Berkeley
technology law journal
ANNUAL REVIEW OF LAW AND TECHNOLOGY

Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"

David J. Rosen

VOLUME 27
AR ONLINE
2012

UNIVERSITY OF CALIFORNIA, BERKELEY
SCHOOL OF LAW
BOALT HALL

LIMITING EMPLOYEE LIABILITY UNDER THE CFAA: A CODE-BASED APPROACH TO "EXCEEDS AUTHORIZED ACCESS"

David J. Rosen[†]

David Nosal was a senior executive at Korn/Ferry International, an executive search firm.[1] Upon his resignation from Korn/Ferry in 2004, Nosal agreed to serve as a consultant for one year in exchange for monthly payments of $25,000. The consultancy contract included a provision that prohibited Nosal from competing with Korn/Ferry for the duration of the agreement.[2]

While still under contract, Nosal allegedly conspired with three Korn/Ferry employees to obtain source lists, names, and contact information from the company's proprietary "Searcher" database.[3] The employees possessed valid user names and passwords that allowed them to access the data in Searcher.[4] All of the employees, however, had signed agreements that specified that the information in Searcher could be used only for "legitimate Korn/Ferry business."[5]

Korn/Ferry became suspicious when an audit revealed that the employees had downloaded an unusually large number of records from Searcher.[6] After conducting an investigation and learning that Nosal had obtained source lists and other client contact information from the database, Korn/Ferry filed a civil suit against Nosal and his accomplices, in state court,

---

† J.D. Candidate, 2013, University of California, Berkeley School of Law.

1. United States v. Nosal (*Nosal I*), No. CR 08-00237, 2009 WL 981336, at *1 (N.D. Cal. Apr. 13, 2009).

2. *Id.*

3. *Id.*

4. *Id.* at *4.

5. United States v. Nosal (*Nosal*), 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011).

6. *See* Declaration of Dan Demeter in Support of Plaintiff Korn/Ferry International's Ex Parte Applications for Temporary Restraining Order and Order to Show Cause and for Leave to Take Expedited Discovery at 1–4, Korn/Ferry Int'l v. Becky Christian, No. CIV 448606 (Cal. Supr. Ct. San Mateo Cnty. Aug. 3, 2005).

for theft of trade secrets.[7] In addition, Korn/Ferry notified the federal authorities of the alleged theft.[8] The FBI began a criminal investigation, which led to an indictment by a federal grand jury.[9] The indictment, not surprisingly, charged Nosal with the theft of Korn/Ferry's proprietary information.[10] But the indictment charged Nosal with more than substantive trade secret crimes: it also charged him with violating the Computer Fraud and Abuse Act ("CFAA"), a law enacted in the 1980s to address the problem of computer hacking.[11]

The charges against Nosal are part of a trend. For years, criminal prosecutions under the CFAA primarily targeted hackers and other outsiders who accessed computers "without authorization."[12] Recently, however, the government has begun to use the CFAA to prosecute employees who "exceed[] authorized access" on their employers' computers.[13] Unlike the targets of past CFAA prosecutions, these employee defendants have not misused a computer to obtain information that they are not authorized to access. Rather, they have obtained information with authorized access and

7. Complaint, Korn/Ferry Int'l v. Becky Christian, No. CIV 448606 (Cal. Supr. Ct. San Mateo Cnty. Aug. 2, 2005); *see also* Joann S. Lublin, *A Company And Its Secrets*, WALL ST. J., Aug. 16, 2005, at B1.

8. *Nosal I*, 2009 WL 981336, at *1.

9. *Id.* at *2.

10. The indictment charged Nosal and one of his accomplices, Becky Christian, with the theft and misappropriation of trade secrets in violation of the Economic Espionage Act. *See Nosal I*, 2009 WL 981336, at *2. Christian eventually reached a plea agreement with the government, leaving Nosal as the only defendant at trial. The indictment also included several mail fraud charges, which were later dismissed. *See id.* at *7–9.

11. *See* H.R. REP. NO. 98-894, at 10–11, 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695–97, 3706 (focusing on "hackers" who "trespass into" computer systems); S. REP. NO. 99-432 at 2–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480–81 (discussing a "group of adolescents" who "broke into" a medical center's computer system and gained access to patients' medical records).

12. *See, e.g.*, United States v. Lindsley, 254 F.3d 71 (5th Cir. 2001) (prosecuting defendants who "used their personal computers to illegally access Sprint Corporation's . . . computer system" to obtain Sprint calling card numbers); United States v. Petersen, 98 F.3d 502, 504 (9th Cir. 1996) (prosecuting defendant for " 'hacking' into credit reporting services"); United States v. Morris, 928 F. 2d 504 (2d Cir. 1991) (prosecuting defendant who exploited vulnerabilities in various programs to launch worms that harmed hundreds of computers on the internet).

13. *See, e.g.*, *Nosal*, 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Zhang, No. CR-05-00812, 2011 WL 4954152, at *1 (N.D. Cal. Oct. 18, 2011); *see also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1583 (2010) [hereinafter Kerr, *Vagueness Challenges*] ("In the last five years, cases applying the CFAA to allegedly disloyal employees have become by far the most common type of CFAA case.").

then used the information in a manner that violated their employers' use policies.[14]

In the prosecution of David Nosal, the government's theory was that Nosal and his accomplices exceeded authorized access to Searcher when they obtained information from the database for a purpose not permitted by the terms of their access.[15] In *United States v. Nosal*, a divided Ninth Circuit panel essentially accepted the government's theory, holding that an employee "exceeds authorized access" when the employee violates his employer's explicit restrictions regarding the use of information on his employer's computer.[16] If Nosal's accomplices had notice of the policy that restricted their use of Searcher to "legitimate Korn/Ferry business," and if the accomplices violated this policy when they obtained information from Searcher for the purpose of starting a competing firm, then they exceeded authorized access to Searcher.[17]

Judge Campbell dissented. The majority's construction of "exceeds authorized access," Judge Campbell argued, is inconsistent with the purpose of the CFAA, which was designed to prevent "computer crimes" such as "hacking."[18] Judge Campbell noted that the majority's interpretation would, contrary to Congress's intent, "proscribe fraud (a standalone crime) that happens to be effectuated through the use of a computer and in violation of a computer use policy."[19]

Judge Campbell is not the first judge to conclude that the CFAA should not criminalize the mere violation of an employer's use restrictions.[20] But Judge Campbell's reading of the statute raises a difficult question: If the

---

14. *See* discussion *infra* Section II.C.1.

15. *See* Brief for the United States at 19, *Nosal*, 642 F.3d 781 (No. 10–10038). The government did not allege that Nosal directly accessed Searcher; rather, Nosal's liability under the CFAA was premised on both *Pinkerton* liability and an "aiding and abetting" theory. *See id.* at 4 n.4.

16. *Nosal*, 642 F.3d at 783.

17. *Id.* at 783–84. After the panel's judgment, Nosal successfully petitioned for rehearing en banc. United States v. Nosal, 661 F.3d 1180 (9th Cir. 2011). At the time of this writing, the ruling of the en banc panel is pending.

18. *Nosal*, 642 F.3d at 789 (Campell, J., dissenting).

19. *Id.* at 791.

20. *See, e.g.*, Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) ("It would be imprudent to interpret the CFAA, in a manner inconsistent with its plain meaning, to transform the common law civil tort of misappropriation of confidential information into a criminal offense."); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) ("[T]he CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); Lockheed Martin Co. v. Kelly, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *1, *5 (M.D. Fla. Aug. 1, 2006) (holding that § 1030(a)(4) addresses access to information, not use of information).

CFAA's "exceeds authorized access" language does not cover the misuse of information, then what does the language cover? What does it mean to "exceed authorized access" on a computer? If a person is authorized to access a computer, how does the person exceed her authority if not by misappropriating or misusing information obtained from the computer?

