The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying *United States v. Nosal*

*Jonathan Mayer**

Abstract

Over the past decade, courts have radically reshaped the landscape of federal computer crime law. Through a set of innovative interpretive maneuvers, the judiciary has both greatly clarified and sharply narrowed the scope of Computer Fraud and Abuse Act ("CFAA") liability. This "narrow" CFAA doctrine is winning rapid adoption; it has persuaded three courts of appeals and numerous district courts.

But the narrow interpretation of the CFAA has proven perplexing for scholars and practitioners. It does not neatly match prior judicial constructions of the statutory scheme. It also does not match prior scholarly interpretations, including the "code-based" standard that has captured academic favor.

This Article aims to clarify and formalize the narrow CFAA doctrine. It makes three contributions: First, it explains the recent trends in judicial interpretation, demonstrating the precise textual constructions that courts have developed. Second, the Article reviews how the narrow CFAA doctrine applies to common fact patterns involving disloyal employees and breaches of contract-like restrictions. Third, it makes a normative argument in favor of the narrow CFAA doctrine. Courts are making critical concessions to substantial societal interests—while remaining firmly grounded in legislative text and history.

Table of Contents

* Cybersecurity Fellow, Stanford University; J.D., 2013, Stanford Law School; Ph.D. candidate, 2016, Stanford University Department of Computer Science. The Author is currently serving as Chief Technologist of the Federal Communications Commission Enforcement Bureau. All views are solely the Author's own and do not reflect the position of the United States Government or the Federal Communications Commission. The Author is grateful to the many colleagues who contributed insights to this work, including Ryan Calo, Hanni Fakhoury, Laura Fong, Jennifer Granick, James Grimmelmann, Marcia Hofmann, Orin Kerr, Mark Lemley, Whitney Merrill, Paul Ohm, Kurt Opsahl, Chris Riley, Peter Swire, David Thaw, Lee Tien, George Triantis, and Barbara van Schewick. The Author is also greatly appreciative of Lindsay Klein and the editors of *The George Washington Law Review*, who provided valuable input on substance and style. This Article draws upon ideas articulated in the draft appendix of Jonathan Mayer, *Cybercrime Litigation*, 164 U. Pa. L. Rev. 1453 (2016).

December 2016 Vol. 84 No. 6

INTRODUCTION

When the Ninth Circuit handed down its en banc opinion in *United States v. Nosal*,[1] it unambiguously signaled a turning point in computer crime law. For decades, a nearly unbroken string of appellate decisions had steadily expanded the scope of the primary federal computer crime statute, the Computer Fraud and Abuse Act[2] ("CFAA").[3] Prior opinions sustained computer crime liability on a diverse array of theories, including objective misconduct,[4] deviating from agency duties,[5] and breach of contract.[6]

---

1 United States v. Nosal, 676 F.3d 854, 856–64 (9th Cir. 2012) (en banc).

2 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012).

3 Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that breach of principles of agency law is sufficient for liability).

4 *See, e.g.*, United States v. Phillips, 477 F.3d 215, 219–21 (5th Cir. 2007); United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991). *But see* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–63 (1st Cir. 2003) ("[W]e think that in general a reasonable expectations test is not the proper gloss on subsection (a)(4) and we reject it.").

5 *See, e.g.*, *Citrin*, 440 F.3d at 420–21.

6 *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001); United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

Ever since *Nosal*, however, the trend among federal courts has been to sharply constrain criminal and civil CFAA liability. Both the Second Circuit and the Fourth Circuit have expressly adopted *Nosal*'s interpretation of the CFAA, and no subsequent appellate opinion has disagreed with *Nosal*'s reasoning or holding.[7]

Nosal and similar decisions plainly convey a mood of hostility toward sweeping interpretations of computer crime law. But how, exactly, have courts narrowed the CFAA's reach? Some scholars argue that the post-*Nosal* cases have adopted a "code-based" interpretation of the CFAA, where only a circumvention of a technical security protection is legally actionable.[8] Other observers have suggested that the recent CFAA case law is simply incoherent.[9] This Article respectfully disagrees with both perspectives.

The courts have articulated a new doctrine, often dubbed the "narrow" interpretation of the CFAA.[10] The doctrine does not neatly match prior scholarly perspectives, nor does it implement a principled policy position. Rather, the narrow CFAA doctrine has emerged in a herky-jerky fashion, as the consequence of several discrete textual maneuvers.

This Article aims to make three contributions. First, it conveys the core components of the narrow CFAA doctrine and synthesizes them into a four-step analysis. Each interpretive move, it emphasizes, is firmly grounded in CFAA's statutory text.

Second, this Article matches the narrow interpretation of the CFAA against common fact patterns. It works through recurring instances of both employee misconduct and breach of contract-like re-

---

7 The Second Circuit and Fourth Circuit have followed *Nosal*'s interpretation of the CFAA. *See* United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015); United States v. Steele, 595 F. App'x 208, 210–12 (4th Cir. 2014); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205–07 (4th Cir. 2012).

8 *See, e.g.*, Orin Kerr, *The CFAA Meets the "Cannibal Cop" in the Second Circuit—and Maybe Beyond*, WASH. POST: VOLOKH CONSPIRACY (May 13, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/13/the-cfaa-meets-the-cannibal-cop-in-the-second-circuit-and-maybe-beyond/.

9 *See, e.g.*, Eric, Comment to Venkat Balasubramani, *Nosal Convicted of Computer Fraud and Abuse Act Crime Despite His Ninth Circuit Win* – US v. Nosal, TECH. & MKTG. L. BLOG (Apr. 26, 2013), http://blog.ericgoldman.org/archives/2013/04/govt_obtains_co.htm ("This case baffles me . . . . Did [the defendant] violate the Computer Fraud & Abuse Act? No, and it's not even close."); Eric, Comment to Venkat Balasubramani, *Ex-Employee's Access/Misuse of Employer Files States CFAA Claim* – Weingand v. Harland Financial, TECH. & MKTG. L. BLOG (Aug. 8, 2012), http://blog.ericgoldman.org/archives/2012/08/employees_poste.htm ("I think it's safe to declare that the CFAA jurisprudence is officially a mess.").

10 *See, e.g.*, Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615–17 (E.D. Pa. 2013) (describing the "broad" and "narrow" interpretations of CFAA).

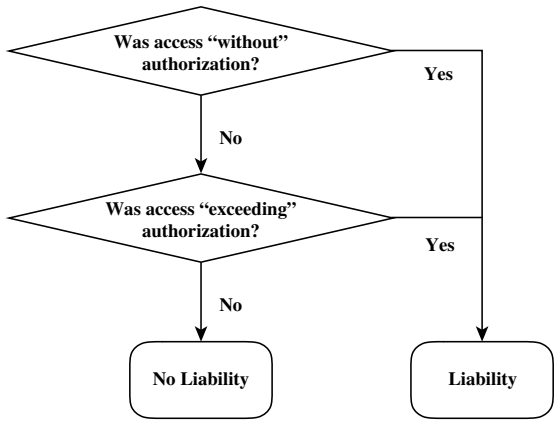
strictions. The doctrine that emerges may not be intuitive, but it is very workable.

This Article's third contribution, in its Conclusion, is a normative argument in favor of the narrow CFAA doctrine. Courts have confined themselves to the CFAA's statutory framework, as they must. But they have also managed to integrate meaningful accommodation for important policy interests. Until Congress comprehensively revisits the CFAA, the narrow interpretation of the statute functions as a vital and legitimate means of reform.

I. Constructing the "Narrow" CFAA Doctrine

The core provisions of the CFAA are predicated on two types of misconduct: access to a computer that is "without" authorization and access to a computer that "exceeds" authorization (Figure 1).[11] If a defendant commits either act, she is automatically guilty of a misdemeanor[12]—and possibly more.[13]

Figure 1. The Core Structure of Computer Fraud and Abuse Act Liability



11 18 U.S.C. § 1030(a)(1) (2012).

12 *Id.* § 1030(a)(2)(C). Although the broadest statutory offense within the CFAA includes additional elements (intent, access, obtaining information, and a protected computer), those elements are easily satisfied in computer misuse cases and are rarely a genuine issue of fact. *See* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) ("In the case of the CFAA, the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent."); *Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112 Cong. 42 (2011) (testimony of Orin S. Kerr, Professor, The George Washington University Law School).

