A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act

*Patricia L. Bellia**

Abstract

Thirty years ago, Congress passed the Computer Fraud and Abuse Act ("CFAA") to combat the emerging problem of computer crime. The statute's core prohibitions targeted one who "accesses" a computer "without authorization" or who "exceeds authorized access." Over time, the incremental statutory changes and large-scale technological changes have dramatically expanded the potential scope of the CFAA. The question of what constitutes unauthorized access has taken on far greater significance than it had thirty years ago, and courts remain deeply divided on this question. This Article explores the text, purpose, and history of the CFAA, as well as a range of normative considerations that should guide interpretation of the statute. This Article concludes that courts should pursue a narrow and "code-based" understanding of unauthorized access under the CFAA—both in terms of what it means to access a computer without authorization and in terms of what it means to exceed authorized access. The CFAA has strayed far from its original purpose: Congress failed to define key terms in the CFAA, and courts have overlooked limiting principles within the statute. From a normative perspective, even if it is desirable to provide owners of networked computer systems with stronger legal protection for their systems, the CFAA's unauthorized access provisions are not the proper vehicle for doing so.

Table of Contents

---

* William J. and Dorothy K. O'Neill Professor of Law, Notre Dame Law School. The Author thanks her fellow participants in *The George Washington Law Review*'s Symposium "Hacking into the Computer Fraud and Abuse Act: The CFAA at 30" for their helpful discussion and comments.

INTRODUCTION

More than thirty years ago, to "stem the tide of criminal behavior" involving the abuse of computer technology,[1] Congress adopted the first federal statute specifically addressing computer crime. The statute, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[2] was quite narrow: it protected national security information, information in financial records, and computers used by or on behalf of the U.S. government.[3] Within that narrow sphere, the statute introduced a core concept of unauthorized access, encompassing "access[ing] a computer without authorization" or using authorized access for purposes to which it does not extend.[4] Beginning with the Computer Fraud and Abuse Act of 1986 ("CFAA"),[5] Congress amended the statute on several occasions, to reach a greater number of computers and to add civil liability. With each amendment, however, the concept of unauthorized access—"access[ing]" a computer "without authorization" or, in some contexts, "exceed[ing] authorized access"—remained the trigger for nearly all of the statute's substantive provisions.[6]

Despite the fact that what is now known as the CFAA has always encompassed unauthorized access offenses, courts remain deeply divided on what it means to access a computer without authorization or to exceed authorized access. The ubiquity of computer technology, coupled with the fact that the CFAA now reaches virtually any internet-connected computer, makes the CFAA an increasingly attractive tool for combating a range of inappropriate behavior. The

1 H.R. REP. NO. 98-894, at 4 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3690.

2 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 1873, 2190–91.

3 *Id.*

4 *Id.* (codified at 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985)).

5 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213–16 (codified as amended at 18 U.S.C. § 1030 (2012)).

6 *Id.*

government and civil litigants alike have invoked the CFAA to target employee disloyalty, unfair competition, the use of confidential information for personal purposes, and even online bullying.

These far-ranging applications of the CFAA raise difficult doctrinal and normative questions. This Article explores the text, purpose, and history of the CFAA, as well as a range of normative considerations that should guide interpretation of the statute, and concludes that courts should pursue a narrow and "code-based" understanding of unauthorized access under the CFAA—both in terms of what it means to access a computer without authorization and in terms of what it means to exceed authorized access. Congress failed to define key terms in the CFAA. The combination of incremental statutory changes and dramatic technological changes creates the potential for the CFAA to reach far beyond its original purpose. Courts have overlooked limiting principles within the statute itself. From a normative perspective, moreover, even if it is desirable to provide owners of networked computer systems with stronger legal protection for their systems, the CFAA's unauthorized access provisions are not the right vehicle for doing so.

This Article proceeds as follows. Part I begins by describing five paradigms of unauthorized access that existing cases reflect. Part II explores the text, purpose, and history of the CFAA for clues about how to interpret the statute. The discussion demonstrates how the CFAA has strayed far from its original purpose, as the interplay of incremental statutory modifications and dramatic changes in technology has swept virtually all internet-connected devices within the statute's reach. The question of what it means to access a computer without authorization or to exceed authorized access has far greater significance than it did thirty years ago. Part III examines the relevant normative considerations, both as they bear upon the question of statutory interpretation and as they bear upon how Congress might reshape the CFAA.

I. Paradigms of Unauthorized Access

As noted above, the CFAA currently encompasses two forms of unauthorized access to a computer: "access[ing]" a computer "without authorization" and "exceed[ing] authorized access."[7] The statute does

[7] 18 U.S.C. § 1030(a)(1) (2012) ("having knowingly accessed a computer without authorization or exceeding authorized access"); *id.* § 1030(a)(2) ("intentionally accesses a computer without authorization or exceeds authorized access"); *id.* § 1030(a)(3) ("intentionally, without authorization to access . . . [certain computers], accesses such a computer"); *id.* § 1030(a)(4)

not define what it means to "access[]" a computer or what it means to do so "without authorization." The statute defines the phrase "exceeds authorized access"[8] as follows: "[T]o 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."[9]

Courts have long struggled to apply these concepts of accessing a computer without authorization and exceeding authorized access. Indeed, the caselaw reflects at least five different interpretive paradigms.[10] This Part explores those five paradigms, with a few important caveats. First, the goal of this analysis is purely descriptive; it seeks to call attention to courts' varied approaches without (yet) passing on which fits best with the statute. Second, the descriptive labels below do not necessarily align with those that courts attach. Many courts summarizing the caselaw refer only to two different approaches—"broad" and "narrow."[11] As will become clear, the matter is far more

("knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access"); *id.* § 1030(a)(5)(B) ("intentionally accesses a protected computer without authorization"); *id.* § 1030(a)(5)(C) ("intentionally accesses a protected computer without authorization").

8 Congress first adopted the phrase "exceeds authorized access" in 1986, replacing the more cumbersome original language covering one who "uses the opportunity such access [with authorization] provides for purposes to which such authorization does not extend." *Compare* 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985), *with* 18 U.S.C. § 1030 (a)(1)–(2), (4) (Supp. IV 1987) (codifying the Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213–16).

9 18 U.S.C. § 1030(e)(6).

10 For other efforts to synthesize the unauthorized access caselaw, see, e.g., Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1624–40 (2003); Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 Hamline L. Rev. 81, 102–14 (2013); Katherine Mesenbring Field, Note, *Agency, Code or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819, 822–29 (2009); Kelsey T. Patterson, Note, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 Charleston L. Rev. 489, 497–513 (2013); David J. Rosen, Note, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"*, 27 Berkeley Tech. L.J. 737, 746–59 (2012).

11 *See, e.g.*, United States v. Steele, 595 F. App'x 208, 211 (4th Cir. 2014) (describing "broad view" and "narrower construction"); LivePerson, Inc. v. 24/7 Customer, Inc., 83 F. Supp. 3d 501, 512–13 (S.D.N.Y. 2015) (characterizing cases as narrow or broad); Aquent LLC v. Stapleton, 65 F. Supp. 3d 1339, 1346 (M.D. Fla. 2014) (describing narrow and broad interpretations); Amphenol Corp. v. Paul, 993 F. Supp. 2d 100, 110 (D. Conn. 2014) (discussing trend toward narrow approach); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615 (E.D. Pa. 2013) (describing "split between what is cast as a broad versus a narrow interpretation"); Advanced Micro Devices, Inc. v. Feldstein, 951 F. Supp. 2d 212, 217 (D. Mass. 2013) (describing broader and narrower interpretations); JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 521–22 (S.D.N.Y. 2013) (describing "broad construction" and "narrow approach"); Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 686 (E.D. Mich. 2012) (describing narrow and broad construc-

complicated. Third, the differences between some of the paradigms are subtle, and classifying a decision in one way or another may depend on one critical fact that a court relied on or ignored. Even if courts or commentators would disagree with how the analysis below classifies individual decisions, however, the goal is to offer a taxonomy that will press courts and commentators to think more carefully about what constitutes unauthorized access.

A. Agency Paradigm

Under the *agency paradigm*, the boundaries of permissible access to a computer covered by the CFAA depend upon principles of agency law. This approach typically arises in cases involving disputes between an employer and a disloyal (former) employee who uses information from the employer's computer system to compete with the employer. In the influential decision of *International Airport Centers, LLC v. Citrin*,[12] for example, the U.S. Court of Appeals for the Seventh Circuit adopted an agency approach to reverse the dismissal of a claim that a former employee acted without authorization when he deleted files from his company-owned laptop.[13]

In *Citrin*, a group of real estate companies had hired the defendant to identify properties to purchase and had provided the defendant with a company-owned laptop for that purpose.[14] After the defendant decided to start a competing business, he allegedly used a secure-erasure program to delete from the laptop both company data and information that could have revealed that he violated his employment contract.[15] The employer claimed, among other things, that the defendant violated what is now § 1030(a)(5)(B) of the CFAA, which reaches one who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes dam-

---

tions of the CFAA); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (adopting "narrow" reading of the CFAA); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 46 (D. Mass. 2009) (describing parties as urging broad and narrow interpretations); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) (describing and adopting "broad" view of statutory language and legislative history); State Analysis, Inc. v. Am. Fin. Servs. Assoc., 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (noting that courts have differed "as to how broadly or narrowly" to construe the statute).

