


4-29-2020

The Common Law of Cyber Trespass

Michael J. O'Connor

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/blr>

 Part of the [Common Law Commons](#), [Computer Law Commons](#), [Internet Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Michael J. O'Connor, *The Common Law of Cyber Trespass*, 85 Brook. L. Rev. (2020).
Available at: <https://brooklynworks.brooklaw.edu/blr/vol85/iss2/4>

This Article is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Law Review by an authorized editor of BrooklynWorks.

The Common Law of Cyber-Trespass

Michael J. O'Connor[†]

INTRODUCTION

For over thirty years, the federal government has relied on the Computer Fraud and Abuse Act (CFAA) as its principal weapon for punishing computer misuse.¹ Shortly after the movie *WarGames*² popularized the idea that teenage boys were hacking into Pentagon supercomputers, Congress first drafted the CFAA to protect a few federal computers. From that narrow beginning, Congress has repeatedly expanded the law, with its current incarnation protecting at least every computer connected to the internet.³

Despite its age, key terms in the CFAA remain undefined. In particular, neither Congress nor the Supreme Court has explained what it means to access a computer “without authorization.”⁴ This phrase pervades the statute, dividing innocent computer use from malicious computer abuse. And yet the circuits split deeply over its meaning.⁵

Two philosophical extremes have developed. On one side, some scholars and civil rights groups claim that virtually any

[†] J.D., University of Pennsylvania Law School; B.S., Penn State University (Computer Science). This article was written while I was a Visiting Assistant Professor of Law at Penn State. My thanks to James Grimmelman, Ben Johnson, Orin Kerr, Steve Ross, and Megan Wright for their helpful suggestions. Michael Antonino and Ettore Carchia, Penn State Law Class of 2020, provided valuable research assistance.

¹ See Paul J. Larkin, Jr., *Reasonably Construing the Computer Fraud and Abuse Act to Avoid Overcriminalization*, HERITAGE FOUND. (June 19, 2013), <https://www.heritage.org/government-regulation/report/reasonably-construing-the-computer-fraud-and-abuse-act-avoid> [<https://perma.cc/T66F-Z7XZ>] (“The Computer Fraud and Abuse Act (CFAA) is the federal government’s principal legal weapon in the battle to protect computer systems and electronically stored information from thieves and vandals.”).

² WARGAMES (United Artists 1983).

³ See 18 U.S.C. § 1030(e)(2) (defining “protected computer” to include every computer “which is used in or affecting interstate or foreign commerce or communication”); Paul J. Larkin, Jr., *United States v. Nosal: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIR. REV. 257, 261 (2012) (“The CFAA effectively reaches any computer connected to the Internet by wire or wireless technology, as well as perhaps any other, unconnected computer that any company or person worldwide uses in any commercial or financial transaction that has an effect on commerce in the United States.”).

⁴ *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) (“Congress did not define the phrase ‘without authorization,’ perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive.”).

⁵ See *infra* Part II.

CFAA enforcement departs from the principles underpinning a free and open internet. To separate criminal hacking from mere bad behavior, they propose a bright-line rule: unless a suspected hacker bypasses a password gate, no CFAA liability attaches.⁶ On the other extreme, some courts consider “without authorization” to capture not only external hackers, but workers disloyal to their employers and even website users that violate terms of service.⁷ Unhappy with both extremes, courts have usually staked out a middle ground, picking and choosing principles from each side.⁸ Unfortunately, without a clear philosophical anchor, this precedent whipsaws back and forth.⁹ And it has fragmented in an extraordinary way. Providing a definitive count for total approaches may prove impossible. Various court opinions and scholarly articles put the number somewhere between two and five.¹⁰ That condition cannot stand. The law loses the public trust when the same actions garner an acquittal in Los Angeles and a conviction in Chicago.

Trespass law could remedy that confusion. Trespass law builds upon centuries of disputes, chronicling human strengths and frailties, recognizing rights and obligations. It explains when we can shut others out and when we must let them in. It can do the same now, with cyber-trespass. But scholars have traditionally opposed importing trespass precedents to hacking statutes, concerned with creating an “anti-commons” where system owners like Comcast, website owners like Twitter, and content owners like Disney can stake claims to vast internet property and enforce them through criminal law.¹¹ Courts have been similarly reluctant to import traditional trespass rules. Though less clear in their reasons, judges referring to “a cybernaut with a BitTorrent protocol” may have difficulty drawing the necessary analogies between old concepts and new technologies.¹²

Still, scholars recognize that the deepening circuit split is untenable. In recent articles, leading scholars and practitioners like Orin Kerr, Josh Goldfoot, and Aditya Bamzai acknowledge that the trespass framework could resolve the wrangling over CFAA authorization.¹³ At the same time, others suggest that

⁶ See *infra* Section II.D.