13 *See* Hanni Fakhoury, *How the Sentencing Guidelines Work Against Defendants in CFAA Cases*, Elec. Frontier Found.: Deeplinks Blog (Apr. 9, 2013), https://www.eff.org/deeplinks/2013/03/41-months-weev-understanding-how-sentencing-guidelines-work-cfaa-cases-0.

The precise relationship between these two types of misconduct has puzzled courts, practitioners, and scholars for decades.[14] Section I.A begins by explaining how courts have adopted shifting distinctions between the concepts of access *without* authorization and access *exceeding* authorization.[15] Section I.B then reviews how courts have traced the scope of a computer system or information within a computer system—a set of critical factual determinations that are latent within CFAA case law. Sections I.C and I.D respectively address how the narrow CFAA doctrine evaluates whether access is *without* authorization or *exceeding* authorization. Finally, Section I.E reconstructs the narrow interpretation of the CFAA, synthesizing a four-step analysis to facilitate clarity and consistency in applying the new doctrine.

A. What Is the Difference Between Access "Without" Authorization and Access "Exceeding" Authorization?

The CFAA draws a textual distinction between "access[ing]" a computer system "without authorization" and "exceeding authorized access" to a computer system.[16] Courts have struggled to locate the "paper thin"[17] difference between these sources of liability, usually taking one of three approaches.[18]

First, many opinions just ignore or sidestep the distinction between *without* and *exceeding* authorization. The two theories of liability play an identical role for the CFAA's broadest offenses, leaving courts ample room to dodge.[19] In some cases, civil plaintiffs or crimi-

---

14 *See, e.g.*, *Nosal*, 676 F.3d at 858–59 (comparing statutory interpretations that reconcile "without" and "exceeding" authorization); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (describing the difference between CFAA's two types of computer abuse as "paper thin . . . but not quite invisible").

15 In the interest of doctrinal clarity, this Article adopts a stylistic convention of italicizing *without* and *exceeding* authorization.

16 18 U.S.C. § 1030(a)(2).

17 *Citrin*, 440 F.3d at 420.

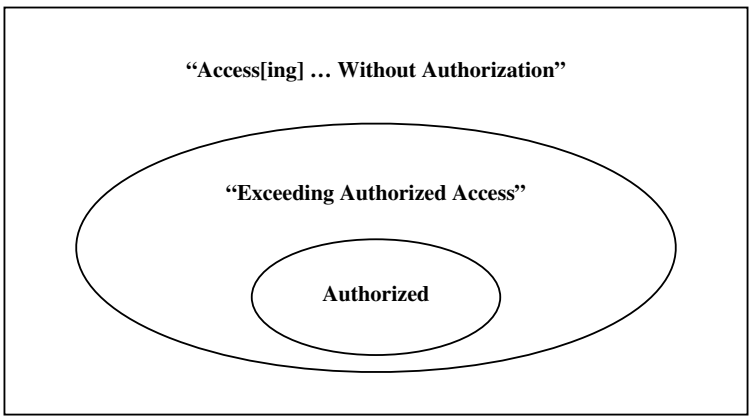
18 *See* Nicholas R. Johnson, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 572–74 (discussing the distinction between "without authorization" and "exceeding authoriz[ation]"); Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11, 14–16 (2008) (same).

19 The broadest statutory offense is 18 U.S.C. § 1030(a)(2)(C). *See supra* note 12. The CFAA's fraud offense, § 1030(a)(4), is also exceedingly broad owing to generous judicial interpretations. *See* Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, VOLOKH CONSPIRACY (Jan. 20, 2013, 1:10 PM), http://volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030/ (describing CFAA's fraud offense as "redundant"). Courts are more pressed to address the distinction when presented with an unintentional damage (18 U.S.C. § 1030(a)(5)(B)–(C)) claim,

nal prosecutors allege only one of the two theories, allowing courts to ignore the other.[20] When both theories are actually litigated and a court finds liability, it often rests its conclusion on just one of the two.[21] And when a court finds no liability, it often glosses over the two tests as a single standard.[22]

A second approach among courts is to treat the difference between *exceeding* and *without* authorization as a matter of degree (Figure 2). Both theories of liability would attach to the same underlying misconduct, such as breach of contract, deviation from agency duties, or departure from computer use norms. A defendant's minor misconduct would equate to *exceeding* authorization, while a defendant's egregious misconduct would constitute acting *without* authorization.

FIGURE 2. THE DEGREE INTERPRETATION OF *WITHOUT* AND *EXCEEDING* AUTHORIZATION



The Seventh Circuit has held, for example, that an employee who merely violates workplace policy might *exceed* authorization, but an

by contrast, since there is no "exceeding" authorization liability. *See, e.g.*, United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991) (rejecting an "exceeding" authorization defense to a "without" authorization charge).

20 *E.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 n.7 (9th Cir. 2009) ("On appeal, [plaintiff] argues *only* that [defendant] was "without authorization" to access [plaintiff's] computer and documents.") (emphasis added).

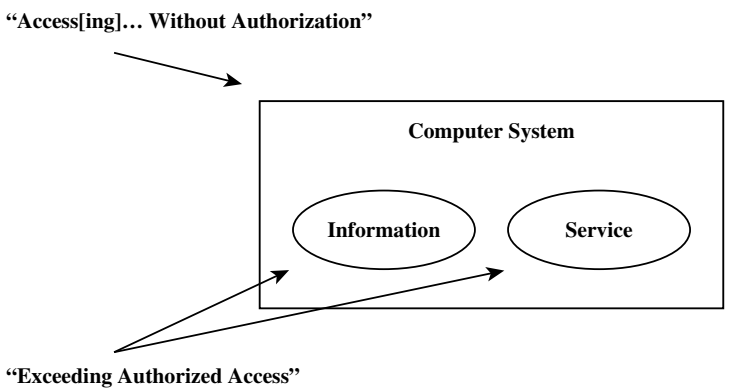
21 *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001) (finding "exceeding" authorization liability and so declining to address "without" authorization arguments).

22 *See, e.g.*, Koch Indus. v. Does, No. 2:10CV1275DAK, 2011 WL 1775765, at *7–*8 (D. Utah May 9, 2011) (analyzing "without" and "exceeding" authorization together in rejecting CFAA claims); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 384–86 (S.D.N.Y. 2010) (same).

employee who commits a "*serious* breach of loyalty" also acts *without* authorization.[23]

The narrow interpretation of the CFAA takes a third approach, treating the distinction between *without* and *exceeding* authorization as a matter of granularity (Figure 3).[24] In interpreting the CFAA, liability regarding access *without* authorization relates to the computer system as a whole; access *exceeding* authorization relates to particular information stored in the system or services offered by the system. The Sixth[25] and Ninth[26] Circuits have expressly adopted this view, as has (arguably) the Second Circuit.[27] This granular interpretation has the benefit of closely tracking the statutory definition of "exceeds authorized access," which refers to "information *in* the computer."[28]

FIGURE 3. THE GRANULARITY INTERPRETATION OF *WITHOUT* AND *EXCEEDING* AUTHORIZATION



23 Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (emphasis added); *see* Sam's Wine & Liquors, Inc. v. Hartig, No. 08 C 570, 2008 WL 4394962, at *2–*3 (N.D. Ill. Sept. 24, 2008) (reading *Citrin* as a rejection of the granularity interpretation).

24 Some courts and commenters use the terms "initial" and "subsequent" or "outsider" and "insider" to draw the same distinction. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (en banc). This Article avoids those terms because of their imprecise connotations; timing and organizational relationships are not relevant to the granularity interpretation.

25 Pulte Homes, Inc. v. Laborers' Int'l Union, 648 F.3d 295, 303–04 (6th Cir. 2011).

26 *Nosal*, 676 F.3d at 858; LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); *see* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1075–79 (9th Cir. 2016); United States v. Nosal, 828 F.3d 865, 872–80 (9th Cir. 2016).

27 United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015).

28 18 U.S.C. § 1030(e)(6) (2012) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter *information in the computer* that the accesser is not entitled so to obtain or alter.") (emphasis added).