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

13 *Id.* at 420–21. The Seventh Circuit relied heavily on the district court decision in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

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

15 *Id.* at 419–21.

age."[16] The defendant's use of the secure-erasure program was "without authorization," the court reasoned, because the defendant's "breach of his duty of loyalty terminated his agency relationship" with his employer and the agency relationship was "the only basis of his authority" to access the laptop.[17] In other words, when the defendant engaged in disloyal conduct, he lost any authority to access the laptop, making any further access (in this case, to erase the laptop's contents) "without authorization" for purposes of the CFAA.[18]

In siding with the employer and concluding that the defendant accessed the laptop without authorization, the Seventh Circuit did not base its conclusion that the defendant lacked authorization on the violation of any term of the defendant's employment contract or of a company policy constraining the defendant's access to the laptop or his authority to delete files from it.[19] The court stated only that the defendant breached his duty of loyalty and his employment contract by going into competition with his employer.[20] The case thus suggests that even in the absence of specific contractual restrictions on access to a protected computer, a court can import freestanding agency principles to set the boundaries of permissible access under the CFAA. Several district courts have followed the *Citrin* court's approach.[21]

B. Norms-of-Access Paradigm

Under the *norms-of-access paradigm*, the limits of permissible access under the CFAA turn on certain shared understandings of or reasonable expectations about how far access to a covered computer should extend. Although it is possible to interpret certain employee loyalty cases as applying a norms-of-access paradigm, the paradigm is

---

16 18 U.S.C. § 1030(a)(5)(B) (2012). Between 2001 and 2008, the quoted language appeared at § 1030(a)(5)(A)(i). *See* Pub. L. No. 107-56, § 814(a)(1)–(3), 115 Stat. 272, 382–83 (2001) (codified at 18 U.S.C. § 1030 (2006)); Pub. L. No. 110-326, § 204(a)(1), 122 Stat. 3650, 3561–63 (2008) (codified at 18 U.S.C. § 1030 (2012)). To avoid confusion and facilitate comparison of similar cases, this Article uses the current section numbers.

17 *Citrin*, 440 F.3d at 419–21.

18 *Id.*

19 In fact, the employment contract permitted Citrin to "return or destroy" data in the laptop. *Id.* at 421.

20 *Id.* at 420.

21 *See, e.g.*, Ryan, LLC v. Evans, No. 8:12–CV–289–T–30TBM, 2012 WL 1551285 (M.D. Fla. Apr. 30, 2012); Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc., 793 F. Supp. 2d 1302, 1315 (N.D. Ga. 2011); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1061 (S.D. Iowa 2009); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006).

perhaps best understood through the lens of an early case involving a criminal prosecution, *United States v. Morris*.[22]

Morris, a graduate student in computer science at Cornell University, created a "worm" that exploited security flaws in certain programs that allowed users to transmit or retrieve information from internet-connected computers.[23] Morris claimed that he developed the worm to expose internet security weaknesses.[24] He launched the worm from a computer at MIT and it replicated more quickly than anticipated, thereby slowing or damaging a number of computers.[25] The version of the CFAA in effect in 1988, when Morris's conduct occurred, did not contain what is now § 1030(a)(5)(A), which prohibits intentionally causing "damage without authorization" through "the knowing transmission of a program, information, code, or command."[26] Because the CFAA lacked a provision specifically covering the transmission of potentially harmful code, Morris's conduct could violate the CFAA only if it fit within a provision covering one who "intentionally accesses" a covered computer "without authorization" and thereby "alters, damages, or destroys information" or "prevents authorized use of any such computer or information."[27]

Morris appealed his jury conviction, and the U.S. Court of Appeals for the Second Circuit had to confront whether Morris's transmission of the worm constituted "intentionally access[ing]" a computer "without authorization."[28] Morris claimed that the programs the worm exploited—"sendmail" and "finger demon" programs—were programs that he had authorization to access at the various institutions affected.[29] At most, he argued, his conduct could constitute exceeding authorized access, which the provision in question did not cover.[30] The court rejected this argument on the ground that Morris did not use the sendmail and finger demon functions "in any way related to their *intended function* . . . . He did not send or read mail nor discover information about other users; instead he

22 United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991).

23 *Id.* at 505.

24 *Id.*

25 *Id.* at 506.

26 18 U.S.C. § 1030(a)(5)(A) (2012).

27 *See* 18 U.S.C. § 1030(a)(5) (Supp. V 1988).

28 *Morris*, 928 F.2d at 505.

29 *Id.* at 506.

30 *Id.* at 509–10; *see* 18 U.S.C. § 1030(a)(5) (Supp. V 1988).

found holes in both programs that permitted him a special and unauthorized access route into other computers."[31]

In focusing on the programs' "intended function," the court sought to arrive at some understanding of what would constitute appropriate use of the technology in question.[32] The court did not examine Morris's conduct through the lens of any agency relationship created by Morris's status as a computer science graduate student.[33] Nor did the court rely on specific policies or contractual terms that constrained Morris's access to the affected computers or the technology Morris exploited.[34] Rather, the court developed a concept of authorized access based on its understanding of how one *ought* to use the technology in question.

In employee loyalty cases, courts have likewise focused on how a particular computer system ought to be used. An early federal district court case involving a former employee's alleged misappropriation of confidential information is illustrative of a norm-based approach, although one that the court of appeals ultimately rejected.[35] Former employees of EF Cultural Travel, a company that designed and marketed student tours, formed a competing tour company called Explorica.[36] Explorica hired a technology consultant to design a program to "scrape" pricing information from EF's website, so that Explorica could attempt to undercut EF's prices.[37] The scraper relied on certain proprietary tour codes that were publicly available on EF's website, but that were not readily understandable to the general public.[38]

The district court held that Explorica violated § 1030(a)(4) of the CFAA, which prohibits one from "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."[39] The district court held that the scope of Explorica's authorization to use EF's website should depend on whether the conduct was "'in line

---

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

32 *See id.* at 509–10.

33 *See id.*

34 *See id.* at 510.

35 The district court opinion is unpublished, but is described in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) and *EF Cultural Travel BV v. Zefer Corporation*, 318 F.3d 58, 62–63 (1st Cir. 2003).

36 *Zefer*, 318 F.3d at 60.

37 *Id.*

38 *Id.*

39 18 U.S.C. § 1030(a)(4) (2012).

with the 'reasonable expectations' of the website owner and its ordinary users."[40] Although EF's website did not specifically address the use of scrapers, the district court concluded that Explorica's use of the scraper was inconsistent with reasonable expectations for use of its site.[41]

Like the *Morris* court, the *Explorica* district court thus attempted to arrive at an understanding of how the computer in question—in this case, a publicly available web server—ought to be used. The potential breadth of the district court's approach was not lost on the U.S. Court of Appeals for the First Circuit, which first cast doubt on the "reasonable expectations" test[42] and then rejected it.[43] In an appeal involving Explorica and its founders, the court found it unnecessary to rule on the district court's "reasonable expectations" test, because it identified an alternative basis for concluding that Explorica's scraper exceeded authorized access under the CFAA: the former employee was subject to a confidentiality agreement that restricted use of proprietary information "which might reasonably be construed to be contrary to the interests of EF."[44] Although the confidentiality agreement in no way addressed the terms of permissible access to EF's website, the court implied that, by virtue of the agreement, the former employee ought to have known that the manner in which he accessed the website was improper.[45] In a subsequent case involving the developer of the scraper—who was not subject to the confidentiality agreement and whose authority to access the website therefore could not turn on that agreement—the court of appeals rejected the "reasonable expectations" test, suggesting that the lack of common understanding underpinning the notion of reasonable expectations in this context would place users "at the mercy of a highly imprecise, litigation-spawning standard."[46] Despite the First Circuit's rejection of the district court's approach, other courts have invoked similar con-

---

40 *Explorica*, 274 F.3d at 582 n.10 (quoting district court opinion); *see also id.* at 580 (describing district court as holding that EF would likely prove that Explorica used its website "in a manner outside the 'reasonable expectations' of both EF and its ordinary users") (quoting district court opinion).

41 *See Zefer*, 318 F.3d at 62.

42 *Explorica*, 274 F.3d at 582 n.10.

43 *Zefer*, 318 F.3d at 63.

44 *Explorica*, 274 F.3d at 583.

45 *See infra* Section I.C.

46 *Zefer*, 318 F.3d at 61, 63. The court nevertheless sustained the injunction against the developer of the scraper, on the ground that any use of the scraper would assist Explorica in violating the injunction to which it was subject. *Id.*

cepts of intended use or reasonable expectations in interpreting the CFAA.[47]

C. Policy Paradigm

Under the *policy paradigm*, whether access to a computer is unauthorized for purposes of the CFAA turns on whether the owner of a computer system has a policy designed to notify users of the boundaries of permitted access.[48] Under the policy approach, one who violates the stated limitations on access is acting without or in excess of authorization. The breadth of the CFAA under this approach depends on (1) how the system owner notifies users of its policy, and (2) what sort of limitations qualify as limitations on *access*.

