CFAA's authorization language in *United States v. Nosal*, this time in the context of a criminal case.[102] *Nosal* also involved a situation in which employees used their authorized access to download company information for the purpose of starting a competing company.[103] However, in *Nosal*, the employer had explicit company policies prohibiting this action.[104] Nosal was a former employee at the time he downloaded the documents.[105] He was charged under Section 1030 (a)(4) of the CFAA for aiding and abetting some of the company's current employees in "'exceed[ing their] authorized access' with intent to defraud."[106]

---

offenses, and thus was meant to address only these new categories of crime. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1603 (2003); Chung, *supra*, at 238–39.

96. *Brekka*, 581 F.3d at 1134–35.

97. *Id.* at 1135 (quoting United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)).

98. *Id.* at 1134.

99. *Id.* at 1135.

100. *Id.* ("There is no dispute that Brekka was given permission to use LVRC's computer and that he accessed documents or information to which he was entitled by virtue of his employment with LVRC . . . . [therefore] he did not access a computer 'without authorization.'"); *see also* Leaders, *supra* note 14, at 291–92 (evaluating the *Brekka* court's holding).

101. *Brekka*, 581 F.3d at 1135.

102. United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc). It is irrelevant whether the case is criminal or civil for the purpose of analyzing how the courts have interpreted the scope of the CFAA authorization language because the civil damages only flow if the employee would be found criminally liable. *See* 18 U.S.C. § 1030(g) (2006 & Supp. 2012).

103. *Nosal*, 676 F.3d at 856.

104. *Id.*

105. *Id.*

106. *Id.*

The court rejected the broad interpretations of the CFAA adopted by the Fifth, Seventh, and Eleventh Circuits.[107] Instead, the *Nosal* court opted to follow the *Brekka* court's approach, and urged the other circuits to reconsider their interpretations.[108] The court adopted the *Brekka* court's narrow interpretation of the CFAA authorization language, holding that, "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions."[109]

II. WEC CAROLINA ENERGY SOLUTIONS: DEEPENING THE CIRCUIT SPLIT AND LEAVING EMPLOYERS SCRATCHING THEIR HEADS

The Fourth Circuit joined the Ninth Circuit's narrow interpretation of the CFAA in *WEC Carolina Energy Solutions*.[110] WEC Carolina Energy Solutions (WEC) sued its former employee, Miller, under the CFAA's private right of action provision alleging violations of Sections 1030 (a)(2)(C), (a)(4), (a)(5)(B), and (a)(5)(C), "each of which require that a party either access a computer 'without authorization' or 'exceed[] authorized access.'"[111] While still employed at WEC, Miller e-mailed confidential company information to his personal computer from his company laptop and, after resigning, he used that information to make a presentation to a potential customer on behalf of one of WEC's competitors.[112] WEC had established company policies prohibiting the use of company information in this manner.[113]

---

107. *Id.* at 862–63.

108. *Id.*

109. *Id.* at 863. The *Nosal* case has followed an interesting trajectory. Prior to the en banc rehearing in 2012, the Ninth Circuit panel used the *Nosal* opinion (*Nosal panel*) as an opportunity to narrow the holding in *Brekka* to the specific facts of the case, effectively nullifying the narrow interpretation of the CFAA's authorization language. *See* Jeff Neuburger, *Ninth Circuit Panel Says Employee Violation of Employer Computer Use Policy Can Support CFAA Criminal Charge*, NEW MEDIA & TECH. L. BLOG (April 29, 2011), http://newmedialaw.proskauer.com/2011/04/29/ninth-circuit-panel-says-employee-violation-of-employer-computer-use-policy-can-support-cfaa-criminal-charge/. The *Nosal panel* opinion aligned the Ninth Circuit with the Fifth and Eleventh Circuits by adopting the intended use theory. *See id.* (stating that the *Nosal panel* reversed the district court and "explicitly weighed in on the side of the other circuit courts that have addressed the issue"). However, as noted above, the *Nosal panel* opinion was reversed en banc and reinvigorated the *Brekka* court's interpretation. *See Nosal*, 676 F.3d at 863 ("[W]e continue to follow in the path blazed by *Brekka*."). For a recounting of the interesting procedural history of *Nosal*, see Paul J. Larkin, Jr., *United States v. Nosal: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIRCUIT REV. 257, 264–69 (2012).

110. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013) (explaining that the court agrees with the Ninth Circuit's "literal[] and narrow[]" interpretation of the CFAA's authorization language).

111. *Id.* at 201–03. WEC Carolina Energy Solutions LLC also alleged nine additional claims under state law against Miller. *Id.* at 202.

112. *Id.* Apparently, Miller had access to confidential information stored on the company's network through his company-issued laptop, including trade secrets, "pricing terms, pending projects[,] and the technical capabilities of WEC." *Id.* As a result of Miller's presentation, WEC's potential client decided to work with the competitor. *Id.*

113. *Id.*

The court held that WEC did not have a claim against Miller under the CFAA.[114] The court adopted a narrow interpretation of the statute's authorization language, holding that it only applies "when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access."[115] The *WEC Carolina Energy Solutions* court employed reasoning similar to the Ninth Circuit in *Brekka* and *Nosal*, and explicitly rejected the agency theory and the intended use theory, holding that the narrow interpretation is better supported by the plain meaning of the statute and the rule of lenity.[116]

In adopting the Ninth Circuit's interpretation, the *WEC Carolina Energy Solutions* court added credibility and support to the access means access theory.[117] Since the Fourth Circuit issued the *WEC Carolina Energy Solutions* holding, the narrow interpretation, which was once described as contrary to well-supported precedent,[118] has been deemed "a trend that other courts will follow."[119] The issue has also recently been described as having "new potential . . . to reach the Supreme Court."[120]

The deepened circuit split causes significant problems for employers because a situation that would result in liability under the CFAA in one state may not result in liability in another.[121] For example, according to one commentator, "whether an employer can bring CFAA claims against employees who steal company data in violation of computer usage policies depends on where the

---

114. *Id.* at 206–07.

115. *Id.* (explaining that Miller's actions did not meet this requirement because, although he "may have misappropriated information, [he] did not access a computer without authorization or exceed [his] authorized access").

116. *See id.* at 203-07; LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

117. *See WEC Carolina Energy Solutions*, 687 F.3d at 203.

118. *See* Brief of Appellant at 10, WEC Carolina Energy Solutions LLC v. Miller 687 F.3d 199 (4th Cir. 2012) (No. 11-1201), *cert. dismissed*, 133 S. Ct. 831 (2013).

119. Matthew J. Hank, *Fourth Circuit Joins Courts Limiting Use of Computer Fraud and Abuse Act to Prosecute Disloyal Employee*, UNFAIR COMPETITION & TRADE SECRETS COUNSEL (Aug. 02, 2012), http://www.unfaircompetitiontradesecretscounsel.com/federal-law/computer-fraud-abuse-act/fourth-circuit-joins-courts-limiting-use-of-computer-fraud-and-abuse-act-to-prosecute-disloyal-emplo/index.html. The lesson to learn from *WEC Carolina Energy Solutions* is that, "where the employee downloads information to which he was permitted access and then misuses that data to benefit a competitor, the employer will not have recourse to a CFAA claim and should focus on state-law claims." *Id.*

120. Ilana Rubel & Sebastian Kaplan, *Ninth Circuit Scales Back CFAA Application to Data Misappropriation Cases*, FENWICK & WEST LLP, http://www.fenwick.com/publications/Pages/Ninth-Circuit-Scales-Back-CFAA-Application-to-Data-Misappropriation-Cases.aspx (last visited Jan. 09, 2014).

121. Taylor, *supra* note 3, at 202–03 (explaining that the circuit split "leaves employers in a very uncertain position as to how best to protect their data"). This determination is contingent on which circuit a particular state falls within and which theory that circuit advocates. An even more difficult situation for employers is when the jurisdiction in which they file their action has yet to establish a position. *See id.*

employer can file suit."[122] The confusion resulting from the circuit split has been described as creating a bleak and confusing situation for employers.[123]

While this issue has struggled to reach the United States Supreme Court, it is increasingly important that employers receive definitive guidance.[124] The Supreme Court denied the petition for certiorari in *WEC Carolina Energy Solutions* on January 2, 2013.[125] Additionally, following the Ninth Circuit's en banc decision in *Nosal*, the United States Department of Justice declined to file a petition seeking review.[126] These missed opportunities for direction from the Supreme Court only heighten the confusion and chaos surrounding the CFAA's authorization language.