The narrow interpretation of the CFAA substantially clarifies how the statute's two bases for liability are distinct. It also helpfully resolves that the two types of CFAA liability are mutually exclusive.[29] If a defendant *exceeds* authorized access with respect to certain information or services, then she necessarily is not *without* authorization to access the system as a whole. Similarly, if a defendant accesses a computer system *without* authorization, then she cannot *exceed* authorization with respect to specific information or services.

Treating the *without* and *exceeding* authorization theories as a matter of granularity provides resolution for tricky doctrinal questions, but it gives rise to others. For purposes of evaluating whether a defendant's conduct is authorized, what is the scope of a computer system, and what is the scope of information or services within a system? When is access to a computer system *without* authorization? When does access to information or services *exceed* authorization? The following sections review how the narrow interpretation of the CFAA responds to these questions, then reconstruct the new doctrine into a four-step analysis.

B. What Is the Factual Scope of a Computer System, or Information or Services Within a Computer System?

The granularity interpretation of the CFAA necessitates a fact-specific line drawing exercise. Both the *without* and *exceeding* theories of liability are attached to specific technology components; *without* authorization liability is attached to a computer system as a whole, while *exceeding* authorization liability is attached to particular information or services within the system. In order to properly evaluate these theories of liability, a court must necessarily sketch the boundaries of the computer system and the information and services that the defendant accessed.

The CFAA's statutory text does not give guidance in how to conduct this line drawing exercise. Are these hardware boundaries? Software boundaries? Objective boundaries, based on user perceptions or some other criterion? The answers are critical for CFAA liability, because they establish the reference points for evaluating whether a defendant's conduct was authorized.

In order to illustrate this issue for *without* authorization liability, consider the facts of *United States v. Phillips*.[30] In that case, the Fifth

---

29 The statutory basis for this mutual exclusivity is the definition of "exceeds authorized access," which includes "access[ing] a computer with authorization." 18 U.S.C. § 1030(e)(6).

30 United States v. Phillips, 477 F.3d 215 (5th Cir. 2007).

Circuit found that a University of Texas student acted *without* authorization when he guessed passwords to faculty and staff accounts on a course management website.[31] The relevant computer system for CFAA purposes was, plainly, less than the entire university information technology infrastructure.[32] But was it the specific website that the student breached? The database that powered it? The physical server that hosted the website? Each user account? The *Phillips* court applied these units interchangeably, and other courts have not seriously defined the scope of a computer system.[33]

Imagine, in a slight variant of *Phillips*, that the student had his own account on the course management website. Access to that account would unambiguously have been authorized under the CFAA; the university would have intentionally provided the account and furnished credentials. But what about when the student accessed faculty accounts? If the relevant computer system for CFAA purposes is an individual account, then the student would be acting *without* authorization. If the relevant computer system is the website, or the database, or the server, by contrast, then the access to faculty accounts would be *exceeding* authorization.

The facts of *United States v. Czubinski*[34] demonstrate how these scoping challenges can be particularly difficult when evaluating *exceeding* authorization liability. In that case, the defendant was an Internal Revenue Service ("IRS") employee who provided assistance to taxpayers.[35] As part of the defendant's role, he was permitted to retrieve confidential information about those taxpayers from an IRS database.[36] The defendant additionally accessed information on unrelated taxpayers, including a former political opponent and an ex-girlfriend; the First Circuit concluded that he had "unquestionably exceeded authorized access."[37]

But what was the information or service that the defendant exceeded authorized access to? Was it the entire IRS database? If so, that analysis would favor the defendant, because he had clear em-

---

31 *Id.* at 219–21.

32 *See id.* at 218 (describing the "TXClass" course enrollment website).

33 *See id.* (noting in the span of two sentences that the defendant accessed the "TXClass" website, the "TXClass database," "UT's main server," and UT's "unified database").

34 United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997). A very similar fact pattern was the basis for *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).

35 *See Czubinski*, 106 F.3d at 1071.

36 *See id.*

37 *Id.* at 1078.

ployer authorization (in some circumstances) to query the database.[38] Alternatively, was the relevant scope each taxpayer's record within the database? That analysis would disfavor the defendant, because he had no legitimate workplace reason to ever inspect most records. Resolving the scope of the information and services that a defendant accessed is not dispositive of CFAA liability, because there remains the question of whether the defendant exceeded authorization. But how a court sketches those factual contours is critical, because they substantially shade the authorization analysis.

The Author's view is that the scope of a computer system, stored information, or a service should not be pinned to particular hardware or software configurations. The modern trend in online service design, sometimes dubbed "cloud computing," is to distribute functionality across shared hardware and software.[39] Even a simple website could be running on a dozen different computers, using a dozen different application platforms, shared with a dozen unrelated web services. There is no longer a meaningful mapping between specific hardware, software, and each user's experience.[40]

The better approach, and the approach applied in recent lower court opinions,[41] is to evaluate the objective contours of a computer system, information store, or service. An ordinary user would perceive an entire website, for example, to constitute one system, regardless of the underlying technical design. Similarly, an ordinary user would perceive each personal account on a system to represent a distinct set of information, regardless of the technical implementation.

The discussion so far has reviewed how courts are treating the CFAA's *without* and *exceeding* authorization theories of liability as a matter of granularity, and how courts must sketch factual boundaries for applying those two theories of liability. The following sections explain how the narrow CFAA doctrine sets new standards for evaluating whether a defendant's access to a computer system is *without*

---

38 *See id.* at 1071.

39 *See* PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3 (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (describing the Software as a Service, Platform as a Service, and Infrastructure as a Service models for cloud computing).

40 *See* Ingrid Lunden, *Amazon's AWS Is Now a $7.3B Business as It Passes 1M Active Enterprise Customers*, TECHCRUNCH (Oct. 7, 2015), http://techcrunch.com/2015/10/07/amazons-aws-is-now-a-7-3b-business-as-it-passes-1m-active-enterprise-customers/ (describing how Amazon's shared cloud platform has over one million active customers).

41 *See infra* Sections I.C and I.D.

authorization and whether a defendant's access to information or services within a system *exceeds* authorization.

C. When Is Access "Without" Authorization?

Until recently, courts struggled with the scope of access *without* authorization. Some courts recognized liability for objective misconduct,[42] violating principles of agency law,[43] and other expansive constructions of the provision.

No longer. Under the narrow interpretation of the CFAA, *without* authorization liability is a sharply constrained construct, for two reasons.

First, *without* authorization liability operates at the level of a computer system as a whole. As explained above, courts look to whether a defendant had authorization to access the system, not particular information or services within the system.[44] The pragmatic result of this interpretive maneuver is a heightened burden for prosecutors and plaintiffs, because they cannot subdivide a computer system's components to develop multiple plausible zones of unauthorized access.

Second, recent constructions of *without* authorization liability have placed textual emphasis on the absolute quality of the term "without." Rather than assessing whether a *particular* instance of computer system access was unauthorized, courts evaluate whether the defendant was *entirely* without authorization to access the computer system. Put differently, the inquiry is whether a defendant had authorized access to *any* information or service within the computer system. If the defendant did, then she is not susceptible to *without* authorization liability.

The facts of *Pulte Homes v. Laborers International Union*[45] illustrate the new doctrine's operation.[46] In that case, a union launched a spam email campaign during the course of a labor dispute.[47] The employer sued, alleging that the union had accessed its email system *without* authorization.[48] A Sixth Circuit panel unanimously disagreed, reasoning that the email system was open to the public—including the

---

42 *See, e.g.*, United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991).

43 *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

44 *See supra* Section I.B.

45 Pulte Homes, Inc. v. Laborers' Int'l Union, 648 F.3d 295 (6th Cir. 2011).

46 *Id.* at 303–05; *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

47 *Pulte Homes*, 648 F.3d at 298.