Judges and scholars have yet to provide satisfactory answers to these questions. Some courts, for example, have concluded that the term "exceeds authorized access" regulates employees who exceed limits on access to information, not limits on use of information.[21] When defending this interpretation, these courts have offered incomplete explanations and hypotheticals that make it difficult to understand what limits on access might look like and how a computer user would exceed those limits.[22]

Meanwhile, the leading scholarly approach to interpreting the CFAA—the "code-based" theory—focuses primarily on outsiders who access computers "without authorization."[23] Under a code-based theory, a user acts without authorization by circumventing code that regulates access to a computer.[24] Defenders of the theory, however, do not explain in any detail how or if a code-based interpretation might apply to an employee who "exceeds authorized access" on an employer's computer, thus exposing the theory to the criticism that it effectively reads the phrase "exceeds authorized access" out of the statute.[25]

This Note attempts to explain how a code-based reading of "exceeds authorized access" can be consistent with the text and purpose of the CFAA. The Note expands on the code-based theory in the employer-employee

---

21. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); United States. v. Nosal (*Nosal II*), No. C 08-0237, 2010 WL 934257 at *1, *6 (N.D. Cal. Jan. 6, 2010), *rev'd*, 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011); *Lockheed*, 2006 WL 2683058, at *5.

22. *See* discussion *infra* Part II.D.

23. *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2254–58 (2004); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) [hereinafter Kerr, *Cybercrime's Scope*].

24. Kerr, *Cybercrime's Scope*, *supra* note 23, at 1642.

25. *See, e.g.*, Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW 1395, 1419 (2007) ("Unfortunately, code based readings of unauthorized access are flatly inconsistent with the explicit language of an unauthorized access statute such as the CFAA, which makes a clear distinction between 'unauthorized access' and 'access in excess of authorization.' "); *see also* Brief for the United States at 19, United States v. John, 597 F.3d 263 (5th Cir. 2010) (No. 08–10459) ("[A code-based interpretation] would mean that any employee with access to a computer system . . . could do anything while using that access and not run afoul of the 'exceeds authorized access' prong of the statue [sic]. . . . This would essentially read the 'exceeds authorized access' prong of the statute out of existence and leave only the 'without authorization' with any meaning.").

context, explaining how an employee can exceed authorized access by bypassing technical barriers to employer-maintained computer systems and applications. The discussion demonstrates that the Ninth Circuit's "misappropriation" interpretation, which is shared by at least two other circuits,[26] is not necessary to preserve the meaning of the phrase "exceeds authorized access" in the statute.

This Note proceeds in three parts. Part I summarizes the text and history of the phrase "exceeds authorized access" in various provisions of the CFAA. Part II surveys different scholarly and judicial approaches to defining "authorization" in the CFAA. Two of the judicial approaches have transformed the CFAA, a computer misuse statute, into a broader law that regulates various forms of employee misconduct. Finally, Part III offers a proposal for interpreting the phrase "exceeds authorized access" in the employer-employee context. The proposal preserves the distinction between acting without authorization and in excess of authorization, respects the legislative intent to distinguish between outsiders and insiders, and focuses on prohibiting computer misuse.

I. OVERVIEW OF "EXCEEDS AUTHORIZED ACCESS" IN THE CFAA

A. STATUTORY TEXT

The Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030, identifies seven distinct crimes in seven subsections of § 1030(a). Three of those subsections—§§ 1030(a)(1), (a)(2) and (a)(4)—include the phrase "exceeds authorized access."[27] Section 1030(a)(1), which covers obtaining classified information to injure the United States, has never been used.[28] Both §§ (a)(2) and (a)(4), on the other hand, arise frequently in criminal and civil contexts.

26. *See* discussion *infra* Section II.C.1.

27. 18 U.S.C. § 1030 (2010).

28. *See* ORIN S. KERR, COMPUTER CRIME LAW 27 (2d ed. 2009) [hereinafter KERR, COMPUTER CRIME LAW].

Section 1030(a)(2) subjects to punishment anyone who:

> intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> [. . .]
>
> (C) information from any protected computer.[29]

The CFAA does not include a definition of "without authorization."[30] The statute does, however, provide a definition of "exceeds authorized access." According to § 1030(e)(6), the term "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[31]

Subsection 1030(a)(2)(C) exposes to liability those who obtain "information from any protected computer."[32] The definition of "protected computer" is very broad. The term encompasses a computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"[33] In recent years, several courts have concluded that any computer connected to the Internet is a "protected computer."[34] Today, the CFAA covers practically every workplace computer in the United States.[35]

Punishments for violations of § 1030(a)(2) vary. Most violations are punished as misdemeanors.[36] Some violations, however, may be charged as felonies if the offense was committed for purposes of commercial advantage

---

29. 18 U.S.C. § 1030(a)(2).

30. See Part II, *infra*, for a discussion of how courts have formulated approaches to this definitional vagueness.

31. 18 U.S.C. § 1030(e)(6).

32. *Id.* § 1030(a)(2)(C).

33. *Id.* § 1030(e)(2)(B). Section (e)(2)(A) states that a "protected computer" can also be a computer that is "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government."

34. *See, e.g.*, Multiven, Inc. v. Cisco Systems, Inc., 725 F. Supp. 2d 887, 892 (N.D. Cal. 2010) (concluding that a computer is "protected" within the meaning of the CFAA if it is connected to the internet); National City Bank v. Prime Lending, Inc., No. CV-10-034-EFS, 2010 WL 2854247, at *1, *4 n.2 (E.D. Wash. July 19, 2010) (stating that "any computer connected to the internet is a protected computer").

35. *See* Kerr, *Vagueness Challenges*, *supra* note 13, at 1570–71.

36. *See* 18 U.S.C. § 1030(c)(2)(A).

or private financial gain, in furtherance of any criminal or tortious act, or if the value of the information obtained exceeded $5,000.[37]

Section 1030(a)(4), the provision of the CFAA at issue in *Nosal*, contains many of the same terms as § 1030(a)(2). Section 1030(a)(4) subjects to punishment anyone who:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.[38]

Like section 1030(a)(2), section 1030(a)(4) covers one who accesses without authorization, or exceeds authorized access on, a protected computer. There are, however, significant differences between the two sections. Whereas the mens rea required under § 1030(a)(2) is simple intent, the mens rea required under § 1030(a)(4) is "knowingly and with intent to defraud."[39] Furthermore, punishments are generally more severe under § 1030(a)(4). All violations of § 1030(a)(4) are felonies.[40]

Finally, the CFAA offers civil remedies to those who suffer damages as a result of violations of the law, including violations of §§ 1030(a)(2) and (a)(4). Section 1030(g) states that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[41] Although the CFAA is primarily a criminal statute, most of the cases that hinge on the meaning of "unauthorized access" or "exceeds authorized access" in the workplace arise in the civil context.[42]

---

37. *Id.* § 1030(c)(2)(B).
38. *Id.* § 1030(a)(4).
39. *Id.*
40. *See id.* § 1030(c)(3).
41. *Id.* § 1030(g).
42. *See, e.g.*, Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378 (S.D.N.Y. 2010) (considering advertising company's claim against its employee for accessing information in the company's database and then giving it to a competitor); Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122 (E.D. Cal. 2008) (considering prosthetic care company's claim against its former employees for obtaining patient lists from the company's computers for the purpose of starting a competing company); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008) (considering Black & Decker's claim against its employee for copying proprietary information from Black & Decker's computer and then sharing that information with a competitor); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087 (N.D. Cal. 2006) (considering