This issue has also been addressed in a proposed amendment to the Cybersecurity Act of 2012 (CSA), which highlighted the importance of finding

---

122. Abigail Rubenstein, *Circuit Split On CFAA Leaves Employers Scratching Heads*, LAW 360 (Aug. 13, 2012, 10:02 PM), http://www.law360.com/whitecollar/articles/369259/circuit-split-on-cfaa-leaves-employers-scratching-heads. For now, employers located in the Fourth Circuit will have to rely on state law claims to prosecute employees suspected of absconding with confidential information. John Marsh, *WEC Carolina Energy Solutions v. Miller: The Fourth Circuit Adopts the Reasoning of U.S. v. Nosal and Limits the Computer Fraud and Abuse Act to Hacking*, TRADE SECRET LITIGATOR BLOG (July 30, 2012, 11:00 PM), http://www.hahnloeser.com/tradesecretlitigator/post/2012/07/30/WEC-Carolina-Energy-Solutions-v-Miller-The-Fourth-Circuit-Adopts-the-Reasoning-of-US-v-Nosal-and-Limits-the-Computer-Fraud-and-Abuse-Act-to-Hacking.aspx.

123. Rubenstein, *supra* note 122; Matt Lampe, *Employer Lawsuits Against Employees Under the Computer Fraud and Abuse Act*, LABOR & EMPLOYMENT N.Y. ("LENY") THE OFFICIAL BLOG OF THE NEW YORK STATE BAR ASSOCIATION'S LABOR AND EMPLOYMENT LAW SECTION (August 17, 2012, 12:35 PM), http://nysbar.com/blogs/LENY/2012/08/ ("[T]he circuit split is sure to remain for the foreseeable future and the application of the CFAA to the employment context will be unresolved."). There may be more benefits for employers filing actions in federal court under the CFAA than for employers who resort to state law claims, such as lessening what the employer must show to bring suit against the employee and providing the ability to bring suit against the former employee's new employer and to request injunctive relief. Kapitanyan, *supra* note 20, at 418.

124. *See* Michael P. Maslanka, *Circuits Split on Important CFAA Issue*, TEXAS LAWYER (Oct. 1, 2012), http://www.law.com/jsp/tx/PubArticleTX.jsp?id=1202572840856&thepage=1&slreturn=20121019154119 (describing this issue as one ripe for review because it is an issue of interest for employers and there is "well-developed" support for the different interpretations of the statutory language).

125. WEC Carolina Energy Solutions LLC v. Miller, 133 S. Ct. 831 (2013). WEC Carolina Energy Solutions filed a petition for writ of certiorari on October 24, 2102 asking the Court to review whether an employer's restrictions on the purpose electronic information is used for can provide the basis for CFAA liability. Petition for Writ of Certiorari, WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (No. 12-518), *cert. dismissed*, 133 S. Ct. 831 (2013).

126. Rubenstein, *supra* note 122. According to Orin Kerr, the Justice Department declined to file a petition seeking Supreme Court review of the *Nosal* opinion "because [the government] 'may have been scared off by Judge Kozinski's [*Nosal*] opinion . . . [which is] a pretty powerful brief against the government's position.'" David Kravets, *DOJ Won't Ask Supreme Court to Review Hacking Case*, WIRED.COM (Aug. 10, 2012, 2:10 PM), http://www.wired.com/threatlevel/2012/08/computer-fraud-supreme-court/.

finality on the issue.[127] Although the amendment was not accepted, it would have, in effect, adopted the plain language approach espoused by the Fourth and Ninth Circuits.[128]

Beyond the purely legal reasons why this issue should be reviewed, this issue has implications for many individuals, as demonstrated by the recent high-profile prosecution of Aaron Swartz.[129] The government charged Swartz with violating the CFAA after he illegally accessed the Massachusetts Institute of Technology's computer network to download approximately 4.8 million academic articles from a database called JSTOR, in direct violation of JSTOR's terms of service.[130] If convicted, Swartz could have faced up to thirty-five years in federal prison and a fine of one million dollars.[131] Swartz committed suicide before his case could reach trial.[132] Illustrating the disparate approaches taken by the various circuits, Swartz would have been arraigned under First Circuit precedent, thus whether a violation was properly alleged under the CFAA depends on which of the three approaches the First Circuit court chose to follow.[133]