48 *Id.* at 301.

defendant union.[49] That meant the union had *some* authorized access and therefore could not be liable under the CFAA's *without* authorization provisions.[50]

A pair of recent Ninth Circuit opinions function as additional signposts for *without* authorization liability. In *Facebook v. Power Ventures*, a panel sustained Facebook's *without* authorization claim against a social network news aggregator.[51] The court reasoned that, so long as the defendant business had plausible authorization to access Facebook's computer systems (by virtue of user consent), it was not subject to *without* authorization liability.[52] But once Facebook sent a cease-and-desist letter, expressly revoking all authorization, the defendant acted *without* authorization in continuing to access Facebook computer systems.[53]

In an opinion handed down the same month, *United States v. Nosal* (returned after a new indictment and trial), a panel of the Ninth Circuit considered the scope of CFAA liability for departed employees.[54] The court concluded that once an employee leaves a business and has his or her login credentials deactivated, all authorization to access the business's internal computer systems is terminated.[55] Borrowing a current employee's login credentials and accessing an internal system, consequently, constitutes access *without* authorization.[56]

Two key principles emerge from *Pulte Homes*, *Facebook*, and *Nosal*. First, there is a sliding scale latent within the narrow CFAA doctrine. Courts will sustain *without* authorization liability where the defendant's permission is scoped by written guidance or agency duties, rather than technical security barriers. But in cases involving unsophisticated misconduct, courts will demand an extraordinary degree of clarity about the defendant's lack of authorization. A mere breach of terms of service or a faithless act will not suffice to establish liability. Rather, a defendant must receive a letter that *entirely* revokes authori-

---

49 *Id.* at 304.

50 *Id.*

51 Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1075–79 (9th Cir. 2016).

52 *Id.* at 1076–77.

53 *Id.*

54 United States v. Nosal, 828 F.3d 865, 872–80 (9th Cir. 2016); *see* United States v. Steele, 595 F. App'x 208, 210–11 (4th Cir. 2014) (addressing a similar fact pattern and arriving at the same conclusion).

55 *Nosal*, 828 F.3d at 874–76.

56 *Id.* at 878.

zation, or must be terminated from employment such that he or she *entirely* loses authorized access.[57]

The second key principle that emerges for CFAA's *without* authorization branch is that liability will rarely extend to mass market online services. A defendant will almost always have some authorized access to Google's search engine, Facebook's social network, and similar offerings to the public at large. In the narrow interpretation of the CFAA, *without* authorization liability is primarily applicable to private computer systems dedicated to an organization's internal use or a person's individual use.

D. When Is Access "Exceeding" Authorization?

For decades, the CFAA's *exceeding* authorization component also vexed the federal judiciary. As with the *without* authorization component, courts countenanced a broad range of liability theories, including deviations from agency duties[58] and breach of contract.[59] Scholars, meanwhile, coalesced around a theory that liability should turn on circumvention of technical protections.[60] No court has

---

57 *See Facebook*, 828 F.3d at 1078 (distinguishing between website terms of service and a cease-and-desist letter); *Nosal*, 828 F.3d at 874–76 (distinguishing between current and former employees).

58 *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000).

59 *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001); United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

60 Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1640, 1644–45, 1648–49 (2003); *see* Johnson, *supra* note 18, at 570 (explaining the code-based perspective); Sarah Boyer, Note, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661, 677 (2009) (same); Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 244–45 (2010) (same); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 825–27 (2009) (same); Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1560–61 (2012) (same); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1379–82 (2011) (same). The notion of a code-based scope to computer crime liability appears to have been proposed at least as early as 1996, when a California court interpreted the state computer crime statute in that manner. People v. Lawton, 56 Cal. Rptr. 2d 521, 522 (Cal. App. Dep't Super. Ct. 1996) (holding a state computer crime offense "can be committed by use of a public access terminal to bypass security and penetrate levels of software not open to the public"). A similar approach appears in the Digital Millennium Copyright Act of 1998, which prohibits circumvention of "a technological measure that effectively controls access to a [copyrighted] work." 17 U.S.C. § 1201 (2012).

adopted this "code-based" test for CFAA liability, however, and at least four opinions have recently rejected it.[61]

The narrow interpretation of the CFAA charts a different course. The recent trend in the federal judiciary has been to draw a distinction between *access* to information and *use* of that information. In this new construction, liability for *exceeding* authorization only reaches conduct where information *access* is unauthorized. A restriction on information *use*, by contrast, is not enforceable.

The modern doctrinal line traces its intellectual roots to *International Association of Machinists & Aerospace Workers v. Werner-Masuda*[62] and *Lockheed Martin v. Speed*,[63] a pair of mid-2000s district court opinions that sought to limit liability under the CFAA's *exceeding* authorization theory.[64] The narrow interpretation percolated among lower courts, and finally won widespread adoption with the Ninth Circuit's 2012 en banc opinion in *United States v. Nosal*.[65] Both

---

61 *Nosal*, 828 F.3d at 878 ("Nosal [argues] that the CFAA only criminalizes access where the party circumvents a technological access barrier. Not only is such a requirement missing from the statutory language, but it would make little sense because some § 1030 offenses do not require access to a computer at all."); NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816, 831 (N.D. Cal. 2014) ("[A] nontechnological barrier can revoke authorization."); United States v. Nosal (*Nosal II*), 930 F. Supp. 2d 1051, 1060–61 (N.D. Cal. 2013) ("The [*Nosal*] court did not address limits on liability under the CFAA based on the *manner* in which access is limited, whether by technological barrier or otherwise."); Weingand v. Harland Fin. Sols., Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) ("[A]lthough *Nosal* clearly precluded applying the CFAA to violating restrictions on *use*, it did not preclude applying the CFAA to rules regarding *access*."); *see* Synopsys, Inc. v. ATopTech, Inc., No. C 13-cv-02965 SC, 2013 WL 5770542, at *10 (N.D. Cal. Oct. 24, 2013) (summarizing the state of the law); Recent Case, *Statutory Interpretation — Computer Fraud and Abuse Act — Ninth Circuit Holds that Employees' Unauthorized Use of Accessible Information Did Not Violate the CFAA* — United States v. Nosal, *676 F.3d 854 (9th Cir. 2012) (en banc)*, 126 HARV. L. REV. 1454, 1461 n.61 (2013) (explaining that the Ninth Circuit did not adopt the code-based view). *But see* Kerr, *supra* note 8 (arguing that *Nosal* adopted the code-based interpretation of *exceeding* authorization liability).

62 Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005).

63 Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).

64 *Werner-Masuda*, 390 F. Supp. 2d at 499 ("[T]he CFAA . . . do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access."); *Speed*, 2006 WL 2683058, at *5 ("The gist of [Plaintiff's] complaint is aimed not so much at [Defendants'] improper access of . . . information, but rather at [Defendants'] actions subsequent to their accessing the information. As much as [Plaintiff] might wish it to be so, § 1030(a)(4) does not reach the actions alleged . . . .").

65 *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) ("[W]e continue to follow in the path blazed by . . . the growing number of courts that have reached the same conclusion [to narrowly construe CFAA]."). Lower courts have consistently read the *Nosal* opinion to stand for an access vs. use test, not a code-based test. *See, e.g.*, *Nosal II*, 930 F. Supp. 2d at 1061 ("The court did not address limits on liability under the CFAA based on the *manner*

the Second Circuit[66] and Fourth Circuit[67] expressly followed *Nosal*, as have a number of lower courts.

The critical textual move for this construction resides in the statutory definition of "exceeds authorized access."[68] In order to satisfy that provision, a defendant must "obtain or alter" information without authorization.[69] In the view of the Ninth Circuit en banc majority, and other courts that follow the same school of thought, a condition on *obtaining* information is necessarily a condition on *accessing* that information.[70]

---

in which access is limited, whether by technological barrier or otherwise."); Craigslist Inc. v. 3Taps Inc. (*Craigslist I*), 964 F. Supp. 2d 1178, 1180–81, 1183–85, 1187 (N.D. Cal. 2013) (allowing CFAA claim where plaintiff expressly and completely revoked defendant's authorization by letter); *Weingand*, 2012 WL 2327660, at *3 (allowing CFAA claim where plaintiff arguably delineated defendant's authorization by verbal statement); *see* Recent Case, *supra* note 61, at 146 n.61 (explaining that the Ninth Circuit did not adopt the code-based view). A number of commenters have critiqued this interpretation of *Nosal*, it should be noted, as insufficiently vindicating the vagueness and lenity underpinnings of the en banc opinion. *See, e.g.*, Justin P. Webb, Nosal *on Remand-Another Reading of CFAA's "Exceeds Authorized Access"; Court Denies Motion to Dismiss*, CYBERCRIME REV. (Mar. 13, 2013), http://www.cybercrimereview.com/2013/03/nosal-on-remand-another-reading-of.html.