⁷ See *infra* Sections II.A, B.

⁸ See *infra* Section II.C.

⁹ See *infra* Part II.

¹⁰ See *infra* Part II.

¹¹ See *infra* Section II.D.

¹² *Washington v. U.S. Dep't of State*, 318 F. Supp. 3d 1247, 1262 (W.D. Wash. 2018).

¹³ See, e.g., Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1478 (2016) (“The text, structure, and history of the CFAA all indicate that its ‘without authorization’ term incorporates preexisting

resources like antitrust law can manage the “anti-commons” risks.¹⁴ But scholars remain divided over broadly importing specific trespass precedents. Professor Kerr suggests that we cannot easily analogize these precedents to modern facts.¹⁵ He believes that we face an unappealing choice: either 1) we must wait long years for independent computer trespass norms to develop; or 2) the courts must resolve the uncertainty and impose norms now.¹⁶ Mr. Goldfoot and Professor Bamzai argue that trespass precedents prove more than capable, but decline to begin drawing analogies from old precedents to resolve current disputes in the case law.¹⁷

This article agrees with Goldfoot and Bamzai’s contention and starts to fill the gap left in the scholarship. Trespass precedents provide a framework for dealing with the wide factual differences among potential cases. Courts have hammered out how a property owner’s rights intersect an employee’s rights and how both affect a customer. As Warren and Brandeis once said in their famous article on privacy, “[T]he common law provides [us] with [a weapon], forged in the slow fire of the centuries, and today fitly tempered to [our] hand.”¹⁸

This article focuses on specific trespass precedents, using them to hone the CFAA’s edge. When we examine trespass more deeply, many insights emerge. These precedents reject at least three main CFAA approaches taken by the Courts of Appeals and scholars.¹⁹ They suggest ways to channel the final approach.²⁰ They also suggest resolutions to particular applications that have similarly split the circuits, like what to do when an outsider induces an employee to steal secrets.²¹

Part I of this article discusses the CFAA’s history. Part II explains the current circuit split over authorization, and applies trespass precedents to reject certain approaches and narrow the

physical trespass rules.”); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016) (“[C]oncepts of authorization rest on trespass norms.”).

¹⁴ See *infra* Section III.B.2.

¹⁵ See Kerr, *supra* note 13, at 1157–58 (“[C]ourts cannot merely invoke existing trespass norms to interpret authorization to access a computer. It’s not clear any widely shared norms exist yet. . . . Courts must instead decide between competing claims for what the trespass norms should be, imposing an answer as a matter of law now rather than allowing them to develop organically.”).

¹⁶ See *id.*

¹⁷ See Goldfoot & Bamzai, *supra* note 13, at 1499 (“Precedents on physical trespass provide a richer and more nuanced set of doctrines than has been previously appreciated.”).

¹⁸ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1890).

¹⁹ See *infra* Sections II.A, II.B, & II.D.

²⁰ See *infra* Section II.C.

²¹ See *infra* Section III.A.

split overall. Part III explains and applies precedents from trespass law to situations that arise repeatedly in CFAA litigation.

I. HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT

The CFAA arose from popular pressure to combat computer hacking²² and genuine concern that existing laws did not cover common hacking crimes.²³ At first, Congress carefully limited its scope to computers implicating national security and financial privacy.²⁴ Then, Congress expanded the statute's scope to reach all computers in interstate commerce.²⁵ At the same time, companies expanded the internet's scope so that interstate commerce reached all computers. Today, the CFAA essentially encompasses every computer and computer user in the United States, and many beyond the United States' territorial limits. Its use in litigation has grown in parallel. Though the first case referencing the CFAA does not appear until 1990,²⁶ 5 cases appeared in 1998, 141 cases appeared in 2008, and 223 cases appeared in 2018.²⁷