---

127. *See* Orin Kerr, *Recent Developments – Both in the Courts and in Congress–on the Scope of the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), http://www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act/ [hereinafter *Kerr on Volokh*]. The Cybersecurity Act of 2012 (CSA) was a bipartisan effort developed to protect private and governmental organizations from cyber attacks. *Securing America's Future: The Cybersecurity Act of 2012: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 112th Cong. 1–4 (2012) (statement of Sen. Joseph Liberman, Chairman, S. Comm. on Homeland Sec. & Gov't Affairs). The drafters of the CSA shared many of the same fears as the drafters of the CFAA, including the potential for cyber attacks on critical infrastructure and for damage the economy. *See id.* at 1–2.

128. *See Kerr on Volokh*, *supra* note 127. The proposed language would have changed United States Code Section 1030(e)(6) by inserting the following language:

> "alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized."

158 CONG. REC. S5403 (daily ed. July 25, 2012). Although the Court may wish to wait for a legislative fix to this growing problem, the legislative branch can move very slowly and the severity of this issue only deepens with technological advances.

129. *See* Justin Peters, *Aaron Swartz May Have Violated JSTOR's Terms of Service. Should That Be a Crime?*, SLATE (Feb. 15, 2013, 4:12 PM), http://www.slate.com/blogs/crime/2013/02/15/aaron_swartz_suicide_should_violating_a_website_s_terms_of_service_be_a.html.

130. *See id.*

131. Press Release, U.S. Attorney's Office for the Dist. of Mass., 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.

132. *See* Peters, *supra* note 129.

133. *See id.* The plain meaning theory would not control Aaron Swartz's case if he was indicted in Massachusetts; his case would have been controlled by First Circuit precedent. *See* Indictment, United States v. Swartz, (D. Mass. July 14, 2011), *available at* http://web.mit.edu/bitbucket/Swartz,%20Aaron%20Indictment.pdf.

Although Swartz's case did not involve a private right of action brought by an employer,[134] it presents larger questions as to the negative effects of allowing expansive prosecutorial discretion under some interpretations of the CFAA's language. This tragic event may prove to be the catalyst that results in Supreme Court review of the circuit split over the CFAA's authorization language.

III. THE WEC CAROLINA ENERGY SOLUTIONS APPROACH IS NECESSARY

A. A Logical Interpretation of the Plain Meaning of the CFAA

In *WEC Carolina Energy Solutions*, the Fourth Circuit followed the analysis for interpreting the CFAA's authorizing language as set out by the Ninth Circuit.[135] The court addressed WEC's interpretation of the CFAA's language supporting the claim that Miller's actions violated the CFAA by exceeding his authorized access.[136] WEC relied on the *Nosal* panel's reasoning and argued that the word "so" in the statutory definition of "exceeds authorized access" should be interpreted to mean "in a manner or way that is indicated or suggested."[137] Therefore, an employee exceeds his authorized access under the CFAA "if he uses such access 'to obtain or alter information [on] the computer that [he] is not entitled [in that manner] to obtain or alter.'"[138]

However, interpreting "so" in this way insufficiently supports WEC's claim that Miller violated the CFAA by his violating the company's use policy.[139] The Fourth Circuit explained that under WEC's proposed definition, the statute could mean that the employee violates the CFAA when he lacks actual authorization to access the information.[140] Under such an interpretation, the CFAA's authorization language refers to the *means* of obtaining information, not the employee's *use* of that information after the initial access.[141] For example, an employee who disregards company policies and removes a thumb drive containing information he is only authorized to access at the office would be implicated by this interpretation.[142] Although the employee is not violating a policy that dictates the way that the information may be used, he has still

---

134. Swartz was not an employee of JSTOR and JSTOR declined to purse civil charges against him. *See* Press Release, JSTOR, JSTOR Statement: Misuse Incident and Criminal Case (July 19, 2011), http://about.jstor.org/news/jstor-statement-misuse-incident-and-criminal-case.

135. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204–07 (4th Cir. 2012) (adopting the method of analysis used by the Ninth Circuit in *Nosal*), *cert. dismissed*, 133 S. Ct. 831 (2013).

136. *Id.*

137. *Id.* at 204–05 (quoting United States v. Nosal, 642 F.3d 781, 785 (9th Cir. 2011)) (internal quotation marks omitted), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012)).

138. *Id.* at 205 (quoting *Nosal*, 642 F.3d at 785–86).

139. *See id.*

140. *See id.*

141. *Id.*

142. *Id.* (citing *Nosal*, 676 F.3d at 858).

"obtain[ed] information 'in a manner' that lacks authorization" by removing information he is not authorized to take from the office.[143]

Furthermore, WEC's theory places great significance on "so," "a two-letter word that is essentially a conjunction."[144] This reliance may be misplaced because, as the court suggests, Congress could have intended a different meaning or purpose for "so," such as, use "as a connector or for emphasis."[145] The most persuasive interpretation of the CFAA is that the plain meaning of the statute only prohibits improperly accessing information, and an employee exceeds his approved access when he uses it "to obtain or alter information that falls outside the bounds of his approved access."[146]

Although this interpretation is the most logical, alternative interpretations are at least plausible. But it is well-established that when a criminal statute is susceptible to two plausible interpretations, the court must favor the one that has a softer effect on the defendant.[147] As a result, the statute should be read strictly, which is better accomplished by the narrower, plain meaning theory.

B. Employers Have Numerous Other Ways to Address Misappropriation of Company Information by Employees

Rather than stretching the scope of the CFAA beyond the bounds originally intended by Congress,[148] employers should utilize one of the many other forms of redress available to them in combating employee misappropriation of company information.[149] In many scenarios arising from employee misconduct, companies suing under the CFAA could have availed themselves of state law remedies instead, such as suing the employee for misappropriation of a trade secret.[150] A trade secret is "some sort of information that has value because it is

---

143. *Id.* (citing *Nosal*, 676 F.3d at 858).

144. *Nosal*, 676 F.3d at 857 (referencing the government's interpretation in *Nosal*, which is similar to the plaintiff's argument in *WEC Carolina Energy Solutions*).

145. *WEC Carolina Energy Solutions LLC*, 687 F.3d at 205 (quoting *Nosal*, 676 F.3d at 858).

146. *See id.* at 204.

147. *See* Jones v. United States, 529 U.S. 848, 858 (2000) (quoting United States v. Universal C.I.T. Credit Corp., 344 U.S. 218, 221–22 (1952)) (explaining when the rule of lenity applies). The rule of lenity has been described as "a necessary safety valve in an adversarial system of justice." *The Supreme Court—Leading Cases*, 122 HARV. L. REV. 276, 475 (2008). The Supreme Court has justified the rule of lenity in part on the grounds that, "when [a] choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *See Universal C.I.T. Credit Corp.*, 344 U.S. at 221–22.

148. Hernacki, *supra* note 5, at 1574–75 (arguing in favor of a narrow interpretation of the CFAA's authorization language that is consistent with Congress's original intent to treat the CFAA as an anti-hacking statute).

149. *See infra* text accompanying notes 150–57.

150. *See generally* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 6 (2007) (explaining that unlike CFAA violations, trade secret civil cases must be tried in state courts because trade secret law derives from common law and thus varies by state).

not generally known."[151] The Uniform Trade Secret Act (UTSA) allows for recovery if trade secrets are "misappropriated," meaning obtained by "improper means."[152] This private right of action is available to most employers because all but six states have enacted some version of the UTSA."[153]

Additionally, several states have concluded that employees owe a duty of loyalty to their employers.[154] This duty of loyalty requires that an employee "not divert business from his or her employer to a competing business nor engage in self-dealing while in the company's employ."[155] The Sixth Circuit, in a diversity of citizenship case, held the duty of loyalty imposed by the state in question included "the obligation not to act against the employer's interest."[156] Bringing a private suit alleging trade secret misappropriation and breach of a duty of loyalty is a more appropriate means of redress for employers than stretching the CFAA beyond its intended purpose.