66 United States v. Valle, 807 F.3d 508, 508 (2d Cir. 2015).

67 WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012) ("[W]e agree with [the *Nosal*] view."). There is a possible reading of *WEC Carolina* that goes "a step further" than *Nosal*. *Id.* In the alternative reading, the Fourth Circuit held that if *any* form of "access" is authorized, then CFAA liability is unavailable. *Id.* at 206. In that case, an employer alleged former employees had downloaded confidential materials to their personal devices in violation of its access policies. *Id.* at 206–07. The Fourth Circuit began and ended its analysis with the employees having *some* authorized means of access to the materials. *Id.* at 206. It was irrelevant whether the employees actually used that authorized avenue, or accessed the documents in a different way. *See id.* Put differently, the Fourth Circuit suggested it would have found liability only if the employees had *no* authorized access to the materials *under any circumstances*. *Id.* Two hypotheticals offered in *WEC Carolina* help distinguish the some-none test from the access-use test. Imagine an employee is authorized to access information on his workstation screen, but is prohibited by policy from accessing the information with software that copies it to a thumb drive. *Id.* at 205. Under the access-use test, the employee could be liable—the anti-copying policy could be an enforceable restriction on a means of access. Under the some-none test, though, the employee is not liable—he had *some* authorized access to the information. There was a set of facts under which the employee could access the information with authorization, namely, on his workstation screen. Alternatively, assume an employee has valid login credentials for a workplace computer system. *Id.* The employee nevertheless borrows a colleague's credentials to access the system. *Id.* Under the access-use test, the employee might be liable—the password wall could be an enforceable access restriction. Under the some-none test, the employee is not liable—she had *some* authorized access to the system, by using her own credentials.

68 18 U.S.C. § 1030(e)(6) (2012).

69 *Id.*

70 *See, e.g.*, *Nosal*, 676 F.3d at 858.

The access-use distinction is plainly an attempt to narrow the CFAA's scope, in recognition of the policy risks posed by overbroad computer crime liability and skepticism that Congress intended such expansive causes of action. This narrow interpretation of *exceeding* authorization also addresses due process concerns that the CFAA's text is too ambiguous (under void-for-vagueness doctrine)[71] or susceptible to equally plausible interpretations (under the rule of lenity).[72] In common fact patterns, discussed further in Part II, the access-use test leads to consistent and defensible results.

That is not to say that the access-use dichotomy is a paragon of doctrinal clarity. A review of lower court access-use delineations, including every CFAA opinion in the Ninth Circuit subsequent to *Nosal*, reveals a set of recurring challenges in applying the new doctrine.

First, how should a court evaluate whether a defendant's access to information is authorized? Opinions have variously emphasized the defendant's employment status and job duties,[73] contract-like conduct between the parties,[74] the defendant's technical account permissions,[75] and the extent to which the defendant's conduct resembles

---

71 *See* United States v. Drew, 259 F.R.D. 449, 462–67 (C.D. Cal. 2009) (holding that an interpretation of CFAA that reaches violation of a website terms of use is constitutionally void for vagueness).

72 *See* United States v. Valle, 807 F.3d 508, 526–28 (2d Cir. 2015) (applying the rule of lenity); *Nosal*, 676 F.3d at 863 (same); *WEC Carolina*, 687 F.3d at 205–06 (same).

73 United States v. Steele, 595 F. App'x 208, 210–11 (4th Cir. 2014) (allowing CFAA claim where former employee had valid login credentials, but employment was completely terminated); Integral Dev. Corp. v. Tolat, No. C 12-06575 JSW, 2013 WL 5781581, at *4 (N.D. Cal. Oct. 25, 2013) (rejecting CFAA claim when "at the time of the alleged acquisition of [plaintiff employer's] materials, [defendant] was working for [plaintiff] and had access to virtually all of [plaintiff's] trade secret information and confidential and proprietary intellectual property"); Hat World, Inc. v. Kelly, No. CIV S-12-01591 LKK/EFB, 2012 WL 3283486, at *5 (E.D. Cal. Aug. 10, 2012) (allowing CFAA claim when former employee accessed systems after resignation); Weingand v. Harland Fin. Sols., Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (allowing CFAA claim when former employee accessed systems after termination); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 936 (W.D. Tenn. 2008) ("Because [defendant] had permission to access the information in question and doing so was within the scope of his duties, it cannot be successfully argued that his access constituted a trespass.").

74 *Craigslist I*, 964 F. Supp. 2d 1178, 1183 (N.D. Cal. 2013) (allowing CFAA claim where plaintiff expressly and completely revoked defendant's authorization by letter); *Weingand*, 2012 WL 2327660, at *3 (allowing CFAA claim where plaintiff arguably delineated defendant's authorization by verbal statement); Koch Indus. v. Does, No. 2:10CV1275DAK, 2011 WL 1775765, at *7–*8 (D. Utah May 9, 2011) (rejecting CFAA claim where manifestation of assent to website's terms of use was insufficient for contract formation); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) (same).

75 Oracle Am., Inc. v. TERiX Comput. Co., No. 5:13-cv-03385-PSG, 2014 WL 31344, at *6–*7 (N.D. Cal. Jan. 3, 2014) (allowing CFAA claim where company with no issued credentials

"hacking" in the abstract.[76] Remarkably, some courts have even held that principles of agency law[77] or employer computer system policies[78]

---

to paid service used shared credentials to access the service); Spam Arrest, LLC v. Replacements, Ltd., No. C12-481RAJ, 2013 WL 4675919, at *20 (W.D. Wash. Aug. 29, 2013) (holding that because plaintiff email provider's servers accept email from anyone, they authorize "*everyone* . . . to send email to its customers"); Farmers Ins. Exch. v. Steele Ins. Agency, Inc., No. 2:13-cv-00784-MCE-DAD, 2013 WL 3872950, at *19–*20 (E.D. Cal. July 25, 2013) (holding employees who had credentials to access a database were authorized, but an employee who borrowed credentials was not authorized); Advanced Micro Devices, Inc. v. Feldstein, 951 F. Supp. 2d 212, 219 (D. Mass. 2013) (noting "valid login credentials" in holding access was authorized); *Nosal II*, 930 F. Supp. 2d 1051, 1060–62 (N.D. Cal. 2013) (sustaining a CFAA charge for using a voluntarily shared password); Oracle Am., Inc. v. Serv. Key, LLC (*Oracle Am. I*), No. C 12-00790 SBA, 2012 WL 6019580, at *5 (N.D. Cal. Dec. 3, 2012) ("This conduct—using legitimate access credentials to access websites and then distributing information obtained from such access to third parties who have no right to receive such information—is precisely the type of conduct that *Nosal* held was beyond the scope of the CFAA."); Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n, No. 10-cv-120-SM, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012) (holding employees who had credentials to access certain data on employer's servers were authorized, but an employee who borrowed credentials was not authorized); United States v. Zhang, No. CR-05-00812 RMW, 2012 WL 1932843, at *5 (N.D. Cal. May 29, 2012) ("[Employee] had 'authorized access' to [employer's system] when he downloaded the information from [employer's system] because he had active log-in credentials at that time."); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) ("[Defendants] concededly were granted unfettered access to [plaintiff's] computer system and information residing on it. In consequence, [plaintiff] has failed to adduce any evidence that they accessed its computer system without authorization or exceeded their authorized access in violation of the CFAA."); ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 610 (M.D. Tenn. 2010) ("The Verified Complaint expressly alleges that [defendant] had access, including remote access, to [plaintiff's] computer system and to [its] source code . . . .").

76 *See* Matot v. CH, 975 F. Supp. 2d 1191, 1193 n.5 (D. Or. 2013); Xcedex, Inc. v. VMware, Inc., No. 10-3589 (PJS/JJK), 2011 WL 2600688, at *4–*5 (D. Minn. June 8, 2011) (looking for "breaking and entering" conduct in assessing the scope of authorization).

77 NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1059 (S.D. Iowa 2009) ("The Court notes that the broad view does not focus on an employee's later misuse of information but rather focuses on an employee's initial *access* of the employer's computer with the intent to either obtain information or defraud the employer, thereby obtaining something of value.").