Enacted in 1984, the CFAA was originally a narrow statute designed to criminalize access to computers in which the federal government had a substantial interest.²⁸ Congress limited the 1984 statute to three specific scenarios: "computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers."²⁹

²² See, e.g., H.R. REP. NO. 98-894, at 10 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3696 ("For example, the motion picture 'War Games' [sic] showed a realistic representation of the automatic dialing and access capabilities of the personal computer."); Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, VA. J.L. & TECH., Summer 2014, at 1, 27 ("Notably, the first version of the CFAA was passed shortly after the release of *WarGames*, almost as if the law were drafted to directly address the types of activities carried out by [Matthew Broderick's character] Lightman.").

²³ See, e.g., H.R. REP. NO. 98-894, at 6 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3691 ("There is no specific federal legislation in the area of computer crime. Any enforcement action in response to computer-related crime must rely on statutory restrictions that were designed for other offenses, such as mail fraud (18 U.S.C. 1341) or wire fraud (18 U.S.C. 1343) statutes. Even if an approach is devised that apparently covers the alleged acts in computer-related crimes, it still must be treated as an untested basis for prosecution in the federal trial courts.").

²⁴ See *infra* notes 28–29 and accompanying text.

²⁵ See *infra* notes 30–31 and accompanying text.

²⁶ See *United States v. Riggs*, 739 F. Supp. 414, 416, 423 (N.D. Ill. 1990).

²⁷ Obtained from Westlaw searches for "Computer Fraud and Abuse Act" conducted on all federal and state cases for the referenced years. Results on file with the author.

²⁸ See Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92.

²⁹ Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010) (citing 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985)).

In 1986, Congress added interstate offenses committed over an interstate computer network.³⁰ The change meant little at the time; three decades ago, when the internet was a curiosity rather than the backbone of global commerce, hacking crimes were infrequent.³¹ In 1994, the CFAA's civil provision first appeared.³² Employers have often used this provision to punish suspected trade secret misappropriation.³³ Indeed, one article calls the CFAA “the employer’s new weapon.”³⁴ Plaintiffs have also used this civil provision as a backdoor method for obtaining federal jurisdiction over claims that they must typically try in state court, like theft of trade secrets and breach of noncompete agreements.³⁵

In 1996, Congress dramatically expanded the CFAA. Of principal interest are two changes to Section 1030(a)(2), now the broadest and most commonly used provision for punishing hacking.³⁶ First, the “Federal interest” computer protected under the statute was replaced by a new category called the “protected computer.”³⁷ While the prior definition covered crimes involving computers in two or more states, the “protected computer” included any machine “used in or affecting interstate or foreign commerce or communication.”³⁸ Any computer connected to the internet is fair game.³⁹ Second, Section 1030(a)(2) went from prohibiting unauthorized access that obtains certain sensitive information to prohibiting unauthorized access that obtains *any* information.⁴⁰ Obtaining information includes merely reading it.⁴¹

³⁰ See *id.* at 1565.

³¹ *Id.* at 1565 (“[W]hen use of the Internet remained in its infancy, few crimes would be included in its reach.”).

³² See Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX § 290001(d), 108 Stat. 2097, 2098 (codified at 18 U.S.C. § 1030(g)).

³³ See, e.g., *WEC Carolina Energy Sols., LLC v. Miller*, 687 F.3d 199, 201–02 (4th Cir. 2012).

³⁴ Richard Warner, *The Employer’s New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL’Y J. 11, 11 (2008).

³⁵ See 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, 496 (2013) (“[A]sserting a claim under a federal statute, such as the CFAA, opens the door to federal court.”).

³⁶ See Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), <https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology> [<https://perma.cc/5CPD-YG4T>] (referring to 18 U.S.C. § 1030(a)(2)(c) as the “broadest provision”).

³⁷ See Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491–92 (codified as amended in scattered sections of 18 and 42 U.S.C.).

³⁸ 18 U.S.C. § 1030(e)(2).

³⁹ See Kerr, *supra* note 29, at 1568.

⁴⁰ *Id.* at 1566–67.

⁴¹ S. REP. NO. 99-432, at 6 (1986), as reprinted in 1986 U.S.C.C.A.N. 2479, 2484 (explaining that “obtaining information” in the statute included “mere observation of the data”); see also *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000).