C. The WEC Carolina Energy Solutions Approach Ensures that Innocent Behavior Will Not Become Criminalized

The narrow interpretation of the CFAA better circumscribes the CFAA's scope. Under the agency theory, a valid CFAA claim merely requires that the employee used a computer in a way that breached his duty of loyalty to the employer or was adverse to the interests of the employer.[157] Under the intended-use theory, the validity of the CFAA claim depends on whether the employee violated company policies.[158] Both of these broad interpretations

---

151. *Id.*

152. *See id.* at 8. The term "improper means," as defined in the UTSA, "includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." UNIF. TRADE SECRETS ACT § 1(1) (1986). Commentators have noted that improper conduct "includes acts that are actionable in and of themselves—trespass, breach of contract, conversion of physical property, and, under modern laws, the misuse of computer networks." Risch, *supra* note 150, at 10.

153. *See id.* at 15. The type of remedy awarded under an action for misappropriation of a trade secret varies depending on the court. 14 Am. Jur. Proof of Facts 3d *Misappropriation of Trade Secret under the Restatement of Torts* § 19 (1991) (explaining the damages that plaintiffs may typically recover in trade secrets cases and highlighting common methods for determining compensation).

154. *See, e.g.*, Meehan v. Shaughnessy, 535 N.E.2d 1255, 1266-67 (Mass. 1989) (holding that the employee owed a duty of loyalty to the employer); Chelsea Indus., Inc. v. Gaffney, 449 N.E.2d 320, 327 (Mass. 1983) (same); Cameco, Inc. v. Gedicke, 724 A.2d 783, 789 (N.J. 1999) (same).

155. Benjamin Aaron & Matthew Finkin, *The Law of Employee Loyalty in the United States*, 20 COMP. LAB. L. & POL'Y J. 321, 322 (1999).

156. DSG Corp. v. Anderson, 754 F.2d 678, 682 (6th Cir. 1985).

157. *See supra* Part I.B.

158. *See supra* Part I.C. Under the intended-use theory, it would be difficult for employees to know in any given instance whether their computer use is authorized or not. *See* United States v. Nosal, 642 F.3d 781, 790 (9th Cir. 2011), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012). In other words, unless the employer issues a detailed company policy handbook, it would be challenging to know whether a particular behavior constitutes a crime. *Id.* Broad interpretations of the CFAA implicate criminal consequences when the policies are not "necessarily drafted with the definiteness

potentially criminalize a wide swath of otherwise-innocent behaviors such as, online shopping or checking social networking profiles from a work computer, which may be adverse to an employer's interest, but are far from criminal.[159] The *WEC Carolina Energy Solutions* court highlighted the deficiencies in both of these broad interpretations. The court explained that under these interpretations, "any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems. "[160] An interpretation that raises such serious public policy concerns cannot have been what Congress intended or what courts should allow.

IV. CONCLUSION

Courts and scholars have struggled with how to best interpret the CFAA's authorization language. The two broad interpretations, agency and intended use theory, may offer the employer an easy solution for combating employee misappropriation of company information, but in practice, these judicial interpretations give employers extraordinary discretion in defining what constitutes criminal activity. The *WEC Carolina Energy Solutions* court and others following the narrow access means access theory have attempted to find a workable balance between enforcement and flexibility. The access means access theory provides the best approach for determining the scope of the CFAA in the workplace environment. This issue is very important and, if not addressed, will continue to cause confusion as a result of conflicting circuit court opinions.

---

or precision that would be requires for a criminal statue." *Id.* The void-for-vagueness doctrine "requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983). Other commentators have argued that the void-for-vagueness doctrine requires courts to adopt the narrow interpretation of the CFAA. *See* Kerr, *supra* note 40 (arguing that due to the CFAA's broad reach, a broad reading of the statute could "render it unconstitutional" by providing "insufficient notice of what is prohibited or fail[ing] to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process of the law").

159. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013); *Nosal*, 676 F.3d at 860. Just because an activity distracts someone from her work does not mean that she should be held criminally liable. This result is disproportionately harsh.

160. *WEC Carolina Energy Solutions LLC*, 687 F.3d at 206.