B. LEGISLATIVE HISTORY

In 1984, Congress passed the Comprehensive Crime Control Act. This Act included three provisions that later became part of the CFAA,[43] including an early version of § 1030(a)(2) that prohibited a person from accessing a computer without authorization to obtain information contained in a financial record of a financial institution.[44] The legislative record indicates that Congress designed the provisions to deter various forms of computer hacking.[45] Similar to the current version of §1030(a), each provision prohibited accessing a computer "without authorization."[46] None of the provisions, however, included the phrase "exceeds authorized access." In the place where "exceeds authorized access" is today, the text read: "[o]r having accessed a computer with authorization, uses the opportunity such access provides for purposes to which authorization does not extend."[47]

Two years later, Congress passed the CFAA, which amended most of the substantive provisions of 18 U.S.C. § 1030.[48] Congress replaced the phrase "[h]aving accessed a computer with authorization, uses the opportunity such access provides for purposes to which authorization does not extend" with the phrase "exceeds authorized access" in § 1030(a)(2).[49] In addition to revising the existing provisions of § 1030, Congress added several new computer crimes, including the felony provision for fraud in § 1030(a)(4), which included the term "exceeds authorized access" as well.[50]

The legislative history contains little indication of what Congress intended when it added the term "exceeds authorized access." The 1986 Senate Report that accompanied the bill is largely unhelpful: it describes the term as "self-explanatory."[51] Perhaps because of the sparse legislative record, judges generally steer clear of the CFAA's legislative history when

electrical engineering company's claim against its employee for deleting files from the company's server and the employee's company-issued laptop).

43. *See* H.R.J. Res. 648, 98th Cong. (1984) (enacted).

44. 18 U.S.C. § 1030(a)(2) (Supp. II 1985).

45. *See* H.R. REP. NO. 98-894, at 10–11, 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695–97, 3706 (focusing on "hackers" who "trespass into" computer systems).

46. 18 U.S.C. § 1030(a)(1)–(3).

47. *Id.* For a more detailed history of the Comprehensive Crime Control Act of 1984, see Kerr, *Vagueness Challenges*, *supra* note 13, at 1563–64.

48. H.R.J. Res. 4718, 99th Cong. (1986) (enacted).

49. *Id.*

50. 18 U.S.C. § 1030(a)(4) (Supp. IV 1987).

51. S. REP. NO. 99-432 at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2491.

interpreting the meaning of "exceeds authorized access" in §§ 1030(a)(2) and (a)(4).[52]

Although judges tend to avoid discussing the CFAA's legislative history, advocates are not as reticent. In its briefing for *Nosal*, the government focused on the original language in 18 U.S.C. § 1030: "[h]aving accessed a computer with authorization, uses the opportunity such access provides for purposes to which authorization does not extend."[53] The government argued that this language "specifically discussed accesses in violation of purpose-based restrictions" and therefore encompassed Nosal's conduct.[54] Congress later substituted the phrase "exceeds authorized access," the government reasoned, because it was a "shorter" and "simpler" way of expressing the same idea.[55] The Electronic Frontier Foundation ("EFF"), on the other hand, examined the CFAA's legislative history and reached the opposite conclusion. In an amicus brief in support of Nosal, EFF argued that Congress amended the statute in 1986 to eliminate the possibility that a court would find a computer user liable for the mere misuse of information.[56] According to EFF's reading of the legislative history, Congress substituted the phrase "exceeds authorized access" to make clear that the CFAA covered those who exceeded access restrictions, not use restrictions.[57] Against the backdrop of the CFAA's thin legislative history, both the government's and EFF's interpretations are defensible.

Although it is unclear if Congress intended for the phrase "exceeds authorized access" to address acts of information misuse, there is some evidence suggesting that Congress was attempting to distinguish between "insiders, who are authorized to access a computer," and "outside hackers who break into a computer."[58] In explaining why §§ 1030(a)(3) and (a)(5) did not include the term "exceeds authorized access," a 1986 Senate Report stated that those provisions were aimed exclusively at outsiders.[59] The

52. *But see* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) ("The legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.").

53. 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985).

54. Reply Brief for the United States at 10–11, *Nosal*, 642 F.3d 781 (9th Cir. 2011) (No. 10–10038).

55. *See id.* at 11.

56. Brief for Electronic Frontier Foundation as Amici Curiae Supporting Appellee at 6–7, *Nosal*, 642 F.3d 781 (9th Cir. 2011) (No. 10–10038).

57. *See id.*

58. *See* S. REP. NO. 104-357, at 11 (1996).

59. *See* S. REP. NO. 99-432, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, at 2488.

reasonable inference is that Congress aimed the "exceeds authorized access" prongs of §§ 1030(a)(2) and (a)(4) at insiders, not outside hackers.[60]

II. APPROACHES TO INTERPRETING "AUTHORIZATION" IN THE CFAA

Since 2010, three federal circuit courts have issued rulings where a defendant's criminal liability turned on the meaning of "exceeds authorized access" in the CFAA.[61] Before discussing these recent decisions, it will be helpful to survey the different approaches to interpreting the "without authorization" language that appears in most provisions of the CFAA. Sections (a)(2) and (a)(4)—the two subsections of the CFAA under which defendants have been prosecuted for exceeding authorized access on a computer—also prohibit accessing a computer "without authorization."[62] It is difficult to discuss the meaning of "exceeds authorized access" without examining what it means to access a computer with or without authorization. Accordingly, this Part first reviews different approaches to defining "authorization," and then moves to recent judicial readings of "exceeds authorized access."

First, this Part describes the "code-based" approach to authorization. Although the code-based approach tracks well with the early criminal cases decided under the CFAA, courts have been reluctant to use the approach in cases concerning an employee's alleged misuse of a workplace computer. Second, this Part reviews the "agency approach" to authorization—which, despite being endorsed only by the Seventh Circuit, has influenced district court judges in various circuits around the country. Third, this Part turns to the "employer-policy" approach, recently adopted by three circuit courts, that seeks to distinguish acting without authorization from acting in excess of authorization on computers in the workplace. Finally, this Part discusses an unsuccessful—or at least incomplete—attempt by a federal district court to limit the scope of "exceeds authorized access" in the employer-employee context.

---

60. *See* United States v. Phillips, 477 F. 3d 215, 219 (5th Cir. 2007) (relying on legislative history to support the argument that Congress intended to distinguish "insiders . . . who are authorized to access a computer" from "outside hackers who break into a computer").

61. *Nosal*, 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010).

62. *See supra* Section I.A.

A. THE "CODE-BASED" APPROACH

1. Description

In a 2003 law review article, Professor Orin Kerr advocated a "code-based" approach to access and authorization in computer misuse statutes.[63] Under the code-based approach, a user acts without authorization only by circumventing code that regulates access to a computer.[64] The approach has two primary virtues. First, the code-based approach comports with the CFAA's general goal of regulating specific computer use crimes. Circumventing code is a form of the "hacking" that precipitated the enactment of the computer misuse crimes in 18 U.S.C. § 1030.[65] Second, the code-based approach avoids some of the constitutional pitfalls of other approaches to authorization, which risk rendering the access provisions of the CFAA unconstitutional on overbreadth or vagueness grounds.[66] In contrast to the agency and employer-policy approaches, the code-based approach criminalizes a relatively narrow range of conduct.[67]

According to Professor Kerr, there are two ways in which a user can circumvent code and thus access a computer without authorization. First, a computer user can "engage in false identification" by using another person's credentials to obtain access to a computer.[68] The user could, for example, steal or guess another user's password and then use it to sign on to the computer.[69]

The second way a user can circumvent code is by exploiting a vulnerability in the code to gain access to a computer.[70] The facts of *United States v. Morris*,[71] one of the first cases decided under the CFAA,[72] illustrate how a computer user can exploit such a vulnerability. Robert Morris, a computer science graduate student at Cornell University, had coded and launched an internet "worm" that exploited vulnerabilities in the "send mail" and "finger" programs.[73] The worm replicated itself and spread via the Internet, interfering with the operation of thousands of computers at