78 United States v. Valle, 301 F.R.D. 53, 115 (S.D.N.Y. 2014), *rev'd*, 807 F.3d 508 (2d Cir. 2015) ("Unlike the disloyal employees [in *Nosal* and similar cases], [Defendant] did not have unrestricted access to the . . . databases—he was not free to access the information contained in these databases under all circumstances. Instead, his access to the . . . databases was limited to circumstances in which he had a valid . . . purpose for querying the system."); Ruling on Def. Motion to Dismiss Specifications 13 and 14 of Charge II for Failure to State an Offense at 9, United States v. Manning, No. 9504 (U.S. Army 1st Jud. Cir., June 8, 2012), https://s3.amazonaws.com/s3.documentcloud.org/documents/676432/20120608-ae-139-ruling-defense-motion-to-dismiss.pdf ("Applying the Rule of Lenity, the Court shall adopt the narrow [*Nosal*] meaning of 'exceeds authorized access' under the CFAA and instruct the fact finder that the term 'exceeds authorized access' is limited to violations of restrictions on *access* to information, and not restrictions on its 'use.'"); Ruling on Def. Renewed Motion to Dismiss Specifications 13 and 14 of Charge II for Failure to State an Offense at 2, *Manning*, No. 9504, https://s3.amazonaws.com/s3.documentcloud.org/documents/712692/20120718-ae-218-court-ruling-defense-renewed.pdf ("Restrictions on access to classified information can arise from a variety of sources, to include

could be recast as enforceable "access" restrictions. Although those cases are undoubtedly outliers, they exemplify the problem: recognizing a distinction between information "access" and information "use" does not clarify how to evaluate the scope of authorized information "access." That analysis quickly devolves back into grasping for substantive standards, like agency principles and contract law.

A second point of doctrinal difficulty is distinguishing restrictions on information access from restrictions on information use.[79] The issue is particularly acute for contract-like documents, where a formalistic approach would allow trivial circumvention through artful drafting: a plaintiff need only replace "*X* may not *use* this information to do *Y*" with "*X* may not *access* this information for the purpose of using it to do *Y*."[80] At least three courts have looked beyond the plain text of policy documents and determined purported *access* restrictions to constitute *use* restrictions, though offering scant clarity on the distinction.[81] Courts have, however, enforced a policy document that revoked access authorization for all purposes, as well as a verbal statement that allegedly delineated the entire scope of permissible access.[82]

---

regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive.").

79 The Author's synthesis of recent case law is that courts are applying a sliding scale to distinguish information "access" and information "use," much like the test for whether a defendant's access is *without* authorization. Where a contract-like statement is explicit and comprehensive, and a defendant's access to a computer system is not routine, courts appear more likely to find an enforceable "access" restriction; where a policy statement is buried and nuanced (like a website's terms of use), and a defendant's access to the system is commonplace (like an ordinary web user), courts appear more likely to find an unenforceable "use" restriction.

80 *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 620 n.14 (E.D. Pa. 2013) (noting the issue); Recent Case, *supra* note 61, at 1460 (same).

81 Craigslist Inc. v. 3Taps Inc. (*Craigslist II*), 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) ("Although the TOU include a section titled 'Unauthorized Access and Activities,' parts of which are framed in terms of 'access,' these restrictions depend entirely on the accessor's *purpose* . . . . The TOU do not govern *who* may access information, *what* information may be accessed, or the *methods* by which information may be accessed."); Synopsys, Inc. v. ATopTech, Inc., No. C 13-cv-02965 SC, 2013 WL 5770542, at *9–*10 (N.D. Cal. Oct. 24, 2013); Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n, No. 10-cv-120-SM, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012) ("[S]imply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction. Here, the [employer's] policy . . . is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access."); *see Craigslist I*, 964 F. Supp. 2d 1178, 1185 (N.D. Cal. 2013) ("It is true that 'simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction.' Thus, purported 'de-authorizations' buried in a website's terms of service may turn out to be use restrictions in disguise . . . ." (citation omitted)).

82 *Craigslist I*, 964 F. Supp. 2d at 1183 (allowing CFAA claim where plaintiff expressly and

Another challenge for distinguishing *access* from *use* is the ability to fashion certain uses into technical access terms. For example, if a website wants to prevent competitors from using its information in aggregate, instead of writing "you may not use the information from this website in bulk," it could write "you may not access the information on this website with an automated web crawler" or "you may only access the information on this website with an ordinary web browser." Similarly, if an employer wishes to protect confidential information, instead of drafting "you may not use confidential information except for your work," it could write "you may not access confidential information from a home computer" or "you may not access confidential information with copying software." Courts have considered policies against modifying,[83] copying,[84] and printing data,[85] and found all to constitute unenforceable *use* limitations rather than enforceable *access* restrictions.

These sources of doctrinal ambiguity and judicial malleability are unlikely to be resolved soon. They inherently turn on case-specific factual determinations and are not susceptible to easy bright-line resolution. But at least this much is certain about the narrow CFAA doctrine: it introduces a sliding scale for *exceeding* authorization liability. When a defendant engages in egregious and technically sophisticated misconduct, a court will generally sustain liability. But when a CFAA claim essentially sounds in agency or contract law, a court will require unusually unambiguous notice that access was prohibited.

---

completely revoked defendant's authorization by letter); Weingand v. Harland Fin. Sols., Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (allowing CFAA claim where business arguably delineated totality of former employee's authorization by verbal statement).

83 Enki Corp. v. Freedman, No. 5:13-cv-02201-PSG, 2014 WL 261798, at *3 (N.D. Cal. Jan. 23, 2014) ("[Plaintiff] instead hangs its hat on its repeated refusals to grant [defendants] the authority to write or edit [specific files]. That argument, however, speaks to misuse of the [files], not unauthorized access, which under *Nosal* does not run afoul of the CFAA."). Modifying information could arguably fall outside the scope of *Nosal* and similar cases. Those opinions emphasize the statutory definition of "exceeds authorized access," which covers "obtain[ing]" (i.e., accessing) information. 18 U.S.C. § 1030(e)(6) (2012). But the same provision also expressly covers "*alter[ing]*" information. *Id.* (emphasis added).

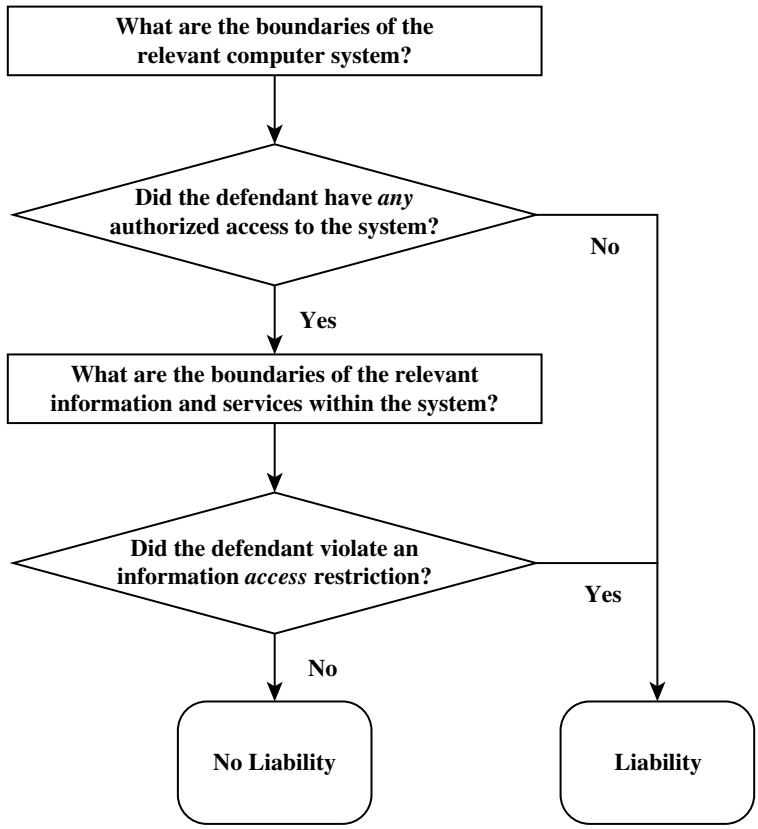
84 *Wentworth-Douglass Hosp.*, 2012 WL 2522963, at *4 ("Here, the [employer's] policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access.").