To bring these two issues into focus, consider two quite different categories of cases in which CFAA claims arise. The first category involves a company that provides others with the opportunity to use its computer system but that attempts to limit such access through an acceptable use policy, terms of service, or similar mechanisms. The provider's policy may preclude access to the system for certain purposes, or it may preclude particular uses of the information the system contains. Early CFAA cases in this category typically involve defendants harvesting email addresses for the purpose of sending unsolicited email[49] or defendants using automated queries to extract information from a rival website.[50] The second category of cases involves situations in which an employer has a policy that restricts access to its com-

---

47 *See, e.g.*, United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (applying "intended use" analysis); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (adopting "expected norms of intended use" analysis); Merritt Hawkins & Assocs., LLC v. Gresham, 79 F. Supp. 3d 625, 635 (N.D. Tex. 2015) (suggesting that deletion of certain files was beyond the "intended use" of the system).

48 As will become clear, some providers seek to use such mechanisms to create a binding contract with the user. The next Section discusses a contract-based paradigm. This Section uses the label "policy" paradigm to describe situations in which a court does not consider the questions of notice and assent that would be necessary to treat the provider's terms as a binding contract and situations in which a court considering those questions would find that no contract exists.

49 *See, e.g.*, Am. Online, Inc. v. Nat'l Health Care Disc., Inc. (*Nat'l Health Care Disc. II*), 174 F. Supp. 2d 890, 892 (N.D. Iowa 2001); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 446 (E.D. Va. 1998).

50 *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–81 (1st Cir. 2001); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 241 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2nd Cir. 2004). For more recent automated query cases, see Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 930–31 (E.D. Va. 2010).

puter system and an employee (or former employee) violates those restrictions.[51]

The cases involving email harvesting provide a useful illustration of the first issue concerning the reach of the CFAA: how a provider must convey its policy before a court can determine that the policy validly sets the boundaries of authorized access. Two early email cases involve defendants who subscribed to America Online ("AOL") for the purpose of harvesting the addresses of fellow AOL subscribers.[52] AOL had a specific policy on unsolicited email as well as terms of service that prohibited the use of AOL membership to harvest email addresses.[53] Based on the unsolicited email policy and the terms of service, AOL successfully claimed that the harvesting of email addresses violated § 1030(a)(2)(C) of the CFAA, which prohibits one from accessing a protected computer without authorization and thereby obtaining information.[54] In both cases, courts gave effect to the policy on unsolicited email and the terms of service, without inquiring whether the defendants had actual or constructive knowledge of the policy or terms (or had agreed to them).[55] Because AOL sent cease-and-desist letters and ultimately sued,[56] one could argue that the defendants had actual knowledge of AOL's objection to their conduct, and the question of whether the policy statement or terms of service put the defendants on notice of the limits of authorization was therefore irrelevant. Both cases, however, also involved damages for conduct that occurred prior to AOL's sending of the cease-and-desist letters.[57] Both courts concluded that it was appropriate to award damages and therefore necessarily relied on the policy and the terms of service as the trigger for liability under the CFAA.[58] In other words, courts deemed the unsolicited email policy and terms of use sufficient to render the defendants' access unauthorized.

---

51 *See, e.g.*, *John*, 597 F.3d at 263; United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010); Aquent LLC v. Stapleton, 65 F. Supp. 3d 1339, 1342 (M.D. Fla. 2014); United States v. Valle, 301 F.R.D. 53, 111 (S.D.N.Y. 2014), *aff'd in part, rev'd in part*, 807 F.3d 508 (2nd Cir. 2015).

52 Am. Online, Inc. v. Nat'l Health Care Disc., Inc. (*Nat'l Health Care Disc. I*), 121 F. Supp. 2d 1255, 1261 (N.D. Iowa 2000); *LCGM*, 46 F. Supp. 2d at 448.

53 *Nat'l Health Care Disc. I*, 121 F. Supp. 2d at 1261; *LCGM*, 46 F. Supp. 2d at 448.

54 *Nat'l Health Care Disc. II*, 174 F. Supp. 2d at 899; *LCGM*, 46 F. Supp. 2d at 450.

55 *See Nat'l Health Care Disc. II*, 174 F. Supp. 2d at 899; *LCGM*, 46 F. Supp. 2d at 450.

56 *Nat'l Health Care Disc. I*, 121 F. Supp. 2d at 1265; *LCGM*, 46 F. Supp. 2d at 448.

57 *Nat'l Health Care Disc. I*, 121 F. Supp. 2d at 1260–61; *LGCM*, 46 F. Supp. 2d at 448.

58 *Nat'l Health Care Disc. II*, 174 F. Supp. 2d at 900–02; *see LCGM*, 46 F. Supp. 2d at 452 (noting that damages would be determined at trial).

To explore the second issue, concerning what sorts of limitations actually qualify as limitations on *access*, we can turn to the automated query and employer database cases. For the most part, the CFAA focuses on the act of *accessing* a computer. A key question that arises when the system owner claims that a defendant's conduct violates the CFAA is whether the system owner must show that the defendant violated a policy governing *access* to the computer or whether it is sufficient that the defendant violated a policy on *use* of information obtained through the defendant's access to the computer. An automated query case is illustrative. *Register.com, Inc. v. Verio*[59] involved a domain name registrar.[60] The entity that accredited the registrar, the Internet Corporation for Assigned Names and Numbers ("ICANN"), required the registrar to maintain a database of information about its registrants and to make that database available to the public.[61] Verio used a series of automated requests to extract information about new registrants and then offered competing services to those registrants.[62] The registrar's system was publicly available, and its terms of use did not purport to restrict automated queries to extract data from the system.[63] The terms of use did, however, prohibit the use of the publicly available data for purposes of sending unsolicited email.[64] The district court concluded that the defendant's access to the registrar's system violated § 1030(a)(2)(C)'s prohibition on gaining unauthorized access to a computer and thereby obtaining information.[65] The court reasoned that when Verio gained access to the system, Verio knew that it would use the data it obtained for an unauthorized purpose.[66] That fact, in the court's view, made Verio's *initial access* to the system to acquire the data unauthorized.[67] One could argue that importing policy-based restrictions on *use* into the analysis of what constitutes unauthorized *access* brings a court's approach closer to a paradigm incorporating agency principles or norms of access, because the court's approach validates access limitations drawn from outside of the access policy itself.

---

59 Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004). The court of appeals did not address Register.com's CFAA claims.

60 *Id.* at 241.

61 *Id.* at 241–42.

62 *Id.* at 243.

63 *Id.* at 249 (noting, in the context of state law trespass-to-chattels claim, that terms of use did not "forbid the particular use of the search robot at issue here").

64 *Id.* at 255.

65 *Id.* at 253.

66 *Id.* at 253–55.

67 *Id.* at 253.

Several cases involving improper conduct by employees or former employees raise similar issues. It is (mainly) in this context that courts have characterized their approaches to unauthorized access under the CFAA as "broad" or "narrow."[68] Faced with claims that employees or former employees have misused confidential information that they were entitled to access, some courts have held that a violation of the CFAA occurs only when a defendant violates a policy on *access* to a computer, not when a defendant violates a policy on the *use* of information that the defendant is authorized to obtain.[69] The courts in this group often characterize their approaches as reflecting a "narrow" view of the CFAA. Other courts have held that a defendant's knowledge that he or she will put information obtained from a computer to an unauthorized *use* makes the *access* to the computer unauthorized, even when the employer's policy does not specifically constrain access to the system.[70]

The distinction between "access" restrictions and "use" restrictions, however, is not as crisply drawn as some courts might suggest. Some courts have enforced restrictions on access that attempt to incorporate restrictions on use. For example, an employer may state that its employees have access to a confidential database for a specific purpose and that access to the database for any other purpose is not permitted. The criminal prosecutions in *United States v. Valle*,[71] *United States v. Rodriguez*,[72] and *United States v. John*[73] each fit this paradigm. In each case, an employee had access to sensitive information,[74] but his or her access to that information was limited to a spe-

---

68 *See supra* note 11 and accompanying text.

69 *See, e.g.*, Advanced Fluid Sys., Inc. v. Huber, 28 F. Supp. 3d 306, 329 (M.D. Pa. 2014) ("[T]he CFAA prohibits unauthorized *access* to information rather than unauthorized *use* of such information."); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 620 (E.D. Pa. 2013) (noting that corporate use restrictions could not alter employees' authorized access); State Analysis, Inc. v. Am. Fin. Servs., Ass'n, 621 F. Supp. 2d 309, 317 (E.D. Va. 2009) (finding allegation that a defendant had "used the information in an inappropriate way" insufficient to state a claim under the CFAA); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007) ("Defining 'authorization' based upon the use of computer information, rather than upon the presence or absence of initial permission to access the computer, is in tension with both a plain reading of the Act and the manner in which the term 'authorization' is used in other parts of the Act.").