63. Kerr, *Cybercrime's Scope*, *supra* note 23.
64. *Id.* at 1642.
65. *See supra* note 11.
66. *See infra* Sections II.A.2, II.C.2.
67. *See* Bellia, *supra* note 23, at 2258.
68. Kerr, *Cybercrime's Scope*, *supra* note 23, at 1645.
69. *See id.* at 1645, 1664.
70. *Id.*
71. 928 F. 2d 504, 510 (2d Cir. 1991).
72. Kerr, *Cybercrime's Scope*, *supra* note 23, at 1645.
73. *Morris*, 928 F. 2d at 506.

universities, military sites, and medical research facilities.[74] The cost of repairing the effects of the worm on each computer ranged from $200 to $53,000.[75]

The government charged Morris with violating § 1030(a)(5)(A) of the CFAA, which, at the time, penalized the conduct of an individual who "intentionally accesses a Federal interest computer without authorization."[76] Morris maintained that his actions were not without authorization. He had valid user accounts on several computers on the Internet, each of which gave him authorized access to the sendmail and finger programs.[77] Morris argued that his use of these programs was not "without authorization" and thus could not serve as a basis for convicting him under § 1030(a)(5)(A).[78]

The Second Circuit rejected Morris's argument, holding that an individual accesses a computer without authorization when using a computer's features in ways unrelated to their intended function.[79] The sendmail program is intended to send e-mail; the finger program is intended to look up the directory information of other computer users.[80] Instead of using these programs for these intended functions, Morris "found holes in both programs that permitted him a special and unauthorized access route into other computers."[81] Thus, Morris had accessed these other computers without authorization.[82]

2. Problems with the Code-Based Approach

The principle criticism of the code-based approach is that it reads the phrase "exceeds authorized access" out of the CFAA. Critics of the approach assert that code-based restrictions can only prevent unauthorized access; these restrictions cannot regulate those who act in excess of authorization.[83] Although Professor Kerr implies that the phrase "exceeds authorized access" could govern "an insider who circumvents code-based restrictions,"[84] he

74. *Id.*
75. *Id.*
76. *See id.*
77. In addition to his access at Cornell, Morris had authorized access to computers at Harvard and UC Berkeley. *Id.* at 509.
78. *Id.* at 507.
79. *Id.* at 510.
80. *Id.* at 507.
81. *Id.* at 510.
82. *Id.*
83. *See* sources cited *supra* note 25.
84. Kerr, *Cybercrime's Scope, supra* note 23, at 1663.

does not offer examples of such restrictions or describe how an insider would circumvent them.[85]

Other advocates of the code-based approach are skeptical of its relevance to the phrase "exceeds authorized access." Patricia Bellia, for example, suggests that non-code-based restrictions could be relevant in defining conduct that exceeds authorized access under the CFAA:

> Some provisions of the CFAA . . . also contemplate conduct that "exceed[s] authorized access," and it is conceivable that restrictions in policy statements or terms of use should be relevant there. Because such provisions are designed to target activities by persons whose access to the system is not constrained by code in the same way as the general public's, such provisions align with a reading of "access[] without authorization" that depends on breach of code-based limitations on access.[86]

As Section II.C discusses, three circuit courts found that "restrictions in policy statements or terms of use" were highly relevant in identifying the sort of conduct that exceeds authorized access under the CFAA.[87] The next Section, however, discusses an approach to authorization where a computer user's access can become unauthorized even if the user has not breached a code-based barrier or violated a use policy.

B. THE AGENCY APPROACH

1. Description

Judge Posner popularized the agency approach in *International Airport Centers v. Citrin*.[88] In *Citrin*, an employer sued a former employee for violating the "computer damage" provision of the CFAA, which subjects to liability anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[89] Citrin, the

85. Kerr states that "it is not clear whether 'exceeding authorized access' governs an insider who breaches contract-based restrictions or an insider who circumvents code-based restrictions." *Id.* at 1663. Kerr suggests that courts should resolve this ambiguity in favor of criminal defendants: "If we interpret the phrase 'exceeds authorized access' to include breaches of contract, we create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment." *Id.*

86. Bellia, *supra* note 23, at 2254.

87. *See infra* Section II.C.1.

88. 440 F.3d 418 (7th Cir. 2006).

89. *Id.* at 419 (quoting 18 U.S.C. § 1030(a)(5)(A) (2006)).

employee, used a laptop provided by his employer.[90] Citrin decided to quit and start his own business in violation of his employment contract.[91]

Before Citrin returned the laptop to his employer, he used a "secure erasure" program to delete all the files on his laptop.[92] The program prevented the employer from restoring the deleted files. The Seventh Circuit considered, among other issues, whether Citrin had accessed his laptop "without authorization" when he deleted the files.[93]

The Seventh Circuit held that Citrin's authorized access to the laptop ceased as soon as he breached a common law "agency" duty of loyalty to his employer.[94] Even though Citrin was still an employee when he accessed his laptop, and even though his employer had no policy prohibiting him from deleting files in the manner that he did, his access was without authorization. "[Citrin's] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit [his employer] in violation of his employment contract, he resolved to destroy files that . . . [were] the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee."[95] In the wake of *Citrin*, several district courts adopted this "agency" theory of unauthorized access.[96]

2. Problems with the Agency Approach

There are two significant problems with the agency approach. First, the approach might violate the due process clause of the Fourteenth Amendment under the void-for-vagueness doctrine.[97] As Professor Kerr has argued, the agency approach "gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited."[98] Furthermore, the approach would "encourage arbitrary and discriminatory enforcement" due to the lack of clear guidelines for law enforcement.[99]

---

90. *Id.* at 419.
91. *See id.*
92. *Id.*
93. *Id.*
94. *Id.* at 420.
95. *Id.*
96. *See, e.g.*, *Nosal I*, No. CR 08-00237, 2009 WL 981336, *1, *4 (N.D. Cal. Apr. 13, 2009); Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008); Calyon v. Mizuho Sec. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, *1 (S.D.N.Y. Sept. 7, 2007); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006).
97. *See* Kerr, *Vagueness Challenges*, *supra* note 13, at 1585–86.
98. *Id.* at 1586.
99. *Id.*

The second problem is that the agency approach, if applied to the text of §§ 1030(a)(2) and (a)(4), would collapse the distinction between "without authorization" and "exceeds authorized access."[100] If an employee's authorization to access a computer ceases as soon as she does something that is not in her employer's interests, then "exceeds authorized access" likely becomes textually superfluous and meaningless.[101] Judge Posner anticipated this objection, writing that the difference between "exceeds authorized access" and "without authorization" is "paper thin . . . but not quite invisible."[102] In support of his claim that "exceeds authorized access" is still textually relevant under his interpretation, he pointed to *EF Cultural Travel BV v. Explorica, Inc.*[103]

EF Cultural Travel concerned a dispute between two "tour companies" with online presences.[104] Several employees of one of the tour companies, EF, left to join another tour company, Explorica. While at Explorica, a former EF employee helped the company build a web site "scraper" that culled pricing information from EF's web site.[105] The scraper used "tour codes" provided by the former EF employees. The significance of these codes "was not readily understandable to the public."[106] Furthermore, the codes were, according to EF, proprietary information and covered by confidentiality agreements.[107] Explorica ran the scraper twice, downloading 60,000 lines of data, which Explorica then used to "systematically undercut EF's prices."[108]

The First Circuit considered whether the use of the scraper "exceed[ed] authorized access" to EF's computer under § 1030(a)(4).[109] The court found that the former employee exceeded his authorized access when he used proprietary information to help build an "efficient" scraper that accessed his former employer's web site.[110] Judge Posner, in *Citrin*, described the holding of *EF Cultural Travel* as follows: "The website was open to the public, so [the defendant] was authorized to use it, but he exceeded his authorization by