85 Givaudan Fragrances Corp. v. Krivda, No. 08-cv-4409 (PGS), 2013 WL 5411475, at *2 (D.N.J. Sept. 26, 2013) ("[Plaintiff's] proposition that [defendant] could not 'review and print' does not fall within the definition of exceeds authorized access.").

E. Reconstructing the Narrow Interpretation of the CFAA

The above Sections reviewed the essential components of the narrow CFAA doctrine. Building from those components, it is possible to reconstruct a coherent, four-step analysis that facilitates doctrinal clarity and application to new fact patterns. Figure 4 provides a diagram of the narrow CFAA doctrine's four-step analysis.

FIGURE 4. ANALYTICAL STEPS IN THE NARROW CFAA DOCTRINE



The first pair of questions resolves whether a defendant violated the CFAA by accessing a computer system *without* authorization. Step one, from Section I.B, is evaluating the boundaries of the relevant computer system. In other words, what was the computer system that the defendant accessed? Step two, from Section I.C, is determining whether the defendant acted *without* authorization to access that computer system. Was the defendant prohibited from accessing that computer system under *all* circumstances? If the answer is affirmative, the defendant is liable for access *without* authorization. If not, analysis proceeds to the next steps.

The second pair of questions address the CFAA's *exceeding* authorization theory. Step three, from Section I.B, requires scoping the information and services within the computer system that the defendant accessed. The last step, from Section I.D, asks whether the defendant violated an *access* restriction (rather than a *use* restriction) on the information and services at issue. If the answer is yes, the defendant is liable for access *exceeding* authorization. If the answer is no, the defendant has not violated the CFAA's core provisions.

This four-step test is, admittedly, somewhat cumbersome. But it provides a clear framework for evaluating potential CFAA liability, and it produces consistent results for recurring fact patterns under the statute. The following Part demonstrates how to apply the four-step analysis, working through a set of common fact patterns.

II. Applying the Narrow Interpretation of the CFAA

Most civil cases under the CFAA, and a plurality of criminal cases, arise from disloyal employees.[86] Sections II.A and B illustrate the mechanics of the four-step analysis by applying it to a pair of recurring workplace disputes: information misappropriation by current employees and information misappropriation by former employees. Sections II.C and D then evaluate potential liability for a pair of fact patterns that, although less common in litigation, have vexed courts and commenters: sharing passwords to a private database and breaching terms of service on a public website.

A. Information Misappropriation by Current Employees

In the prototypical civil CFAA case, a current employee decides to depart for a competing firm.[87] On the way out, the employee duplicates confidential commercial information from a work database that will benefit her prospective employer.[88] The former employer sues under the CFAA's cause of action for misappropriating information.[89]

The plurality criminal CFAA case is closely related. A current government employee has routine access to a database of sensitive personal information. The employee takes advantage of that access

---

86 *See* Jonathan Mayer, *Cybercrime Litigation*, U. Pa. L. Rev. (forthcoming 2016).

87 *Id.*

88 This example involves access to a database so that the civil and criminal fact patterns run parallel. Many civil cases of this type arise from information misappropriation from a workstation or file server, rather than a database. Those factual distinctions in the type of computer system do not alter the outcome under the narrow CFAA doctrine.

89 18 U.S.C. § 1030(a)(2)(C) (2012).

for personal gain (e.g., researching a political opponent) or out of personal interest (e.g., researching a former paramour). The matter is referred to the local United States Attorney's Office, which elects to prosecute for misappropriating information.[90]

The narrow interpretation of the CFAA provides an unambiguous resolution for these fact patterns. The current employee is not liable under the CFAA, because she has neither accessed a computer system *without* authorization nor *exceeded* authorized access to information or services within a computer system. Applying the four-step analysis[91] illustrates why the narrow interpretation of the CFAA compels this outcome.

The first two steps are easy. The relevant scope of the computer system is the database that the employee accessed because it presents as an objectively discrete set of records and services. Plainly, the employee had *some* authorized access to the system because her employer provided credentials and intended that she routinely use the system for workplace responsibilities. The employee cannot, therefore, be liable for access *without* authorization.

The next two steps are subtler. The relevant scope of the information that the employee accessed should be measured by specific records within the database because they present as objectively independent units of data. The employee plainly engaged in unsavory conduct in connection with those specific records—she engaged in subjectively and objectively undesirable activities from the employer's perspective, violated her duties under agency law, and likely breached the employer's computer-use policy.

But the critical fourth step is not whether the employee's conduct with respect to specific information was objectionable. The key question is, did the employer impose a cognizable restriction on the employee's *access* to that information? Or did the employer's restrictions solely attach to the employee's *use* of that information?

Under the narrow interpretation of the CFAA, a *purposive* restriction on information is fundamentally a *use* restriction. Even if the employee violated objective standards of conduct, agency duties, and a general employer computer policy[92] while misappropriating

90 *Id.* When a case involves financial misconduct, prosecutors often charge CFAA's fraud offense, 18 U.S.C. § 1030(a)(4).

91 *See supra* Figure 4.

92 As noted in Section I.D above, an extraordinarily explicit computer policy (e.g., "you are forbidden from looking at record *X* in the database under all circumstances") could potentially be actionable. In practice, computer policies are much more general.

database records, those are all restrictions on information use, not information access. The employee is not liable for *exceeding* authorized access because she has not breached a restriction on information access.

B. Information Misappropriation by Former Employees

In many civil CFAA cases, timing matters. The factual configuration of the employer-employee dispute is the same, but the employee misappropriates confidential commercial information from a database *after* they have departed their position.[93] Usually these cases arise because the employer neglected to disable the former employee's database credentials. The narrow interpretation of the CFAA compels a different outcome for these fact patterns; a former employee is usually liable for misappropriating information.

The first two steps of the four-part analysis are often dispositive. The relevant computer system remains the employer's database. But the former employee now has *no* authorized access to that database. After the employment relationship ends, there is *no scenario* in which the former employee retains legitimate access to her former employer's internal computer systems. The sole reason that access remains feasible is a technical oversight by the former employer. A former employee who misappropriates information, therefore, will generally be liable under the CFAA's access *without* authorization theory.

The entire four-part analysis can become necessary in a particular version of the former employee fact pattern. Sometimes, as a gesture of goodwill, a business will allow a former employee to recover personal information from a workplace computer system.[94] The former employee takes advantage of her temporary access to copy not just personal data, but also confidential business information. In these cases, the former employee will still be liable under the CFAA. Whether the employee is liable for access *without* authorization or access *exceeding* authorization, though, will depend on specific facts.

Suppose that a former employee is temporarily permitted to retrieve files from her office desktop computer. She discovers that a confidential database remains accessible from her old office computer, and she downloads records from that database. The relevant scope of

---

93 *See supra* note 73 and accompanying text (collecting cases where employment status was relevant to the access-use dichotomy).

94 *See, e.g.*, Weingand v. Harland Fin. Sols., Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012).

the computer system remains the database, and the former employee has no authorized access to that database. The former employee is liable for accessing the database *without* authorization.

What if the former employee's personal information is commingled in the database, though, and the former employer permits retrieving that information from the database? In this variant of the fact pattern, the relevant computer system is still the database. The former employee has *some* authorized access to the database, for purposes of retrieving her personal data. She will not be liable for access *without* authorization.

The remaining two steps nevertheless result in liability. The relevant scope of information remains specific records within the database. Plainly, the former employee is authorized to access her personal records within the database. But she is explicitly forbidden from accessing confidential business records within the database, including the records that she pilfered. The restriction that the former employee violated is an *access* restriction, rather than a *use* restriction, because she is forbidden from accessing the business's own records *for any purpose*. The former employee is liable for access *exceeding* authorization.

C. Using a Shared Password to a Private Database

A minority of CFAA cases relate to password sharing.[95] In these scenarios, a legitimate accountholder possesses valid login credentials for a private database, but she shares those credentials to an unrelated third party without permission.[96] The third party then uses those credentials to access the database and retrieve records stored inside.

Under the narrow interpretation of the CFAA, using an impermissibly shared password to a private database gives rise to liability. (Sharing a password also results in secondary criminal liability.[97]) The specific theory of liability, though, is fact dependent.