70 *See, e.g.*, United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); Aquent LLC v. Stapleton, 65 F. Supp. 3d 1339, 1346 (M.D. Fla. 2014).

71 United States v. Valle, 301 F.R.D. 53 (S.D.N.Y. 2014).

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

73 *John*, 597 F.3d 263 (5th Cir. 2010).

74 *Rodriguez*, 628 F.3d at 1258; *John*, 597 F.3d at 263; *Valle*, 301 F.R.D. at 53.

cific business purpose.[75] In each case, the employee obtained information for other purposes. Courts found unauthorized access in each case.[76] It is unsurprising that courts in circuits taking a broad approach would validate such access restrictions. Even some courts in circuits that take a "narrow" view of unauthorized access, however, will validate such restrictions, on the theory that the restriction is a limitation on access rather than use. Under such an approach, liability under the CFAA turns on whether an employer that seeks to restrict its employees' use of confidential information happens to incorporate the use restriction into its policy on access.[77] The line between the "broad" and "narrow" views becomes illusory.

D. Contract Paradigm

The *contract paradigm* is similar to the policy paradigm, except that the contract paradigm encompasses cases in which a court focuses on a contract as the source of restrictions on a user's access to a computer system. As with the policy paradigm, a number of factors influence the scope of the CFAA under this approach, including how carefully a court considers whether an enforceable contract exists and whether the contract addresses access to the computer system or merely use of the information the system contains.

The issue of enforceability presents difficult questions that recur across a range of scenarios implicating technology. For example, courts have wrestled with whether terms presented when a user downloads software are enforceable. Building on "shrinkwrap" cases—cases in which courts enforce licenses included in a box containing software, so long as the consumer has a right to reject the terms by returning the product[78]—courts have enforced "clickwrap"

---

75 *Rodriguez*, 628 F.3d at 1260 (noting that the Social Security Administration conditioned access to its databases on use for a business purpose); *John*, 597 F.3d at 272 (noting that employee's use of information was "contrary to . . . employee policies, of which she was aware"); *Valle*, 301 F.R.D. at 109 (noting that employee received training warning him that accessing databases for non-work-related purposes was improper).

76 *Rodriguez*, 628 F.3d at 1263 ("Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason."); *John*, 597 F.3d at 271 (holding that authorized access "may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system"); *Valle*, 301 F.R.D. at 115 (noting that the defendant's access "was limited to circumstances in which he had a valid law enforcement purpose for querying the system").

77 *Cf.* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 620 n.14 (E.D. Pa. 2013) (noting "open question" of whether "a cleverly crafted employee use policy could define authorized access on the basis of the user's intent").

78 *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452–53 (7th Cir. 1996).

or "click-through" licenses requiring users to click "I Agree" or "I Accept" before downloading a software product.[79] Courts ask in such cases whether the user has reasonable notice of the existence of the governing license terms and whether the "offer" makes clear that clicking the button will signify assent to those terms. Those cases imply that when the owner of a system sets forth terms of use and requires the user to click a button before proceeding, the terms will be enforceable.[80] In cases specifically involving the CFAA, some courts have held that when a user acknowledges limitations on access to a computer system, access that goes beyond those limitations will trigger a violation of the CFAA.[81] Other courts have found that a provider can restrict access to a system simply by including a term stating that anyone who uses the system consents to the provider's terms of use.[82] When a court fails to fully consider difficult issues of notice and assent, the contract paradigm collapses into the policy paradigm.[83]

As for restrictions on access versus restrictions on use, the contract paradigm presents issues similar to the policy paradigm. First, the "contract" the provider seeks to enforce may not address access to the computer system at all.[84] Again, such an approach begins to resemble an agency approach or a norms-of-access approach, under which the court looks beyond any restrictions on access to the system to determine what conduct is "authorized" for purposes of the CFAA.[85] In addition, a carefully worded access restriction can incorporate limitations on use, thereby collapsing the distinction between supposedly "broad" and "narrow" approaches to access.[86]

---

79 *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2243 n.315 (2004) (citing i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010–11 (D.C. 2002) (enforcing forum selection clause where terms were displayed in scroll box and plaintiff subscriber clicked "Accept" button); Caspi v. Microsoft Network, LLC, 732 A.2d 528, 530–31 (N.J. Super. Ct. App. Div. 1999); Moore v. Microsoft Corp., 293 A.D.2d 587 (N.Y. App. Div. 2002); Barnett v. Network Sols., Inc., 38 S.W.3d 200, 204 (Tex. App. 2001)).

80 *See* Bellia, *supra* note 79, at 2244.

81 *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 462 (C.D. Cal. 2009).

82 *See* Bellia, *supra* note 79 at 2244–45 (discussing such cases but noting the importance of not overstating their holdings) (citing Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396, 398–402 (2d Cir. 2004); Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH(BQRX), 2000 WL 525390, at *3 (C.D. Cal. Mar. 27, 2000)).

83 *See id.* at 2245.

84 *See, e.g.*, Aquent LLC v. Stapleton, 65 F. Supp. 3d 1339, 1346 (M.D. Fla. 2014) (noting that defendant signed an offer letter requiring that she "keep such information confidential during [her] employment and at all times thereafter").

85 *See supra* Section I.A, I.B.

86 *See, e.g.*, United States v. Czubinski, 106 F.3d 1069, 1071 (1st Cir. 1997) (finding violation of CFAA where employee browsed tax returns of certain acquaintances, despite having

E. Code Paradigm

Under the *code paradigm*, whether access to a computer is unauthorized depends upon whether an individual breaches a code-based barrier to the system or to certain information on it. The Fourth Circuit's decision in *WEC Carolina Energy Solutions LLC v. Miller*[87] provides an example of how a code-based approach to unauthorized access might operate. Miller, a former employee of WEC, allegedly downloaded proprietary information before resigning his position.[88] He then went to work on behalf of a competitor and used the proprietary information to make a presentation to a customer on behalf of that competitor.[89] WEC had policies limiting unauthorized use of its proprietary information and forbidding the downloading of such information to a personal computer.[90] WEC, relying on *Citrin*, claimed that Miller had no authority to access its computers in a manner adverse to its interests.[91] The court rejected this approach, holding that access "without authorization" occurs only when a defendant "gains admission to a computer without approval,"[92] and access in excess of authorization occurs only when a defendant "uses his access to obtain or alter information that falls outside the bounds of his approved access."[93] The court's understanding of what constituted "approved access" depended not on the employer's policy on the downloading or use of information, but on the fact that the information was accessible in a technical sense to the defendant.[94] Other cases take a similar approach, using the fact that a defendant is technically able to access the information in question as the basis for holding that access is not unauthorized.[95]

The difficulty with *WEC* and similar cases, however, is that they involve situations in which an employee has technical access to a computer system *and* the employer has no policy that speaks clearly to the

---

signed certain documents restricting his "access only [to] those accounts required to accomplish your official duties").

87 WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

88 *Id.* at 200.

89 *Id.*

90 *Id.* at 202.

91 *Id.* at 203.

92 *Id.* at 204.

93 *Id.*

94 *Id.*

95 *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133–35 (9th Cir. 2009); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009).

question of access. In other words, neither the system's code nor a policy or contract incorporates restrictions on access. Thus, one could interpret *WEC* in two ways. First, one could understand *WEC* to mean that unauthorized access under the CFAA is triggered only by a breach of code-based restrictions. Second, one could interpret *WEC* to mean that an unauthorized access claim fails when an employer does not somehow clearly convey the restrictions on access, whether through code or otherwise. In other words, when an employer does not have a policy, contract, or code-based restriction constraining access, a court need not address what sort of limitations on access trigger violations of the CFAA. The *WEC* court, for example, had no occasion to say what it meant to gain admission to a computer "without approval" or what it meant for information to "fall[] outside the bounds of . . . approved access."[96] As discussed above in connection with the policy paradigm[97] and the contract paradigm,[98] a system provider might attempt to condition a user's "access" to the computer on conduct in furtherance of the employer's interests or on the employee's intention to use the information in a manner consistent with the employer's interests. WEC's failure to adopt a policy or contract restricting access meant that the court did not need to grapple with whether access for personal purposes or for purposes adverse to the employer's interests would become access without or in excess of authorization.

Courts' attempts to distinguish *WEC* and similar cases on the grounds that such cases involved no restrictions on access raise the possibility that there are no cases truly fitting the "code paradigm"—that all courts would honor policies or contract terms that explicitly restrict access short of the level of access that is possible as a technical matter. Key language in many of the cases rejecting CFAA liability, however, suggests that at least some courts would take a pure code-based approach. *WEC* offered the example of an employee who uses his computer in a manner contrary to a company access policy—for example, to "check[] the latest Facebook posting or sporting event scores."[99] The court rejected the notion that Congress intended the CFAA to treat such violations of company policy as unauthorized access.[100] The U.S. Court of Appeals for the Ninth Circuit made a simi-

96 *WEC Carolina Energy Sols. LLC*, 687 F.3d at 204.

97 *See supra* Section I.B.

98 *See supra* Section I.C.

99 *WEC Carolina Energy Sols. LLC*, 687 F.3d at 206.