100. 18 U.S.C. §§ 1030(a)(2), (4) (2010).
101. *See* KERR, COMPUTER CRIME LAW, *supra* note 28, at 69.
102. Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).
103. *Id.*
104. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).
105. *Id.*
106. *Id.*
107. *Id.* at 582–83.
108. *Id.* at 580.
109. The First Circuit did not resolve the question of whether the use of the scraper was "without authorization" under § 1030(a)(4). *See id.* at 582 n.10.
110. *Id.* at 583.

using confidential information to obtain better access than other members of the public."[111]

Judge Posner's reading of *EF Cultural Travel,* combined with his agency approach, results in an interpretation of "exceeds authorized access" that seems to frustrate the intent of Congress. As discussed in Section I.B, *supra*, the legislative history suggests that the term "unauthorized access" regulates outsiders while the term "exceeds authorized access" regulates insiders.[112] Judge Posner's approach inverts this understanding. If a current employee, an insider, is accessing an employer's computer, she can never exceed authorized access: as soon as she breaches her common law duty of loyalty to her employer, her access becomes unauthorized. But a former employee—one who is now outside the company—can exceed authorized access by accessing a computer that is "open to the public."[113]

C. THE EMPLOYER-POLICY APPROACH

1. Description

After *Citrin*, many courts refused to embrace the agency approach.[114] Some of these same courts, however, held that employers had the right to define the limits of authorization on their computers, and that employees could be liable under the CFAA for exceeding those limits. For these courts, the problem with the agency approach was that it failed to provide employees with sufficient notice of what activities would render their access without authorization.[115] An employer is free to define authorization according to its interests, but it must communicate those interests in the form of a written use policy.[116] This "employer-policy" approach paved the

111. Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

112. *See supra* note 58.

113. *See* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *1, *6 (M.D. Fla. Aug. 1, 2006) (arguing that *Citrin* turned "the plain reading of the statutory definition of 'exceeds authorized access' on its head" because Congress aimed the phrase at the company insider).

114. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) ("[N]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer.").

115. *See, e.g.*, *Nosal*, 642 F.3d 781, 786 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011) ("How is an employee supposed to know when authorization has been revoked if the employer does not inform the employee of the revocation?").

116. *See id.* at 787–88.

way for three different circuit courts to find employees liable under the CFAA for exceeding authorized access on workplace computers.[117]

In *United States v. John*, the Fifth Circuit interpreted the meaning of "exceeds authorized access" in the context of a criminal prosecution of a bank employee who misused account information to which she had access.[118] The defendant, Dimetriace John, was an account manager at Citigroup.[119] John accessed and printed information pertaining to over seventy corporate customer accounts. She provided the information to her half-brother, who in turn used it to incur fraudulent charges.[120] John was convicted of, among other crimes, "exceeding authorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C)."[121]

On appeal, the Fifth Circuit considered John's argument that § 1030(a)(2) does not prohibit "unlawful *use* of material that she was authorized to access through authorized use of a computer."[122] Instead, John contended, the term "exceeds authorized access" in § 1030(a)(2) applies only to using authorized access to obtain information that an employee is not entitled to obtain or alter information that the employee is not entitled to alter.[123] In rejecting John's argument, the Fifth Circuit held that authorization "may encompass limits on the use of information obtained by permitted access to a computer system and data available on that system."[124]

The Fifth Circuit's opinion makes it difficult to identify its precise holding. On the one hand, the court placed significant weight on the fact that John's misuse of the information was contrary to Citigroup employee policies.[125] The government, the court stressed, demonstrated that Citigroup's policies were reiterated in training programs, and that John was aware of the policies.[126] There is, however, language in the opinion that suggests that the Fifth Circuit would be reluctant to find that an employee exceeds authorized access on her employer's computer whenever she violates a computer use policy. At one point, the court seems to limit its holding to instances in

117. Other commentators have described similar judicial approaches as examples of "contract-based interpretation" of authorization under the CFAA. *See, e.g.*, Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 827–29 (2009).

118. 597 F.3d 263, 269 (5th Cir. 2010).

119. *Id.*

120. *Id.*

121. *Id.* at 270.

122. *Id.* at 271 (emphasis in original).

123. *Id.*

124. *Id.*

125. *See id.* at 272.

126. *Id.*

which the access is "in furtherance of or to perpetuate a crime."[127] It is possible to read *John* as requiring the government to establish a violation of a clear employee use policy *and* an intent to commit a separate crime.[128]

The Eleventh Circuit rejected this reading of *John* in *United States v. Rodriguez*.[129] There, the government prosecuted a Social Security Admiration ("SSA") employee, under the CFAA, for using the agency's computer to access records of women he was romantically interested in.[130] The Eleventh Circuit concluded that the employee exceeded his authorized access under § 1030(a)(2) when he accessed personal records for non-business reasons, in violation of SSA policies.[131] The employee argued that he was not liable under the CFAA because, in contrast to the defendant in *John*, his use of the obtained information was not criminal.[132] The Eleventh Circuit was unpersuaded.[133] John exceeded authorized access, the Eleventh Circuit concluded, when he violated Citigroup policies while accessing a Citigroup computer.[134] Similarly, Rodriguez exceeded his authorized access when he obtained personal information from a SSA computer in violation of SSA policies.[135]

In *United States v. Nosal*, discussed in the Introduction, *supra*, the Ninth Circuit employed essentially the same interpretation of "exceeds authorized access" as the Eleventh Circuit in *Rodriguez*. An employee exceeds authorized access, the Ninth Circuit held, when he violates his employer's policies governing the use of information on the employer's computers.[136] However, unlike the Fifth and Eleventh Circuits, the Ninth Circuit in *Nosal* had to distinguish a recent decision by another panel in its circuit.

Two years before the *Nosal* decision, a different Ninth Circuit panel decided *LVRC Holdings LLC v. Brekka*.[137] There, the operators of a residential treatment center ("LRVC") brought a civil suit against Brekka, a former employee.[138] While working at LRVC, Brekka had emailed "a master

127. *Id.* at 271.

128. *See* Brief for the Appellant at 10–11, United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (No. 09–15265).

129. 628 F.3d 1258 (11th Cir. 2010).

130. *Id.* at 1260–62.

131. *Id.* at 1263.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Nosal*, 642 F.3d 781, 783 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011).

137. 581 F.3d 1127 (9th Cir. 2009).

138. *Id.* at 1128–29.

admissions report, which included the names of past and current [LRVC patients], to his personal email account."[139] In seeking damages under § 1030(g), LRVC argued that Brekka had accessed LRVC's computer "without authorization" when he e-mailed the report with the purpose of "further[ing] his own interests."[140] The Ninth Circuit ruled in Brekka's favor, finding that his act of emailing documents to his own personal computer did not violate either §§ 1030(a)(2) or (a)(4) because he was authorized to access LVRC's computers during his employment with LVRC.[141]

LVRC argued only that Brekka acted without authorization, not that he had exceeded his authorized access.[142] Nevertheless, the panel offered an interpretation of the meaning of exceeds authorized access: "[a] person who 'exceeds authorized access' has permission to access the computer, but accesses information on the computer that the person is not entitled to access."[143] A person would not be entitled to access the information if that access "violate[s] employer-placed limits."[144] What might "employer-placed limits" look like? The panel in *Brekka* did not say, but the panel in *Nosal* offered an answer.