---

95 *E.g.*, Farmers Ins. Exch. v. Steele Ins. Agency, Inc., No. 2:13-cv-00784-MCE-DAD, 2013 WL 3872950, at *19–*20 (E.D. Cal. July 25, 2013) (holding employees who had credentials to access a database were authorized, but an employee who borrowed credentials was not authorized). *See* Mayer, *supra* note 86.

96 This Section reuses the example of a database to promote analytical clarity. The same reasoning would apply to password sharing for other types of private computer systems and information and services within those systems.

97 A user who shares their password can be liable as an accomplice to the CFAA offense or as a member of a CFAA conspiracy. *See Nosal II*, 930 F. Supp. 2d 1051, 1061 (N.D. Cal. 2013). The user may also be liable, both civilly and criminally, under CFAA's unusual password sharing offense. 18 U.S.C. § 1030(a)(6); *see* Oracle Am., Inc. v. TERiX Comput. Co., No. 5:13-cv-03385-PSG, 2014 WL 31344, at *6–*7 (N.D. Cal. Jan. 3, 2014).

The first two steps of the four-part analysis are dispositive, if the third party has no credentials of her own for accessing the database. The relevant computer system is, once again, the database as a whole. The third party possesses no authorized access to the database *under any circumstances*. Her access to the database is, therefore, *without* authorization.

But suppose that the third party does have credentials for the database, albeit credentials that provide access to only a limited subset of records. In these scenarios, the latter two steps in the four-part analysis are essential. The relevant scope for information is each database record because each record constitutes an objectively distinct unit of data. The third party is not permitted to access certain records *for any purpose*; the database owner has clearly delineated which records the third party may access by means of technical protections. As a consequence, the third party is liable for access *exceeding* authorization when she retrieves records using borrowed credentials that are outside of the zone of access permitted by her own credentials.[98]

The analysis above, it is important to note, presumes a private computer system. Commenters have expressed substantial concern about liability for password sharing involving computer systems that are open to the public (e.g., Gmail), or are open to a large population of paying subscribers (e.g., Netflix); millions of consumers routinely swap passwords for these popular online services.[99] How the narrow interpretation of the CFAA will apply to these scenarios remains ambiguous; courts could follow the same liability analysis as for private systems, or they could acknowledge contextual differences for public and quasi-public systems that result in a different outcome.[100]

---

98 The third party may also be liable for accessing webpages within the zone permitted by her credentials, if she accesses those webpages with the shared credentials rather than her own credentials. The narrow interpretation of CFAA has not, so far, clearly addressed those facts. In one reading, the narrow doctrine disallows *exceeding* authorization liability if a defendant has *any* authorized access to particular information or services. In another reading, the narrow doctrine permits enforcement of access restrictions on information—including account credentials—regardless of whether the defendant has *other* avenues of authorized access to the information. For further discussion of this issue, see *supra* note 67 and accompanying text.

99 *See* United States v. Nosal, 828 F.3d 865, 888 (9th Cir. 2016) (Reinhardt, J., dissenting).

100 Courts could, for example, note that the norms surrounding credential sharing to public services are laxer, that many popular services tolerate or even encourage credential sharing, or that a personal account on a public system is more plausibly delegable than a business account on a private system. *See Nosal*, 828 F.3d at 877–78 (suggesting that password sharing for a private system "bears little resemblance" to password sharing for a public system).

D. Breaching Terms of Service on a Public Website

Another fact pattern that is relatively uncommon in the courts—but that has motivated substantial concern from judges and commenters owing to its sweeping implications—is breaching terms of service on a public website. In the most frequently litigated version of this fact pattern, a mass-market online service seeks to restrict a competitor from building a derivative business.[101] The competitor regularly retrieves product and service webpages from the online service's website, and uses the content of those webpages for its own commercial purposes. But the terms of service on the website forbid repurposing information to build a competitive offering.

The first two steps of the four-part analysis clarify that *without* authorization liability is inapplicable in these fact patterns. The relevant computer system is the website, as an objectively discrete collection of information and services. Plainly, the competitor has *some* authorized access to the website because it is open to the public. The competitor does not, therefore, access the website *without* authorization.

The second two steps clarify that, in general, terms of service breaches will also not constitute *exceeding* authorized access. The relevant scope of information is each webpage that the competitor saved because each webpage is an objective set of data. The website's terms of service impose a restriction on that information—but the restriction is fundamentally *purposive* because it restricts leveraging the information only for the purpose of developing a competitor. The terms of service constitute a *use* restriction, not an *access* restriction, and are therefore not enforceable as *exceeding* authorized access.

If an online service wishes to shut out a competitor, it still has CFAA remedies. It could send a letter that explicitly revokes *all* authorized access to its systems, for example, or a letter that explicitly revokes *all* authorized access to particular information or services.[102] A competitor that refused to comply would be liable for access *without* authorization or *exceeding* authorization respectively. But short

---

101 Craigslist, Facebook, and Oracle have all invoked the CFAA in this fashion. *See, e.g.*, *Craigslist I*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (service that mapped apartment postings); *Oracle Am. I*, No. C 12-00790 SBA, 2012 WL 6019580 (N.D. Cal. Dec. 3, 2012) (service that provided software updates); Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012) (service that aggregated social network updates).

102 *See, e.g.*, *Craigslist I*, 964 F. Supp. 2d. at 1183 (allowing CFAA claim where plaintiff expressly and completely revoked defendant's authorization by letter); Weingand v. Harland Fin. Sols., Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (allowing CFAA claim where plaintiff arguably delineated defendant's authorization by verbal statement).

of an overt and unambiguous prohibition of that sort, terms of service are not enforceable under the narrow CFAA doctrine.[103]

Conclusion

The current CFAA places the federal courts in an interpretive dilemma. On the one hand, the CFAA's statutory text is ambiguous and broad. Snippets in the legislative history do hint at an expansive sweep. On the other hand, if the CFAA covers nearly all forms of computer misconduct, the potential liability for ordinary computer users would be intolerable.[104] The statute's legislative history is primarily addressed at sophisticated computer hackers, and it does not speak with clarity befitting the potentially extraordinary extent of liability.

Congress is, of course, ultimately responsible for setting the scope of computer-crime liability. A statutory overhaul could put an end to decades of inconsistent case law and strike a more careful balance between relevant equities. There is much to commend the code-based standard of liability, for example, and the Author's own preference is that Congress implement a version of that approach. But, for the foreseeable future, Congress is not in the business of substantially revising the CFAA's core provisions.

Courts are stuck with the version of the CFAA on the books. And unless they are to legislate from the bench, they must adopt an interpretation that is consistent with the statutory text and legislative history. Much as the code-based test holds appeal, it simply cannot be squared with the statute.[105]

The narrow interpretation of the CFAA offers a path forward for the federal judiciary. It enables courts to meaningfully reform the CFAA's scope and to provide overdue clarity for consumers and employees. But it also remains firmly grounded in the CFAA's text and consistent with the CFAA's legislative history.

To be very clear: this Article is not arguing that the narrow interpretation of the CFAA is normatively preferable to a code-based test, whenever Congress elects to revisit the CFAA. The narrow doctrine

---

103 The narrow interpretation of the CFAA has not clearly addressed policy restrictions on particular *methods* of accessing information or services. A website terms of service agreement that prohibits automated software interaction, such as "crawlers" or "scrapers," could potentially be actionable as a restriction on information *access*.

104 Then-Chief Judge Alex Kozinski of the Ninth Circuit offered a particularly sharp version of this critique in *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

105 *See supra* note 60 and accompanying text.

is not as determinate as the code-based test; distinctions between "access" and "use" remain somewhat mushy, for instance, and the law on password sharing remains unsettled. The narrow doctrine is not as accommodating of mundane conduct as the code-based test; former employees will remain liable, as will recipients of cease-and-desist letters. The narrow doctrine does not derive from clear policy principles, unlike the code-based test; it is difficult to envision a set of policy priorities that would lead to the clumsy four-step analysis.

But the narrow interpretation of the CFAA has a key advantage: courts can adopt it today. That is why the narrow interpretation of the CFAA is so important. And that is why a proper understanding is so vital for scholars and practitioners.