Considering all these changes together, a statute that originally barred hacking into sensitive government computers or centralized financial databases now federally criminalizes all hacking.⁴² This includes hacking where the target computer resides on the same street, on the same floor, or even in the same room as the hacker, so long as the target was connected to the internet.⁴³

II. “WITHOUT AUTHORIZATION” AND “EXCEEDS AUTHORIZED ACCESS”

The CFAA punishes whoever “intentionally accesses a computer without authorization or exceeds authorized access.”⁴⁴ In its wisdom, Congress defined neither “access” nor “authorization.”⁴⁵ Surprisingly, however, Congress *did* define “exceeds authorized access,” explaining that it “means to access a computer with authorization” and then transgress that authorization’s boundaries.⁴⁶

Left with half-defined key terms, both courts and scholars have found themselves somewhat lost at sea.⁴⁷ We don’t

⁴² See Kerr, *supra* note 29, at 1561 (“The statute, originally designed to criminalize only important federal interest computer crimes, potentially regulates every use of every computer in the United States and even many millions of computers abroad.” (footnote omitted)).

⁴³ Subsequent amendment expanded the “protected computer” definition yet again, now reaching any computer even “affecting” interstate commerce. *Id.* at 1569–71. Under current Commerce Clause jurisprudence, this would likely reach every computer, even those lacking any internet connection. See *id.* But given the internet’s modern ubiquity, this may mean a legal distinction without practical difference.

⁴⁴ 18 U.S.C. § 1030(a)(2). Similar language appears throughout the statute, but (a)(2) is the broadest and most frequently charged provision.

⁴⁵ See 18 U.S.C. § 1030(e) (defining neither “access” nor “without authorization”); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) (“Congress did not define the phrase ‘without authorization,’ perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive.”). For over thirty years, Congress has repeatedly refined the CFAA without addressing these terms. See *supra* Part I. At this point, one can only assume intentional inaction. But Congress may well have good reason for staying out of it. As one commentator notes, Congress has decided to sacrifice precision for flexibility, crafting a single statute that can broadly apply to the many ways individuals abuse computers. See Greg Pollaro, Comment, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, ¶ 10 (“Congress decided early in the CFAA’s history that it wanted a single statute to cover the field of computer crime ‘rather than identifying and amending every potentially applicable statute affected by advances in computer technology.’ The price for this legislative expediency is that one relatively brief statute is applied to a range of disparate activities such as fraud, trespass, spam, phishing, worms, viruses and denial of service attacks. This has inevitably forced square pegs into round holes.” (citations and footnotes omitted)).

⁴⁶ 18 U.S.C. § 1030(e)(6) (“[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.”).

⁴⁷ See *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 615 (E.D. Pa. 2013) (“The term ‘authorization’ is not further defined, leaving courts to wrestle with the breadth of its meaning as increasingly, employers have used a statute originally designed to punish hackers against disloyal employees.”); Kerr, *supra* note 29, at 1562 (“The meaning of unauthorized

even know how many approaches exist: at least two,⁴⁸ likely three,⁴⁹ and perhaps four or five.⁵⁰ This article organizes the approaches into four groups—*Citrin's* agency approach, the use contract approach, the access contract approach, and the code-based approach—but acknowledges that other divisions may be equally sensible. The discussion below progresses from the approach generating the most liability to the least, and thus starts with *Citrin's* agency approach, likely capturing the most behavior within the CFAA's civil and criminal ambit.

A. *Citrin's Agency Approach*

In *International Airport Centers, LLC v. Citrin*, the Seventh Circuit attempted to create a comprehensive framework for authorization under the CFAA.⁵¹ The court articulated an agency-based approach that premised authorization on employee loyalty.

Defendant Jacob Citrin decided to go into business for himself, competing with his current employer International Airport Centers (IAC).⁵² Because this violated Citrin's employment agreement, he wanted to hobble his employer's ability to gather evidence showing his bad acts. For that reason, he wiped his work laptop before leaving.⁵³ IAC subsequently sued Citrin under the CFAA for this "damage."⁵⁴

IAC had issued this laptop to Citrin and authorized him to use it. While IAC permitted Citrin to use it for the company's benefit, the Seventh Circuit concluded that IAC's authorization lapsed the moment Citrin decided to use (or abuse) it for his *own*

access is remarkably unclear, however, with courts and commentators disagreeing sharply as to how much conduct counts and what principle of authorization the statute adopts.”).