100 *Id.*

lar point in its en banc decision in *United States v. Nosal* ("*Nosal I*"),[101] a 2012 case rejecting the proposition that employees of an executive search firm "exceed[ed] authorized access" when they downloaded confidential information from a company database for an improper purpose—to provide that information to Nosal, a former colleague who had established a competing firm.[102] The court observed that, under what it described as a "broad" interpretation of the CFAA, "minor dalliances" such as "g-chatting with friends, playing games, shopping or watching sports highlights" in violation of an employer's computer use policy would become federal crimes.[103] Both *WEC* and *Nosal I* suggested that use of a computer in a manner contrary to such policies would not trigger liability under the CFAA's unauthorized access provisions.[104] Importantly, courts taking this position do not suggest that the CFAA is inapplicable because employees might lack notice of the restrictive use policy or might not have agreed to it. Rather, they suggest that the CFAA simply should not apply in such a case.[105] That view necessarily depends on the technical openness of

---

101 United States v. Nosal (*Nosal I*), 676 F.3d 854, 860–61 (9th Cir. 2012) (en banc).

102 *Id.* at 864 ("Because Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of 'without authorization, or exceeds authorized access . . . .'"). After the Ninth Circuit dismissed the CFAA counts that had been based on Nosal's aiding and abetting the employees' alleged misuse of the company's confidential database, the government filed a superseding indictment alleging that once the employees left the executive search firm, they continued to access the database at Nosal's behest through use of a then-current employee's password, and that such access was "without authorization" under the CFAA. The Ninth Circuit affirmed Nosal's conviction under the CFAA for aiding and abetting the former employees' conduct. United States v. Nosal (*Nosal II*), 828 F.3d 865, 880 (9th Cir. 2016).

103 *Nosal I*, 676 F.3d. at 860.

104 *WEC Carolina Energy Sols. LLC*, 687 F.3d at 206 ("Although an employer might choose to rescind an employee's authorization for violating a use policy, we do not think Congress intended an immediate end to the agency relationship and, moreover, the imposition of criminal penalties for such a frolic."); *Nosal I*, 676 F.3d at 862 ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty.").

There is undoubtedly some tension between *Nosal I* and *Nosal II*. *See Nosal II*, 828 F.3d at 894 (Reinhardt, J., dissenting). The latter case, however, did not purport to reject the former case's holding that employees' use of a computer system for the improper purpose of downloading confidential information does not constitute "exceed[ing] authorized access." *Id.* at 869 (noting that the case is not about "violating a company's internal computer-use policies").

105 *See* Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 385 (S.D.N.Y. 2010) (noting that while violation of confidentiality agreements "might sustain a breach of contract, breach of fiduciary duty, or theft of trade secrets claim, it does not . . . support a CFAA claim").

the employer's system, even in the face of policies or contracts that purport to restrict access.[106]

In sum, courts have struggled to resolve what constitutes unauthorized access to a computer system. Courts have fallen in line with what they have characterized as "broad" or "narrow" views of the CFAA. In fact, there are multiple fissures in the caselaw: between courts adopting and rejecting the agency approach; between courts validating and rejecting use limitations as the basis for finding unauthorized access; and between courts validating and questioning nontechnical limitations on access.

II. Rethinking Unauthorized Access: Doctrinal Issues

The difficulties that courts and commentators face in resolving what constitutes unauthorized access under the CFAA stem in part from the statute's incremental evolution in the face of a dramatically shifting technological landscape. Before turning to the interpretive issues, this Part summarizes that evolution—not to claim that the CFAA reflects a single principle to guide the resolution of questions of statutory interpretation, but to provide some context for the interpretive discussion that follows.

A. Legislative Context: The Expansion of the CFAA

Congress first tackled computer crime in 1984, adopting the Counterfeit Access Device and Computer Fraud and Abuse Act as part of a large appropriations and crime control measure.[107] The statute covered one who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend,"[108] and by means of such conduct achieves one of three prohibited ends: (1) obtains national security information;[109] (2) obtains information from a record of a financial institution or

---

106 *See* State Analysis, Inc. v. Am. Fin. Servs. Ass'n, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (describing authorities as rejecting "attempts to apply the CFAA to cases where the defendants are not alleged to have 'broken into' the system but to have abused the privileges of a license"); *cf. Nosal II*, 828 F.3d at 878 (rejecting the argument that the district court ought to have instructed the jury "that the CFAA only criminalizes access where the party circumvents a technological access barrier," but acknowledging that the former employees' use of another's password in fact circumvented a technological barrier to access).

107 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (codified at 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985)).

108 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985).

109 *Id.* § 1030(a)(1).

credit reporting agency;[110] or (3) "uses, modifies, destroys, or discloses information in, or prevents authorized use of" a U.S. government computer.[111] The statute did not define what it meant to "access" a computer or to have "authorization" to do so.

Two years later, in the Computer Fraud and Abuse Act of 1986,[112] Congress clarified the statute and expanded its reach. First, the amendments substituted the phrase "exceeds authorized access"[113] for the more cumbersome concept of "us[ing] the opportunity" that access with authorization provides "for purposes to which such authorization does not extend." Congress retained the existing unauthorized access offenses and added two new ones: in new § 1030(a)(4), unauthorized access with intent to defraud, by which one furthers the intended fraud and obtains anything of value;[114] and in new § 1030(a)(5), unauthorized access that "alters, damages, or destroys information."[115] Congress tied each of these offenses to a "[f]ederal interest computer,"[116] defined to include (1) computers used exclusively or in part by a financial institution or the United States government; and (2) "one of two or more computers used in committing the offense, not all of which are located in the same State."[117]

Despite the introduction of the term "[f]ederal interest computer," the scope of the CFAA remained fairly narrow. The first definition of a federal interest computer overlapped with the range of computers covered in the original 1984 statute. Although the second definition covered computers without a nexus to the federal government or a financial institution, it required an interstate nexus: that the offense involved multiple computers in an interstate computer network or unauthorized access to a networked computer located in another state. The state of technology and the realities of networking thus circumscribed the statute's reach: the internet was not in widespread use, and so the addition of provisions targeting interstate offenses did not dramatically expand the statute's scope.

---

110 *Id.* § 1030(a)(2).

111 *Id.* § 1030(a)(3).

112 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended 18 U.S.C. § 1030 (Supp. V 1988)).

113 *Id.* § 2(c), 100 Stat. at 1213.

114 *Id.* § 2(d), 100 Stat. at 1213–14.

115 *Id.* § 2(d), 100 Stat. at 1214. Congress also added a third crime involving trafficking in a "password or similar information through which a computer may be accessed without authorization." *Id.*

116 *Id.* § 2(d), 100 Stat. at 1213–14.

117 *Id.* § 2(g)(4), 100 Stat. at 1215.

Congress made two important changes to the CFAA in the Violent Crime Control and Law Enforcement Act of 1994,[118] before significantly revising the statute in 1996. First, Congress amended § 1030(a)(5), which had targeted one who accesses a federal interest computer without authorization or exceeds authorized access and thereby "alters, damages, or destroys information."[119] The 1994 version of § 1030(a)(5) no longer required unauthorized access to a computer, but instead focused on one who, "through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command" to a computer without authorization.[120] That conduct, when pursued with intent to cause damage or with reckless disregard for the risk of damage, would violate the CFAA if a certain level of damage or impairment resulted.[121] Second, Congress added a civil cause of action for most violations of the CFAA.[122]

The 1996 amendments, adopted as part of the Economic Espionage Act of 1996,[123] likewise expanded the reach of the CFAA in two significant ways. First, Congress discarded the term "[f]ederal interest computer" in favor of the term "protected computer." The latter term was significantly broader in scope because it focused on the use of a target computer "in interstate or foreign commerce or communication" rather than requiring that two of the computers involved in the offense be located in different states.[124] Under the revised approach, the CFAA could protect virtually any networked computer, regardless of whether the offense itself was interstate in nature. Because any internet-connected computer is used in interstate communication, the growth in use of the internet worked a corresponding increase in the CFAA's coverage.

Second, the Economic Espionage Act expanded key substantive offenses under the CFAA. In prior versions of the statute, § 1030(a)(2) covered one who obtained information from financial records. Congress amended § 1030(a)(2) to cover not only obtaining information from financial records, but also obtaining information

---

118 Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified at 18 U.S.C. § 1030 (1994)).

119 *See supra* notes 117, 118 and accompanying text.

120 Violent Crime Control and Law Enforcement Act § 290001(b), 108 Stat. at 2097–98.

121 *Id.*

122 *Id.* § 290001(d), 108 Stat. at 2098.

123 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. § 1030 (2000)).

124 *Id.* § 201(4), 110 Stat. at 3493.