The *Nosal* majority distinguished *Brekka* on the basis that Brekka had "unfettered access" to his employer's computer, whereas the Korn/Ferry employees were "subject to a computer use policy that placed clear and conspicuous restrictions on the employees' access both to the system in general and to the Searcher database in particular."[145] Brekka, the *Nosal* majority reasoned, did not exceed his authorized access because his employer did not have a policy that prohibited its employees from e-mailing company documents to personal computers; the Korn/Ferry employees, on the other hand, did exceed authorized access because Korn/Ferry had a policy that limited the use of its database to legitimate Korn/Ferry business.[146] If an employer has policies regulating the use of information on its computers, and if the employee has notice of the policies, then the employee "exceeds authorized access" under § 1030(a)(4) when he violates the policies knowingly and with intent to defraud.[147]

139. *Id.* at 1130.
140. *Id.* at 1132.
141. *Id.* at 1137.
142. *Id.* at 1135 n.7.
143. *Id.* at 1134.
144. *Id.* at 1135.
145. *Nosal*, 642 F.3d 781, 787 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011).
146. *Id.* at 787.
147. *Id.* at 786–88.

Recall that § 1030(a)(2), which does not limit liability to those who act "knowingly and with an intent to defraud," also contains an "exceeds authorized access" prong.[148] In response to Nosal's argument that a "misuse" interpretation would, via § 1030(a)(2), make criminals out of millions of employees who routinely violate their employers' computer use policies, the majority stressed that its interpretation applied only to § 1030(a)(4), which requires fraudulent intent and an action that furthers the intended fraud to obtain something of value.[149] The Ninth Circuit's effort to limit its interpretation to § 1030(a)(4) slightly differentiates *Nosal* from *John* and *Rodriguez*, both of which applied an employer-policy approach to § 1030(a)(2).[150] In dissent, however, Judge Campbell pointed out the "firm rule of statutory construction that 'identical words used in different parts of the same statute are generally presumed to have the same meaning.' "[151] Thus, contrary to the majority's assurances, the *Nosal* majority's reading of "exceeds authorized access" could also apply to § 1030(a)(2), which has no fraudulent intent requirement.[152]

2. Problems with the Employer-Policy Approach

The employer-policy approach is, like the agency approach, susceptible to void-for-vagueness challenges. Although the employer-policy approach claims to provide notice by tying authorization to written use policies, the vagueness and breadth of many of these policies pose constitutional problems.[153] In *Nosal*, for example, Korn/Ferry's terms of use specified that the Searcher database could be used only for "legitimate Korn/Ferry business."[154] Such a generally-worded policy provides insufficient notice of what computer use is prohibited. A Korn/Ferry employee's criminal liability under the CFAA turns on the definition of "legitimate . . . business," a vague standard that is susceptible to different interpretations. Is any personal use of Korn/Ferry's computer, for example, inconsistent with legitimate

148. 18 U.S.C. § 1030(a)(2) (2010).

149. *Nosal*, 642 F.3d at 788–89; *see also* discussion *supra* Section I.A.

150. United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 269 (5th Cir. 2010).

151. *Nosal*, 642 F.3d. at 789 (Campbell, J., dissenting) (quoting IBP, Inc. v. Alvarez, 546 U.S. 21, 34 (2005)).

152. *See* U.S.C. § 1030(a)(2).

153. *See Nosal*, 642 F.3d. at 790 n.1 (Campbell, J., dissenting) ("[T]o invoke the federal criminal law, employers merely need to include in their computer access restrictions that an employee's authorization to access a computer ends when he breaches his duty of loyalty.").

154. *Id.* at 782 (majority opinion).

Korn/Ferry business and thus a crime?[155] Given the number of employees who routinely use an employer's computer in violation of a computer use policy, the CFAA could "lend itself to arbitrary enforcement, rendering it unconstitutionally vague."[156]

Even if the government elects not to prosecute employees for routine violations of an employer's computer use policy, the employers can still bring civil suits against employees for minor violations.[157] In *Wendi J. Lee v. PMSI, Inc.*, for example, an employer sued an employee, under the CFAA, for accessing "facebook pages" on company time.[158] The employer's theory was that the employee exceeded authorized access on her employer's computers because the employer had a policy that prohibited employees from accessing Facebook while at work.[159]

The court dismissed the employer's CFAA claim, rejecting the employer's argument that the employee was liable under *United States v. Rodriguez*.[160] The court strained to distinguish *Rodriguez*: whereas Rodriguez accessed information on his employer's (the Social Security Administration's) computers, the court noted, the employee in this case accessed information on Facebook's computers.[161] Although the court dismissed the employer's CFAA claim here, it is not difficult to imagine a less sympathetic judge finding an employee liable under the "employer-policy approach" for violating an employer's routine use restrictions.

D. THE *NOSAL* DISTRICT COURT'S APPROACH TO READING "EXCEEDS AUTHORIZED ACCESS"

As discussed above, there are serious problems—possibly even constitutional problems—with reading the phrase "exceeds authorized access" to cover acts of information misuse. One possible alternative is to limit the phrase's application to acts of access and not acts of use. The

155. *See* Kerr, *Vagueness Challenges*, *supra* note 13, at 1586 ("Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line?").

156. *Nosal*, 642 F.3d. at 790 (Campbell, J., dissenting).

157. *See* 18 U.S.C. § 1030(g).

158. Wendi J. Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1–2 (M.D. Fla. May 6, 2011).

159. *Id.* at *2.

160. *Id.* at *3.

161. *Id.* at *2. The court appeared to either misunderstand or misread the employer's theory of liability. The employer claimed that the employee's use of Facebook resulted in her exceeding authorized access on her employer's computer, not on Facebook's computers. *Id.*

district court in *Nosal II*, which the Ninth Circuit reversed, attempted to describe such an alternative.[162]

The district court, applying the Ninth Circuit's recent decision in *Brekka*,[163] concluded that "an individual only 'exceeds authorized access' if he has permission to access a portion of the computer system but uses that access to *'obtain* or *alter* information in the computer that [he or she] is not entitled so to obtain or alter.' "[164] The court reasoned that the "exceeds authorized access" prong of § 1030(a)(4) applies to exceeding employer-imposed limits on *access* to information, not to exceeding employer-imposed limits on the *use* of information. To illustrate the sort of conduct that would exceed authorized access, the court offered the following example:

> [I]f a person is authorized to access the "F" drive on a computer or network but is not authorized to access the "G" drive of that same computer or network, the individual would "exceed authorized access" if he obtained or altered anything on the "G" drive.[165]

This example leaves out some important information. First, assume the example occurs in a workplace. Is the "G" drive protected by a code barrier that restricts access? That is, does access to the drive require authentication credentials (e.g., a password) that the person in the example does not possess? Or is the "G" drive technically accessible to all employees but, as a matter of policy or protocol, certain employees are not supposed to access the information on it?[166]

It is important to clarify these ambiguities. If access to the "G" drive is protected by an authentication scheme that the employee circumvents (either by using another employee's credentials or by hacking into the drive), then the court is endorsing a code-based approach to defining "exceeds authorized access."[167] If, on the other hand, access to the "G" drive is regulated by a use policy that the employee violates, then the court is proposing a variant of the employer-policy approach to exceeding authorized

---

162. *Nosal II*, No. C 08-0237, 2010 WL 934257, at *1, *6 (N.D. Cal. Jan. 6. 2010), *rev'd*, 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011).

163. *See* discussion *supra* Section II.C.1.

164. *Nosal II*, 2010 WL 934257, at *7 (citing 18 U.S.C. § 1030(e)(6) (2010)) (emphasis in original).

165. *Id.* at *6.

166. Nosal's brief in the Ninth Circuit offered a similarly sparse hypothetical: "An employer may say to an employee: 'You have permission to access the Cronos database but not the Poseidon database, because the Poseidon database is highly confidential.' Under *Brekka*, if an employee violates those limitations, he has committed a crime under the CFAA." Appellee's Brief at 10, *Nosal*, 642 F.3d 781 (9th Cir. 2011) (No. 10–10038).