⁴⁸ See, e.g., *United States v. Valle*, 807 F.3d 508, 524–25 (2d Cir. 2015) (dividing the approaches in two); Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1445 (2016) (“Many courts summarizing the caselaw refer only to two different approaches—‘broad’ and ‘narrow.’”).

⁴⁹ See Patterson, *supra* note 35, at 499 (summarizing scholarly articles as recognizing “the agency-based theory, the code-based theory, and the contract-based theory”).

⁵⁰ See Bellia, *supra* note 48, at 1445 (“[T]he caselaw reflects at least five different interpretive paradigms.”); Patterson, *supra* note 35, at 499–500 (splitting the approaches into agency, broad contract-based, narrow contract-based, and code-based).

⁵¹ *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 419–20 (7th Cir. 2006).

⁵² *Id.* at 419.

⁵³ *Id.*

⁵⁴ *Id.* at 420 (citing 18 U.S.C. § 1030(a)(5)(A)(ii)).

benefit.⁵⁵ But the CFAA never mentions a duty of loyalty.⁵⁶ To read this obligation into the CFAA, the Seventh Circuit looked to agency law, holding that Citrin automatically lost authorization when he transgressed the duty of loyalty that employees owe to their employers.⁵⁷

Citrin bears analytical shortcomings raised repeatedly by courts⁵⁸ and commentators.⁵⁹ Perhaps most notably, it lacks deference to the statutory text. Reading “without authorization” in this way eliminates situations in which a user “exceeds authorized access.”⁶⁰ If a party “use[s their] access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter,” Congress says they “exceed[] authorized access.”⁶¹ But courts adopting *Citrin*’s approach would say that the user’s disloyalty stripped their original authorization, and thus they are “without authorization.”⁶² Under this approach, no situations exist where a party would exceed authorized access.

⁵⁵ *Id.* (“[Citrin’s] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.” (first citing *United States v. Galindo*, 871 F.2d 99, 101 (9th Cir. 1989); then citing *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000); and then citing RESTATEMENT (SECOND) OF AGENCY §§ 112, 387 (AM. LAW INST. 1958))).

⁵⁶ See 18 U.S.C. § 1030.

⁵⁷ See *Citrin*, 440 F.3d at 419–20.

⁵⁸ See, e.g., *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (“[T]he [agency] theory has far-reaching effects unintended by Congress.”); *LVRG Holdings LLC v. Brekka*, 581 F.3d 1127, 1133–35 (9th Cir. 2009).

⁵⁹ See, e.g., Larkin, Jr., *supra* note 3, at 273–74 (finding no evidence that Congress intended to incorporate state law agency principles, based on lack of any settled meaning in common or state statutory law); Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 *HAMLIN L. REV.* 81, 120 (2013) (“To the agency interpretation’s logical conclusion, every employee giving notice spends her last two weeks incurring potential civil and criminal liability each time she accesses a computer.”).

⁶⁰ The Seventh Circuit did address this point but called the difference between access “without authorization” and “exceeding authorized access” “paper thin.” *Citrin*, 440 F.3d at 420. Citing *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001), the Seventh Circuit explained that a former employee that accessed a public website and elevated their access by using confidential information would “exceed[] authorized access.” *Citrin*, 440 F.3d at 420. This distinction makes little sense, as a former employee would still violate their residual duty of loyalty by using confidential information for their own benefit.

⁶¹ 18 U.S.C. § 1030(e)(6).

⁶² See *Diamond Power Int’l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342–43 (N.D. Ga. 2007) (“Under [*Citrin* and *Shurgard*], an employee who accesses a computer with initial authorization but later acquires (with an improper purpose) files to which he is not entitled—and in so doing, breaches his duty of loyalty—is ‘without authorization,’ despite the Act’s contemplation that such a situation constitutes accessing ‘with authorization’ but by ‘exceed[ing] authorized access.’ 18 U.S.C. § 1030(e)(6). The construction of *Citrin* and *Shurgard* thus conflates the meaning of those two distinct phrases” (second alteration in original)); see also Matthew Gordon, Note, *A Hybrid Approach to Analyzing Authorization in the Computer Fraud and Abuse Act*, 21 *B.U. J. SCI. & TECH. L.* 357, 364 (2015).