"from any department or agency of the United States" and "information from any protected computer if the conduct involved an interstate or foreign communication."[125] In addition, the amendments broadened § 1030(a)(5), the provision prohibiting the transmission of harmful code. The earlier version required that the offense be executed "through means of a computer used in interstate commerce or communications,"[126] whereas the new version required only that the transmission reach a "protected computer."[127] As with the other offenses involving a protected computer, the effect of the amendment was to protect any networked computer, rather than requiring a connection between the computer used in the offense and interstate commerce or communication. Congress also added two new offenses for accessing a computer without authorization and causing damage.[128]

Five years later, following the attacks of September 11, 2001, Congress included certain amendments to the CFAA in the USA PATRIOT Act.[129] Again Congress expanded the scope of the CFAA, this time by redefining a "protected computer" to include "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."[130] In theory, the specific reference to computers located outside the United States would overcome any presumption that Congress did not intend for the CFAA to have extraterritorial reach. In addition, by focusing on computers that "affect" interstate commerce or communication, rather than computers used in interstate commerce or communication, the statute could reach as far as the Commerce Clause of the Constitution permits.[131]

In summary, over the last three decades, Congress has repeatedly revisited the scope of the CFAA. Congress has modified or added

---

125 *Id.* § 201(1)(B), 110 Stat. at 3492.

126 Violent Crime Control and Law Enforcement Act § 290001(b), 108 Stat. at 2097–98.

127 Economic Espionage Act § 201(1)(E), 110 Stat. at 3492.

128 *Id.*

129 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 814, 115 Stat. 272, 382–83 (codified at 18 U.S.C. § 1030 (2000 & Supp. I 2001)).

130 *Id.* § 814(d), 115 Stat. at 384.

131 Congress has amended the CFAA on three more occasions, making technical changes in 2002, *see* Criminal Law Technical Amendments Act of 2002, Pub. L. No. 107-273, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), 116 Stat. 1806, 1807–08, 1812–13 (codified as amended at 18 U.S.C. § 1030 (2006)), and enhancing the criminal penalties in 2002 and 2008, *see* Homeland Security Act of 2002, Pub. L. No. 107-296, § 225(g), 116 Stat. 2135, 2158 (codified as amended at 18 U.S.C. § 1030 (2006)); Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 204(a)(2), 122 Stat. 3560, 3561–63 (codified at 18 U.S.C. § 1030 (2012)).

substantive offenses on a number of occasions. Perhaps more important, Congress has extended the statute's coverage to an ever-increasing range of computers. The statute initially covered specific governmental or financial computers. Although Congress covered certain interstate offenses in 1986, the fact that interstate computer networks were not in wide use limited the statute's practical reach. Congress added a civil cause of action when that reach was still limited. The extension of the statute's protection to any computer used in interstate communication, coupled with explosive growth of the internet, transformed the CFAA. The dramatic expansion of the CFAA's coverage in part explains the challenge of interpreting the statute.

With this statutory background in place, the next two Sections examine how courts should understand the concept of unauthorized access.

B. Interpreting "Access"

The CFAA does not define what it means to "access[]" a computer. A court considering the term would likely give "access" its common meaning—for example, "to be able to use, enter, or get near (something)."[132] Dictionary definitions of access in the verb form, however, are susceptible to two different interpretations. From a broad view, to access a computer is simply to transmit electronic signals to it for the computer to process.[133] From a narrower view, to access a computer is to gain entry to it, in the sense of obtaining privileges to use the computer that are not available to the general public.[134]

One's understanding of what it means to "access[]" a computer can have a dramatic effect on the scope of the CFAA. Under the broad view of access, to transmit any command to a computer (or to cause a command to be transmitted to a computer) is to access that computer. For example, when a user sends an email message, the user "accesses" her outgoing mail server by asking the mail server to transmit a message, she "accesses" the intended recipient's incoming mail server, and she even "accesses" the recipient's computer. Similarly, when a user types a URL into a web browser, he "accesses" the domain name servers that translate the URL into an Internet Protocol address and he "accesses" the web server that hosts the web page he is

132 *Access*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003).

133 *See* Kerr, *supra* note 10, at 1646–47.

134 *See* Bellia, *supra* note 79, at 2253–54.

seeking. Under this approach, any internet-related transmission begins a chain of events that results in the user's computer "accessing" a series of networked computers.

Under the narrower approach to "accessing" a computer, only those transmissions that grant a user the functional equivalent of privileged entry into a computer system result in a user "accessing" that system.[135] Returning to the email example, sending an email is not accessing the recipient's computer any more than sending a postcard accesses the recipient's home. Logging into another user's computer, and thereby gaining the technical ability to manipulate the computer in the same way that the user would, would certainly qualify as accessing the computer. Launching the process of contacting a domain name server to translate a domain name into an Internet Protocol address would not constitute accessing the server, but obtaining privileges that would permit one to overwrite a file on the domain name server would constitute accessing the server.

How should courts choose between these two plausible understandings of what it means to "access" a protected computer? The surrounding text and the statute's history provide some insight. Regarding the text of the statute, consider an anomaly that the broader understanding of "access" creates. As discussed earlier, the current statute contains certain computer damage provisions. Section 1030(a)(5)(A) prohibits one from "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."[136] The two subsequent paragraphs, § 1030(a)(5)(B) and (C), prohibit "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage"[137] and "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."[138] All three of these provisions were adopted in the 1996 revision of § 1030(a)(5),[139] although Congress had included a version of the provision governing "transmission of a program, information, code, or command" in the 1994 amendments.[140]

---

135 *See id.*

136 18 U.S.C. § 1030(a)(5)(A) (2012).

137 *Id.* § 1030(a)(5)(B).

138 *Id.* § 1030(a)(5)(C).

139 Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3492.

140 Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(b), 108 Stat. 1796, 2097–98 (codified at 18 U.S.C. § 1030(a)(5)(A) (1994)).

If any transmission of a command to a protected computer constitutes "access" to that computer, then the structure of § 1030(a)(5) is odd. Although each paragraph contains a different scienter requirement, if transmitting a command to a computer is equivalent to accessing that computer, Congress could have varied the scienter requirements but written all three paragraphs to cover "caus[ing] the transmission of a program, information, code, or command," rather than covering a transmission in one paragraph and access in the other two. Likewise, if the concepts of transmission and access were truly interchangeable, Congress could have written all three paragraphs to cover "access[ing] a protected computer." Section 1030(a)(5)(A) may be narrower in theory than the other paragraphs, because it could presumably cover the conduct of one who has authority to access a computer. Still, because several provisions of § 1030 cover both one who acts without authorization and one who exceeds authorized access, it seems unlikely that Congress intended the "caus[ing] the transmission" language to replicate that concept.

In other words, interpreting "accessing" a computer to mean merely transmitting a command to the computer creates interpretive difficulties in § 1030(a)(5). One could argue that the computer damage provisions cannot provide insight into what Congress meant by "access," since the first version of what is now § 1030(a)(5)(A) appeared in 1994,[141] whereas the term "access" was part of the original 1984 statute.[142] Still, the 1994 version of § 1030(a)(5)(A) supplanted a prior provision that covered "access[ing]" a covered computer without authorization and thereby altering, damaging, or destroying information in it.[143] Had Congress equated accessing a computer with causing transmission of a command to it, it need not have substituted transmission for access. Similarly, because Congress rewrote § 1030(a)(5) in 1996,[144] one can presume that if Congress equated transmissions causing damage with access causing damage, it would have used the transmission language throughout all of § 1030(a)(5).

More broadly, the legislative history of the CFAA casts doubt on a reading of the statute that equates accessing a computer with transmitting a command to it.[145] As discussed earlier, when it passed the

---

141 *Id.* § 290001(b), 108 Stat. at 2097.

142 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified at 18 U.S.C. § 1030 (Supp. II 1985)).

143 *See* 18 U.S.C. § 1030(a)(5)(A) (Supp. V 1988).

144 *Id.* § 1030(a)(5).

145 *See* Bellia, *supra* note 79, at 2256–58.

first version of the computer crime statute in 1984, Congress targeted a narrow range of computers: those containing national security information, those containing financial data, and those operated by or on behalf of the government.[146] The House Report accompanying the statute emphasized the government's and businesses' growing reliance on computers, as well as the threat that increased networking would make society more vulnerable to hacking incidents.[147] Although the statute covered both those who would access a computer without authorization and those who would abuse authorized access, none of the computers covered in the statute were available to the general public.[148] The reach of the initial statute, then, is consistent with a concept of accessing a computer in the sense of privileged entry rather than mere transmission.

The 1986 statute maintained the three offenses from the original version of 18 U.S.C. § 1030 (with slight modifications), but added three new ones, two of which were unauthorized-access offenses.[149] As noted earlier, both of these new offenses covered unauthorized access to "[f]ederal interest computers."[150] Although Congress thereby expanded the CFAA's reach to cover certain interstate offenses, nothing in the debate over the statute's passage indicates that Congress sought to extend the statute to unauthorized transmissions to all networked computers.[151] Rather, the legislative record emphasizes issues of security and confidentiality.[152] The legislative history of

---

146 Counterfeit Access Device and Computer Fraud and Abuse Act § 2102, 98 Stat. at 2190–91; *see supra* notes 109–11 and accompanying text.

147 *See* H.R. REP. NO. 98-894, at 8–12 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3694–97.

148 Counterfeit Access Device and Computer Fraud and Abuse Act § 2102, 98 Stat. at 2190–91.

149 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(d), 100 Stat. 1213, 1213–14; *see supra* notes 116–17 and accompanying text.