167. *See* discussion *supra* Section II.A.1.

access.[168] This variant would be different from the approaches in *John*, *Rodriguez,* and *Nosal* in that it would not cover the misuse or misappropriation of information that employees have authority to access.[169] The variant would be similar, however, in that it would allow the employer to set the scope of authorized access via use policies instead of only through code-based restrictions.[170]

It is unclear if the *Nosal II* district court's example represents a code-based approach or an employer-policy approach to defining "exceeds authorized access." In the context of the district court's example, either approach is problematic. Under the code-based scenario, where code completely blocks the employee from accessing the "G" drive, the access is arguably "without authorization" at all. To classify hacking into the "G" drive as "exceeding authorized access," the court needs to explain how authorized access enabled the person to hack the drive.[171]

Under the employee-policy scenario, where the employer's policy forbids the employee from accessing content on the "G" drive, there are similar void-for-vagueness risks that plague the approaches of *John*, *Rodriguez,* and *Nosal*.[172] Admittedly, the risks are lessened because the approach would not cover acts of misuse or misappropriation, but the approach still allows employers to dictate, perhaps through vague policies, what constitutes criminal conduct under the CFAA.[173]

III. A CODE-BASED APPROACH TO "EXCEEDS AUTHORIZED ACCESS" IN THE CFAA

Although the district court in *Nosal II* attempted to confine the scope of "exceeds authorized access" by limiting its application to violations of access restrictions,[174] its approach was ultimately unpersuasive because it failed to describe how an employer could impose limits on access and how an employee could exceed such limits.[175] This Part proposes a reading of "exceeds authorized access" that fills in the gaps in the district court's approach. The proposed approach takes elements of the code-based

168. *See* discussion *supra* Section II.C.1.

169. *See id.*

170. *See id.*

171. *See* 18 U.S.C. § 1030(e)(6) (2010).

172. *See* discussion *supra* Section II.C.2.

173. *See id.*

174. *Nosal II*, No. C 08-0237, 2010 WL 934257, at *1, *6 (N.D. Cal. Jan. 6. 2010), *rev'd*, 642 F.3d 781 (9th Cir.), *reh'g granted en banc*, 661 F.3d 1180 (9th Cir. 2011).

175. *See* discussion *supra* Section II.D.

approach and applies them to the term "exceeds authorized access," tying employee liability to breaches of an employer's technical restrictions on access. The approach is based on the following principles:

- Avoid the void-for-vagueness problems posed by the agency and employer-policy approaches.[176]
- Preserve the textual distinction between "without authorization" and "exceeds authorized access."[177]
- Respect the apparent Congressional understanding that "exceeds authorized access" applies to "insiders."[178]
- Comport with the general statutory purpose of regulating computer misuse, as opposed to any misconduct—even criminal misconduct—that happens to be effectuated through the use of a computer.[179]

A. DESCRIPTION OF A CODE-BASED APPROACH TO EXCEEDING AUTHORIZATION

Under the proposed code-based approach, an employee exceeds authorized access when she (1) encounters a code-based barrier on her employer's computer and then (2) proceeds to use her authorized access to obtain or alter information that exists behind the barrier. The second step—using authorized access to obtain or alter information—occurs when the employee uses a program (to which she has access) for a function for which the program was not intended.

The first element of the approach avoids the potential void-for-vagueness problems of the employer-policy approach.[180] If a user attempts to obtain or alter information, and if a code-based barrier blocks the attempt, the user has clear notice that the attempted action is prohibited. Much like an employee who encounters a locked file cabinet at work, the employee who encounters a code-based barrier on a work computer has notice that they are not authorized to enter the electronic resource unless they have a key (or a password).

The requirement that an employee uses a program in a manner unrelated to its intended function ensures that the approach covers actual computer

176. *See* discussion *supra* Sections II.B.2, II.C.2.
177. *See supra* text accompanying notes 58–60.
178. *See supra* Section I.B.
179. *See Nosal*, 642 F.3d 781, 793 (9th Cir. 2011) (Campbell, J. dissenting).
180. *See supra* Section II.C.2.

misuse.[181] Although the approach borrows language from *United States v. Morris*, the "intended function" test here is subtly but significantly different than the Second Circuit's test in that case.[182] Recall that Morris exploited vulnerabilities in the "finger" and "sendmail" programs that "permitted him a special and unauthorized access route into *other* computers."[183] By using programs in a manner unrelated to their intended function, Morris obtained privileges on computers that he was not authorized to access at all.[184] The proposed approach, by contrast, covers instances where an employee uses her access to exploit a vulnerability to obtain information on a computer to which she has at least some authorized access. Unlike Morris, whose exploit was "without authorization,"[185] the employee's exploit under the proposed approach "exceeds authorized access."

B. HYPOTHETICAL EXAMPLE

Using a hypothetical fact pattern, this Section demonstrates how the proposed approach would distinguish between computer use in excess of authorization, use without authorization, and use with authorization under the CFAA.

Aaron works in the financial aid office of a large public university. Aaron has access to a student information system that contains academic and financial records for all of the university's students. The student information system includes different tools that allow employees to access a central database. Aaron, like his fellow employees, does most of his work using a web browser through which he signs on to a web application that gives him access to student information in the database. Although the web interface is the primary way that employees interact with the system, there are other tools—including a report writer—that employees use to access the data in the information system.

The student information system, like most modern applications, allows the system owner to configure which users get to access which features, pages, and records. The university configured the web application so that the employees in the financial aid office can access the pages that display a student's financial information. The financial aid employees cannot, however,

181. Before the recent explosion of civil and criminal litigation that relied on the agency and employer-policy theories, most CFAA prosecutions targeted instances of computer misuse. *See* cases cited *supra* note 12.

182. *See* United States v. Morris, 928 F. 2d 504, 509 (2d Cir. 1991); *see also* discussion *supra* Section II.A.1.

183. *Morris*, 928 F. 2d at 510 (emphasis added).

184. *Id.*

185. *Id.*

access any of the pages that display a student's courses and grades. Those pages are accessible to employees in the registrar's office, but not to employees in the financial aid office.

One summer evening, Aaron is taking out the garbage when he runs into Bob, his neighbor. Aaron dislikes Bob, whose son Ryan attends the university. Bob constantly brags about how well Ryan is doing in life, and this evening is no exception. Ryan, Bob says, just got his spring semester grades: straight A's.

1. Possible Violation #1

Aaron is skeptical about Bob's boast. The next day at work, Aaron thinks about how he can view Ryan's grades. Aaron opens up his web browser and logs on to the student information system's web application. He navigates around for a while, but finds that the web application is locked down: he can only access pages that display a student's financial aid information. Aaron cannot access any of the pages that would allow him to view a student's grades.

Next, Aaron opens up the report writer client. The report writer connects to the same database as the web application, but it has a different purpose: whereas the purpose of the web application is to permit employees to view and update individual student records, the purpose of the report writer is to query large volumes of data and then to assemble that data into charts and reports. Aaron is thrilled to find that the report writer, in contrast to the web application, does not limit him to financial aid data. The report writer allows him to view all kinds of data, including the grades of students. Aaron uses his access to write a "report" that returns the grade records for a single student: Ryan. Aaron is disappointed to see that Ryan did, in fact, get all A's last semester.

Under the proposed code-based reading of "exceeds authorized access," Aaron has exceeded his authorized access to the student information system database. In the web application that Aaron routinely used to access the database, code-based barriers prevented him from viewing a student's grades. He subverted this barrier by using another tool, the report writer, for a function for which it was not intended. The report writer's intended function is to allow for the querying and aggregating of large volumes of data; it is not intended for the purpose of querying individual records. Aaron thus used his authorized access to view information that he was not permitted to obtain.