Citrin also conflicts with trespass precedent, which ignores loyalty or disloyalty to a landowner when determining whether a trespass has occurred. In *Desnick v. American Broadcasting Companies, Inc.*, ophthalmologist Dr. J. H. Desnick sued for trespass after a news investigation where *PrimeTime Live* reporters used hidden cameras to pose as patients despite telling Desnick the piece “would not involve ‘ambush’ interviews or ‘undercover’ surveillance.”⁶³ But even though consent obtained by fraud is not consent,⁶⁴ the Seventh Circuit held that no trespass occurred.⁶⁵ The law operates on up-front permissions and prohibitions. If the clinic permitted prospective patients, it must likewise welcome the reporters posing as prospective patients.⁶⁶ As the Seventh Circuit explained, the law will not speculate about property owner preferences and peer into the visitor’s mind to determine criminality.⁶⁷ To hold otherwise would expose the unhappy restaurant critic, the frugal window shopper, and the unpleasant dinner guest to trespass charges.⁶⁸ *Desnick* seems consistent with broader precedent. Courts have applied similar principles to acquit unwanted protesters in common areas of private property.⁶⁹ Leading casebooks and treatises never link trespass with loyalty.⁷⁰

⁶³ *Desnick v. Am. Broad. Cos., Inc.*, 44 F.3d 1345, 1347–48 (7th Cir. 1995).

⁶⁴ See 75 AM. JUR. 2D *Trespass* § 79, Westlaw (database updated Aug. 2019) (“Neither express nor implied consent constitutes a viable defense to a trespass action, if it was obtained by misrepresentation or fraud.”); RESTATEMENT (FIRST) OF TORTS § 173 (AM. LAW. INST. 1934) (“Assent of the possessor of land fraudulently obtained or acted upon by the actor is not a consent to his entry thereon.”).

⁶⁵ *Desnick*, 44 F.3d at 1351–53.

⁶⁶ See *id.* at 1352 (“There was no invasion in the present case of any of the specific interests that the tort of trespass seeks to protect. The test patients entered offices that were open to anyone expressing a desire for ophthalmic services . . .”).

⁶⁷ *Id.* at 1351 (“[C]onsent to an entry is often given legal effect even though the entrant has intentions that if known to the owner of the property would cause him for perfectly understandable and generally ethical or at least lawful reasons to revoke his consent.”).

⁶⁸ See *id.* at 1351.

⁶⁹ See *St. Louis County. v. Stone*, 776 S.W.2d 885, 887–88 (Mo. Ct. App. 1989) (rejecting trespass charge where common area remained generally open to public, even though owner posted “no trespassing” signs “to lead ‘certain individuals’ to know that they did not have his consent”).

⁷⁰ Leading authorities include no relevant mentions of loyalty in the trespass sections. See, e.g., GLEASON L. ARCHER, *THE LAW OF TORTS* 174–86 (1920), <https://books.google.com/books?id=Pg4aAAAAYAAJ>; 9 MATTHEW BACON, *A NEW ABRIDGMENT OF THE LAW* 438–550 (1846), <https://books.google.com/books?id=m2kyAAAAIAAJ>; MELVILLE M. BIGELOW, *ELEMENTS OF THE LAW OF TORTS* 206–30 (6th ed. 1896), <https://books.google.com/books?id=B309AAAAIAAJ>; FRANCIS TAYLOR PIGGOTT, *PRINCIPLES OF THE LAW OF TORTS* 329–41 (1885), <https://books.google.com/books?id=mZ0DAAAAQAAJ>; WILLIAM L. PROSSER, *HANDBOOK OF THE LAW OF TORTS* 76–94 (1st ed. 1941); JOHN W. SALMOND, *THE LAW OF TORTS* 155–73 (1907), <https://books.google.com/books?id=5AA0AAAAIAAJ>; 1 THOMAS W. WATERMAN, *A TREATISE ON THE LAW OF TRESPASS IN THE TWOFOLD ASPECT OF THE WRONG AND THE REMEDY* (1875), <https://books.google.com/books?id=3XM9AAAA>