150 Computer Fraud and Abuse Act § 2(d), 100 Stat. at 1213–14.

151 *See* Bellia, *supra* note 79, at 2257.

152 *Id.* at 2257 n.363 (citing 132 CONG. REC. 28,821 (1986) (statement of Rep. Hughes) (noting that bill was designed to "deter[ ] the emergence of the computer criminal"); *id.* (statement of Rep. Wyden) (discussing dangers of hacking); *id.* at 27,640 (statement of Sen. Trible) (discussing need to ensure that "our criminal justice system is capable of addressing the types of offenses that have accompanied the rise of new technologies" and pointing in particular to acts of "theft, vandalism, and trespass" of computer data); *id.* at 27,639 (statement of Sen. Thurmond) (stating that legislation was designed "to address the real and growing danger of computer crime"); *id.* at 12,109 (statement of Rep. Rodino) (noting that legislation seeks to deter "future attempts by high technology criminals in our society"); *id.* at 7816 (statement of Rep. Hughes) (stating that legislation targets "the computer sophisticated criminal who combines his technological skill with old-fashioned greed and criminal intent to rob banks or destroy business records or steal trade secrets")).

the 1996 amendments, which adopted the "protected computer" language that now prevails in the statute,[153] reflects the same concerns.[154]

In short, the term "access" may have a thus far underappreciated role in narrowing the CFAA. Nevertheless, one could argue that even if the term "access" in 1984 or 1986 was properly understood to involve entry into rather than transmission to a computer system, this was so by virtue of the limitations of the systems rather than the limitations of the term "access." The examples of the "broad" view of access offered above included transmissions through mail servers and requests to view particular web pages. The technology involved in the former example was not in wide use, and the technology involved in the latter example did not exist, when Congress first introduced the concept of unauthorized access in 1984. The question of how technological change should affect the task of statutory interpretation has complex normative dimensions that are beyond the scope of this Article. For now, it is enough to say that courts construing the CFAA have neglected the possibility that the term "access" provides a limiting principle for construing the reach of the statute.

C. Interpreting "Without Authorization" or "Exceed[ing] Authorized Access"

The CFAA does not define what it means to be "without authorization" to access a protected computer. The statute does define "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[155] The "exceeds authorized access" definition does not illuminate the concept of "authorization," since it incorporates that term. Courts have therefore turned to dictionary definitions of "authorization" and have concluded that to access a computer without authorization is to

153 Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(4)(A), 110 Stat. 3488, 3493 (codified as amended at 18 U.S.C. § 1030(e)(2) (2000)).

154 Bellia, *supra* note 79, at 2257 n.364 (citing 142 CONG. REC. 27,118 (1996) (remarks of Sen. Leahy) (stating that act will protect "privacy, security, and reliability of computer networks"); *id.* at 25,910 (statement of Rep. Goodlatte) (stating that act will provide "much needed protection for our Nation's important information infrastructure and help maintain the privacy of electronic information"); *id.* at 23,783 (statement of Sen. Kyl) (stating that act will "strengthen current public law on computer crime and protect the national information infrastructure" and "protect banks, hospitals, and other information-intensive businesses which maintain sensitive computer files from those who improperly enter into computer systems"); *id.* at 23,784 (statement of Sen. Leahy) (arguing that existing statute fell short in protecting "privacy and confidentiality of information")).

155 18 U.S.C. § 1030(e)(6) (2012).

access it without permission or approval or without formal warrant or sanction.[156] To exceed authorized access, then, would be to go beyond whatever access is permitted or approved.

Even if we understand "authorization" to mean "permission" or "approval," we still must ask how the owner of a computer system must convey the limits of that permission or approval in order to trigger the CFAA's protection against unauthorized access. There will be some situations in which the signal might be direct and unmistakable—for example, when a system owner specifically revokes an individual user's access.[157] Part III addresses the separate question of whether a system owner's consent (or revocation thereof) *ought* to dictate the contours of unauthorized access. Assuming that a system owner's consent does dictate the contours of unauthorized access, and in the absence of such an explicit signal, the five paradigms described in Part I appear to reflect different answers to the question of how a system owner must signal the limits of his or her consent. Under the agency paradigm, a system owner need not signal which uses of the system are permissible at all, because an external legal obligation (i.e., the duty of loyalty) conveys what is permissible. Likewise, under the norms-of-access paradigm, a system owner need not convey limits on the use of the system, because the user ought to know what they are. The policy and contract paradigms presume that a system owner has a policy or contract in place delineating the limits of access of the system. The difficulty arises when the policy or contract is not clear, or conflates access and use limitations. Finally, under the code paradigm, the limits of access are defined by technical boundaries.

In effect, courts applying the different paradigms will accept as valid different signals of the scope of the owner's consent to use of the system. Agency principles and norms of access provide a proxy for the uses to which the system owner would have consented; the policy, contract, and code-based paradigms signal the uses to which the system owner did consent. Each paradigm reflects a different understanding of how strong a signal must be before a court treats it as triggering a user's actual or constructive knowledge of what uses of the system are permitted or approved.

---

156 *See, e.g.*, *Nosal II*, 828 F.3d 865, 875 (9th Cir. 2016); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).

157 *See Nosal II*, 828 F.3d at 871 ("After Nosal became a contractor and Christian and Jacobson left Korn/Ferry, Korn/Ferry revoked each of their credentials to access Korn/Ferry's computer system.").

Assuming that the concept of unauthorized access should be about the limits of a system owner's consent—a matter on which Part III casts some doubt—the question still remains: does the CFAA point to a particular understanding of how a system owner must signal the limits of his or her permission or approval? Part III explores a range of policy arguments that support an interpretation requiring strong signals of the boundaries of a system owner's consent. For now, it is sufficient to consider how the possible understandings of the boundaries of authorization align with the possible understandings of access.

Assume that the broad understanding of access (i.e., that the transmission of a command to a computer constitutes access) is correct. Assume also that the CFAA validates a wide range of signals concerning the limits of a system owner's consent. Under such an approach, the statute's scienter requirements prove critical. One would have to read the statute to require that the user intends to act without authorization or that the user knows or has reason to know that his or her actions were without authorization. Without a full assessment of what the user knew or intended, the CFAA could validate all stated or implied restrictions on use of a system, making the statute breathtakingly broad. Some commentators' discomfort with the breadth of conduct the CFAA would reach under this interpretation leads them to link a broad definition of access with a far narrower definition of authorization.[158] Under this approach, accessing a computer without authorization is bypassing a code-based barrier, such as a password requirement.[159] The CFAA, under this view, is not concerned with all forms of authorization, but only with a specific type of authorization—that is, authentication.

If one adopts a broad view of "access," the narrower approach to authorization is indeed normatively attractive. As a matter of statutory interpretation, however, it raises two potential difficulties. First, the term "without authorization" is used not only in connection with access-related offenses, but also in the computer damage provision. The premise of the computer damage provision is that one can transmit a harmful command and cause damage "without authorization."[160] If we link "authorization" in the access provisions to a concept of authentication, or to meeting the requirements of a similar code-based barrier, the computer damage provision becomes nonsensical, unless

158 *See, e.g.*, Kerr, *supra* note 10, at 1649.

159 *See id.*

160 18 U.S.C. § 1030(a)(5)(A).

we assign a different meaning of "authorization" for that provision—a step that would run afoul of principles of statutory interpretation.[161] Second, equating authorization with authentication through use of a "key" (such as a password) to a computer system does not, without more, reach problematic conduct such as wrongful use of a password. To reach such conduct, we must incorporate the concept of *proper use* of the means authentication: to access a covered computer without authorization is (among other things) not only to evade a code-based restriction altogether, but to meet the requirements of the code-based restriction by improperly obtaining or possessing the equivalent of the "key." Once we open the concept of acting "without authorization" to encompass improperly obtaining or using something that facilitates accessing a covered computer, however, it is unclear why other sorts of use restrictions do not factor into the authorization. For example, use of a password to obtain information for personal purposes rather than business purposes becomes an action without authorization—possibly rendering redundant the concept of exceeding authorized access in the statute.

The narrower understanding of access, as a form of entry rather than transmission, avoids some of these interpretive difficulties. It reconciles the use of the phrase "without authorization" in the access provisions and in the computer damage provisions because it eliminates the need to import code-based restrictions into the concept of "authorization."[162] It also creates distinct liability for accessing a computer without authorization and exceeding one's authorization to access a computer. The former applies to one who has no privileges to enter the restricted areas of a system; the latter applies to one who has privileges to some areas of a system but not others.

The next Part discusses the normative considerations that point toward a narrow understanding of unauthorized access, whether that understanding is based on narrow concepts of "accessing" a computer or narrow concepts of a lack of authority.

---

161 *See, e.g.*, Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007) ("[I]dentical words and phrases within the same statute should normally be given the same meaning.").

162 *Cf. Nosal II*, 828 F.3d at 878 (observing that a provision equating access "without authorization" to access circumventing a technological barrier is "missing from the statutory language").