It is worth emphasizing that Aaron did not exceed his authorized access merely because he used a program for a purpose that is inconsistent with the program's intended function. Had there been no code-based barrier in place in the web application (i.e., if Aaron could view the "student grades" pages in

the web application), Aaron would not have exceeded authorized access by using the report writer to view Ryan's grades. For an employee to exceed authorized access, he must be trying to find a way around a code-based barrier that prevents access.

Aaron could also have liability under the agency and employer-policy approaches. Under the agency approach, Aaron's access would be "without authorization" if he used the information system in a manner that was contrary to his employer's (the university's) interests.[186] Under the employer-policy approach, Aaron would have exceeded his authorized access if the university had a written policy that prohibited Aaron's purpose or intent in looking up the information. If, for example, the university had a policy that prohibited employees from accessing academic records for non-business reasons, Aaron would have exceeded authorized access.[187]

2. Possible Violation #2

While Aaron viewed Ryan's grades, he noticed that one grade from the spring semester was not yet posted. Aaron thought it would be funny to give Ryan a "D" in the class. Aaron could not insert or change a grade with the report writer tool. The report writer allows for the viewing, but not the updating, of data.

Aaron knew that the student information system was a commercial product that the university had purchased and then configured. He did an online search of the name of the product along with the words "hack" and "exploit," finding instructions for how to launch a cross-site scripting attack that would allow the attacker to hijack another user's web session.[188] There was, Aaron read, a patch available for the vulnerability, but he figured there was a decent chance that the university's IT group had not yet patched the system.

Aaron launched the cross-site scripting attack. It turned out that the system had not been patched, and Aaron was able to hijack the web session of an employee at the registrar's office. Unlike the financial aid office's employees, the registrar office's employees had access to pages that allowed for the updating of student grades. Aaron used this access to assign Ryan a "D" in his final spring semester class.

186. *See supra* Section II.B.1.

187. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1260–62 (11th Cir. 2010).

188. *See* Robert Auger, *Cross Site Scripting*, THE WEB APPLICATION CONSORTIUM, http://projects.webappsec.org/w/page/13246920/Cross Site Scripting (last modified Feb. 1, 2011).

Aaron's access to the system was "without authorization" under the proposed code-based approach. Aaron did not exceed authorized access because he did not use his existing access to obtain or alter information in the system;[189] instead, he directly breached a code barrier in the same way that an outsider would have. The fact that Aaron had some access to the system is not relevant to the analysis. For Aaron to act in excess of authorization (as opposed to without authorization), he must *use his authorized access* to help bypass a code-based barrier. He did not do so here.[190]

3. Possible Violation #3

Aaron is pleased that Bob will soon learn that his son got a "D." But it is not enough for Aaron, who really wants Bob to suffer. Aaron logs on to the student information system and navigates to a financial page that allows him to view Ryan's financial aid records. Ryan has a grant of $7,000 scheduled for distribution at the beginning of fall semester. Purely out of spite, Aaron reduces the award to $1,000. The award reduction violates the financial aid office's policies, which permit award reductions only for certain reasons. Spite is not one of them.

Aaron is not guilty of a crime under the proposed code-based approach to "exceeds authorized access." Aaron's access to the student information system was authorized; he was permitted to view and update a student's financial aid data using the information system. There was no code barrier in place that prevented Aaron from accessing or updating the information. Although Aaron is guilty of violating his employer's policies, and although Aaron may have committed other state and federal crimes, he did not commit a computer misuse crime and did not violate a provision of the CFAA.

By contrast, Aaron would likely have CFAA liability under both the agency and employer-policy approaches. Under the agency approach, Aaron's act of reducing the award amount was probably contrary to his employer's interests and thus without authorization.[191] Under the employer-policy approach, Aaron exceeded his authorized access to the system when

189. *See* 18 U.S.C. § 1030(e)(6) (2010).

190. Neither the agency approach nor the employer-policy approach have much to say about external breaches of technical barriers. Advocates of both approaches would, presumably, agree that the CFAA prohibits code-based breaches of computers. The agency and employer-policy approaches effectively add a layer of prohibited behavior beyond the basic code-based approach. *See* discussion *supra* Part II.

191. *See supra* Section II.B.1.

he violated his office's policies regarding the reasons for reducing a student's award amount.[192]

C. LIMITATIONS OF A CODE-BASED APPROACH TO EXCEEDING AUTHORIZED ACCESS

The proposed code-based approach to "exceeds authorized access" covers a much narrower range of conduct than does the employer-policy approach. As the hypothetical discussed above demonstrates, the code-based approach will often fail to prohibit reprehensible conduct. Indeed, none of the defendants in *John*, *Rodriguez*, and *Nosal* bypassed any code-based barriers, and thus none would have CFAA liability for their misconduct under the proposed code-based approach.[193] It should be noted, however, that John and Nosal are liable for other crimes. John was also charged with committing various federal fraud crimes.[194] And Nosal faces civil and criminal litigation for his alleged theft of his former employer's intellectual property.[195]

The defendant's conduct in *Rodriguez* presents a more difficult case. There, a government employee used his access to Social Security Administration computers to browse the records of women he knew.[196] Although this conduct violated the administration's policies, it was apparently not criminal.[197] If Rodriguez is not liable under the CFAA for exceeding authorized access on his employer's computer, then he may have no criminal liability at all for browsing the women's records.[198]

---

192. *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

193. *See* discussion *supra* Section II.C.1.

194. *John*, 597 F.3d at 269.

195. *See supra* text and accompanying notes 1–7.

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

197. *Id.*

198. James A. Baker, testifying before the Senate Judiciary Committee on behalf of the Department of Justice, argued that a narrow reading of "exceeds authorized access" would rob the Department of a useful tool with which to prosecute and deter "insider threats." Baker stated:

> Employers should be able to set and communicate access restrictions to employees and contractors with the confidence that the law will protect them when their employees or contractors exceed these restrictions to access data for a wrongful purpose. Limiting the use of such terms to define the scope of authorization would, in some instances, prevent prosecution of exactly the kind of serious insider cases the Department handles on a regular basis: situations where a government employee is given access to sensitive information stored by the State Department, Internal Revenue Service, or crime database systems subject to express access restrictions, and then violates those access restrictions to access the database for a prohibited purpose.

There are at least two responses to the issues raised by Rodriguez's lack of criminal liability under the code-based approach to exceeding authorized access. First, not every instance of employee misconduct requires a legal remedy. Employers can address most employee misconduct by disciplining and, if necessary, firing the employee. Second, legislatures can pass laws that protect the privacy of confidential information. If Congress, for example, wishes to prohibit government employees from accessing confidential information for non-business reasons, it may pass a law to address this specific problem. Congress could specify the types of confidential information (e.g., personal medical records) that it wants to protect. A specific law would be more fair, and more effective, than relying on a combination of a broad reading of a computer misuse statute and the content of various agency use policies.

IV. CONCLUSION

Congress passed the CFAA to address the problem of hacking and other forms of computer misuse. Over time, courts developed interpretations of the CFAA that transformed the statute into a broader law that prohibits various forms of information misuse and misappropriation. Most recently, three circuit courts endorsed an employer-policy theory of liability, which holds that employees are liable for "exceed[ing] authorized access" under the CFAA when they violate their employers' computer use restrictions. The employer-policy approach, which risks rendering certain provisions of the CFAA unconstitutional, should be abandoned. Instead, courts should adopt the proposed code-based approach to reading the phrase "exceeds authorized access" in the CFAA. The code-based approach respects the text of the statute, avoids constitutional void-for-vagueness issues, and comports with the CFAA's general purpose of regulating computer misuse crimes.

Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats: Hearing Before the Committee on the Judiciary, 112th Cong. 35–36 (2011) (statement of James A. Baker, Associate Deputy Attorney General).