One notable counterpoint is *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, in which reporters posed as grocery store employees to videotape unsafe food handling practices.⁷¹ The Fourth Circuit held that by breaching their duty of loyalty, the reporters opened themselves to trespass damages.⁷² But even taken at face value, the Fourth Circuit's opinion channels this holding into a less radical form, explaining that the reporters "exce[ded their] authority to enter Food Lion's premises as employees."⁷³ The common law has always allowed a property owner to set the boundaries of consent up-front.⁷⁴ These boundaries may take the form of explicit, up-front prohibitions.⁷⁵ Alternatively, a visitor-turned-trespasser may transgress broadly accepted societal understandings about how far the entry privilege extends.⁷⁶ An employee entering under false pretenses with the intent to plant a hidden video camera could extend beyond societal understanding about an employee's privileges.⁷⁷ The difficulty with *Food Lion* is twofold: first, the Fourth Circuit makes sloppy and unhelpful references to the duty of loyalty when it really relies on a particular view regarding up-front permissions; second, society has difficulty identifying actions that step so far beyond the pale as to transgress entry permission *even when the property owner never explicitly prohibits that action themselves*. But even if we must consider the duty of loyalty, neither *Citrin* nor *Food Lion* suggests that rule extends beyond employee trespasses.

The internet certainly does not invite applying a duty of loyalty to trespass law; if anything, it reinforces the questionable wisdom that would entail. Assuming that an employee bears a duty to his employer, I bear no such duty to every random web service provider. My duty to Amazon extends only so far as they continue to provide me the goods and services I want at competitive prices. Ours is a mercenary relationship. The same holds true for Facebook posters, LinkedIn searchers, and Twitter followers. If taken beyond

IAAJ; 2 THOMAS W. WATERMAN, A TREATISE ON THE LAW OF TRESPASS IN THE TWOFOLD ASPECT OF THE WRONG AND THE REMEDY (1875), <https://books.google.com/books?id=SnM9AAAAIAAJ>.

⁷¹ See *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 510–11 (4th Cir. 1999).

⁷² See *id.* at 518 ("The jury also found that the reporters committed trespass by breaching their duty of loyalty to Food Lion 'as a result of pursuing [their] investigation for ABC.' We affirm the finding of trespass on this ground because the breach of duty of loyalty—triggered by the filming in non-public areas, which was adverse to Food Lion—was a wrongful act in excess of Dale's and Barnett's authority to enter Food Lion's premises as employees." (alteration in original)).

⁷³ *Id.*

⁷⁴ See *infra* notes 218–219 and accompanying text.

⁷⁵ See *infra* notes 218–219 and accompanying text.

⁷⁶ See *infra* notes 218–219 and accompanying text.

⁷⁷ See *Food Lion*, 194 F.3d at 518–19.

the employer context, then *Citrin*'s reach seems boundless and its results dangerous. Perhaps for that reason, several courts have limited these duties to those spelled out in written, formal agreements, a view generally called the contract approach.

B. *The Use Contract Approach*

Seemingly uncomfortable with cabining criminal liability only by the loose concept of agency, no other circuits have adopted *Citrin*'s unalloyed reliance on that doctrine. Instead, some have sought to confine “without authorization” within more definite bounds. Just as the *Desnick* Court based trespass on up-front permissions and prohibitions,⁷⁸ these circuits base CFAA liability on violating contracts and terms of service.⁷⁹ But the contracts don't merely specify the times, circumstances, and methods by which a user can access the system, they often specify what a user can do after they access it. This turns an anti-hacking statute into a general license to combat bad behavior.

The contract approach predates *Citrin*. In *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit concluded that violating a confidentiality agreement, transmitting proprietary data, and using that data to access a public website would likely “exceed[] authorized access.”⁸⁰ No evidence suggested that the proprietary data offered access to secure or exclusive website areas. Indeed, all the pages accessed were publicly available.⁸¹ Even so, the First Circuit concluded that using the data while navigating the “website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website.”⁸²

While questioning *Explorica*'s breadth, in *United States v. John* the Fifth Circuit later agreed with its fundamental conclusion: criminal liability under the CFAA encompasses not

⁷⁸ See *Desnick*, 44 F.3d at 1352 (“There was no invasion in the present case of any of the specific interests that the tort of trespass seeks to protect. The test patients entered offices that were open to anyone expressing a desire for ophthalmic services . . .”).