III. Rethinking Unauthorized Access: Normative Issues

This Part considers some of the normative implications of the different readings of the CFAA discussed thus far. This discussion ties back to the statutory interpretation questions, inasmuch as courts incorporate some of these normative considerations into canons of statutory construction. Some of the normative considerations, however, go beyond questions of statutory construction. In other words, even if Part II's narrow conception of unauthorized access is incorrect, this Part suggests that Congress should rethink the coverage of the CFAA.

A. Constitutional Concerns

First and most important are the constitutional concerns that arise from broad interpretations of unauthorized access under the CFAA. The vast majority of cases construing the CFAA arise in the civil context, but the same conduct that would be the basis for civil liability is also the basis for criminal liability. The Constitution requires that criminal statutes speak with sufficient clarity to provide notice of what conduct is prohibited and to prevent arbitrary or discriminatory enforcement.[163] Wherever possible, a court must "construe, not condemn, Congress' enactments."[164] Part I explored the range of approaches that courts have taken to determine what it means to access a computer without or in excess of authorization.[165] If construing unauthorized access to encompass, for example, a violation of a website's terms of service would render the CFAA unconstitutionally vague, then a court should avoid that construction.[166] In addition, the rule of lenity instructs a court facing an ambiguous statute to choose the construction that favors the defendant.[167] Because courts must construe a statute with both criminal and civil applications consistently across the two contexts, courts apply these canons in civil as well as criminal cases.

Different paradigms for unauthorized access raise significant vagueness concerns. When a court treats a policy or a contract as the basis for liability under the CFAA, it permits private parties to dictate

---

163 *See, e.g.*, Skilling v. United States, 561 U.S. 358, 402–03 (2010); Kolender v. Lawson, 461 U.S. 352, 357 (1983).

164 *Skilling*, 561 U.S. at 403.

165 *See supra* Part I.

166 *Cf.* United States v. Drew, 259 F.R.D. 449, 464–66 (C.D. Cal. 2009) (overturning misdemeanor conviction under CFAA after concluding that construing unauthorized access to include violation of MySpace terms of service would render statute unconstitutionally vague).

167 *See, e.g.*, *id.* at 463.

the contours of the statute.[168] It is difficult to see how such an approach gives fair notice of the basis for criminal sanctions. In addition, the distinction Part I draws between the policy paradigm and the contract paradigm highlights the fact that courts sometimes do not carefully consider whether a user knows or has reason to know of the restrictions on access that a system owner seeks to impose. Interpreting the CFAA to mean that conduct inconsistent with restrictions contained in terms of use, without more, constitutes unauthorized access would raise significant constitutional concerns. It is more difficult to say whether the norms-of-access paradigm raises vagueness concerns. In theory, if a court looks for reasonable expectations or a shared understanding regarding how technology is to be used, the court is measuring societal expectations rather than conjuring its own view of what constitutes permissible access. Still, to the extent that access norms are underdeveloped, interpreting the CFAA to permit reliance on those norms raises constitutional questions.

As for the agency paradigm, under which a court imports agency principles to set the boundaries of permissible access under the CFAA, one could argue that concerns about vagueness are less significant because the premise of the agency approach is that an employee (or other agent) breaches a duty defined by law—albeit one that may be unconnected to any policy or contract purporting to govern access to a protected computer. Still, applying an agency theory to questions of unauthorized access raises significant difficulties. The premise of the agency approach is that it is easy to distinguish situations in which the employee is acting in the employer's interest (and thus as a faithful agent) from situations in which the employee is not. Cases like *Citrin*, in which the defendant started a competing enterprise, lie at one extreme.[169] At the other extreme lie a range of activities—using a computer network to read personal email or to check a Facebook page, for example—that seem more benign, but that still may not serve an employer's interest and may even inflict a cost in terms of lost productivity.[170] There is a range of scenarios in between, and it is difficult to say what factors—the magnitude of the potential loss to the employer? the employee's intent?—should determine which conduct violates the CFAA.

---

168 *See* Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 768–69 (2013).

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

170 *See, e.g.*, WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012).

These concerns about clarity and the need to construe ambiguous criminal statutes favorably to the defendant suggest that approaches under which courts link unauthorized use in the CFAA to policies or terms of use are inappropriate (at least without a full examination of issues of notice and assent). These concerns might also suggest that the norms-of-access and paradigms are also inappropriate.

B. Other Policy Concerns

Assume that each of the paradigms discussed in Part I simply reflects a different way for a system owner to signal the limits of his or her consent to the use of the computer system. Even if the law generally protects the system owner's ability to use a range of mechanisms to signal his or her consent, it is not at all clear that the CFAA should do so.

If authorization under the CFAA is truly about the system owner's consent to the use of his or her system, the fact that the CFAA is a criminal statute means that the limits of that consent for purposes of CFAA liability ought to be conveyed clearly—even if other areas of the law might not demand the same degree of clarity. For example, the agency and norms-of-access paradigms aim to identify the range of uses to which a system owner would consent. By importing questions about the employee's duty of loyalty, the agency approach makes liability under the CFAA turn on the employee's intent. In any given case, an employee's motives may be complex and in flux. The agency approach, in other words, presumes that an employee's motives will generate clarity about the scope of the employer's consent, but that may not be the case.

Similarly, norms of access may be unclear or underdeveloped in some contexts. Indeed, it is not obvious whether a court's inquiry into unauthorized access under this approach should look to how the system owner believes the system ought to be used, or how a reasonable person thinks the system ought to be used. If the norms-of-access paradigm provides no guidance on whose perspective should control, it is hard to see how it could provide clarity to a user.

There is little question that code-based limits on access generally provide better notice of the system owner's consent than do other signals, including policy-based and contractual restrictions. For example, a user must confront and overcome a code-based limitation in order to use the system, but he or she will not always encounter policy-based or contractual limitations when using the system. Moreover, outside the context of code, signals of a system owner's consent sometimes

will conflict in ways that complicate the user's understanding of the scope of permissible access. For example, an employer's policy might state that employees are not permitted to access the company's computer system for any non-work-related purpose. A widespread workplace norm that permits incidental use of the system to send personal email or to monitor one's Twitter feed would conflict with that policy. Similarly, a user browsing a website may encounter no technical barriers to access. Nevertheless, the website may have a term of use that purports to restrict certain uses of the information gathered from the site.

In particular cases, of course, terms of use—or, for that matter, actual notice through a cease-and-desist letter—may be equally effective in signaling the limits of the system owner's permission or approval. And under other legal doctrines, those devices may provide enforceable limits on the use of a computer system.[171] The argument here is simply that in the context of a federal criminal statute, the law should require the sort of unambiguous signals of a lack of permission or approval that code-based restrictions convey.

Note that requiring a system owner seeking the protection of the CFAA to embed signals about consent into the system's code itself does not unduly burden the system owner. It is not the case that a system owner must use code-based restrictions to gain *any* legal protection, only that a system owner must do so to gain the protection of *the CFAA*. The CFAA is not the only cause of action the employer can use to seek damages from the disloyal employee. Indeed, in disputes involving alleged misconduct by employees or former employees, a broad interpretation of the CFAA converts matters of employee misappropriation and unfair competition into criminal conduct.[172] Apart from the fact that such an approach permits a system owner to dictate the contours of the statute, the approach federalizes a range of disputes that have traditionally been within the purview of state law.

In sum, a code-based approach to the CFAA offers a number of advantages. First, the signals that it conveys about the system owner's permitted uses are unmistakable. The same cannot be said for policy-based or contractual restrictions on the use of the system. Second, a code-based approach avoids the significant vagueness concerns that plague broader interpretations of the CFAA. Finally, a code-based

---

171 For an argument that such mechanisms generally *should*, outside the context of the CFAA, provide enforceable limits on the use of a computer system, see Bellia, *supra* note 79, at 2224–25.

172 *See, e.g.*, United States v. John, 597 F.3d 263, 272, 289 (5th Cir. 2010).

approach forces system owners to weigh the costs of closing his or her system. Broad interpretations of the CFAA can have disruptive effects with respect to computer systems that are otherwise open to the public. If the CFAA permits a system owner to eliminate any unwanted uses of his or her computer system simply by objecting to them (and thereby rendering access unauthorized for purposes of the CFAA), the CFAA may displace the balance between access and enclosure that copyright law strikes.[173] The CFAA would thereby permit a system owner to achieve the benefits of closed access without internalizing any of the costs of doing so.

Conclusion

Courts will continue to struggle with what constitutes unauthorized access for purposes of the CFAA. Statutory and technological changes have repositioned the CFAA as a ready weapon in commercial disputes involving access to computer systems or use of information those systems contain. Careful construction of the statute should lead courts to a narrower conception of unauthorized access than that which many courts have adopted to date. In particular, a code-based approach is truer to the text and history of the statute and aligns with a range of normative concerns.

There are, of course, various forms of misconduct that would escape the reach of the CFAA under a code-based interpretation. The law addresses matters such as the theft of trade secrets and misappropriation of information in various ways; a narrow interpretation of the CFAA still preserves a number of legal avenues for those harmed by alleged misuse of a computer system, while avoiding constitutional and policy pitfalls.

---

173 *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 Md. L. Rev. 320, 323 (2004).