⁷⁹ Admittedly, *Citrin* itself notes that the defendant “decided to quit IAC and go into business for himself, in breach of his employment contract.” *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006). But the Seventh Circuit never suggests that *Citrin*'s contract or breach thereof limited his access or use of IAC's systems.

⁸⁰ *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001).

⁸¹ The First Circuit conceded this point in a later companion opinion. See *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 61–63 (1st Cir. 2003) (“[I]t appears that the codes could be extracted more slowly by examining EF's webpages manually, so it is far from clear that Zefer would have had to know that they were confidential. The only information that Zefer received that was described as confidential (passwords for tour-leader access) apparently had no role in the scraper project.” (footnote omitted)).

⁸² *Explorica*, 274 F.3d at 583.

merely circumventing access restrictions, but ignoring use restrictions as well.⁸³ In *John*, defendant Dimetriace Eva-Lavon John was a Citigroup account manager with unrestricted access to customer account information.⁸⁴ She was convicted under the CFAA for passing confidential customer account information to her confederates, which the group used to commit fraud.⁸⁵ John argued that her CFAA conviction could not stand because Citigroup's policies restricted only how she used the information.⁸⁶ The Fifth Circuit held that Citigroup's policies were immaterial, concluding that violating use restrictions sufficed.⁸⁷

Though commonly cited to enforce employment agreements, the use contract approach cannot be so easily confined. Logically, it also encompasses violating website terms of service. Indeed, the U.S. Government advocated precisely this position in *United States v. Drew*.⁸⁸ That case arose when middle-aged mother Lori Drew created a fake MySpace account to humiliate Megan Meier, a teenage girl purportedly spreading rumors about Drew's own daughter.⁸⁹ After Drew's online persona—non-existent teenage boy Josh Evans—befriended then insulted and callously disregarded Meier, the girl committed suicide.⁹⁰ Seeking justice using any tool available, the Government charged Drew with violating the CFAA.⁹¹ The Government's claim: Drew was "without authorization" or "in excess of authorization" by violating the MySpace Terms of Service.⁹² These terms required accurate user profile information and prohibited abusive behavior.⁹³ Arrested, charged, and convicted by the jury, Lori Drew was saved from jail by the district judge.⁹⁴ The Court concluded that MySpace's Terms of Service were too vague to

⁸³ See *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010).

⁸⁴ *Id.*

⁸⁵ *Id.* at 269–70

⁸⁶ *Id.* at 271.

⁸⁷ *Id.* ("The question before us is whether 'authorized access' or 'authorization' may encompass limits placed on *the use* of information obtained by permitted access to a computer system We conclude that it may, at least when the user . . . reasonably should know that he or she is not authorized to access a computer . . . to perpetrate a crime."). One hopes that everyone realizes they are doing something criminal when perpetrating a crime.

⁸⁸ See *United States v. Drew*, 259 F.R.D. 449, 454 (C.D. Cal. 2009).

⁸⁹ See Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRE (July 2, 2009), <https://www.wired.com/2009/07/drew-court/> [<https://perma.cc/7RDT-NU5R>].

⁹⁰ See *id.*

⁹¹ See *id.*

⁹² *Drew*, 259 F.R.D. at 461.

⁹³ *Id.* at 454.

⁹⁴ See *id.* at 462–68.

put Drew on notice that violating them would strip her of authorization to use the site.⁹⁵

Despite Drew's release, the underlying logic holds. If *Explorica* and *John* win out, then terms of service logically bind users just as much as employment agreements. This approach would turn most internet users into criminals. Courts and scholars take it as a given that internet users ignore terms of service.⁹⁶ Empirical studies support this conclusion.⁹⁷ Criminally punishing terms-of-service violations conflicts with our sense of justice. Criminal law should punish exceptional behavior generally opposed by society. The Supreme Court has wisely cautioned against interpreting statutes "to criminalize a broad range of apparently innocent conduct."⁹⁸

Citrin and the use contract approach also ignore a key point: The CFAA repeatedly ties authorization to *access*.⁹⁹ The question is not whether some aspect of the user's interaction with the system was unwanted by the owner, but whether their *access* was unwanted. Indeed, an earlier version of the statute considered use,¹⁰⁰ but Congress abandoned that approach. This

⁹⁵ See, e.g., *id.* at 465 ("The MSTOS does not specify which precise terms of service, when breached, will result in a termination of MySpace's authorization for the visitor/member to access the website.").

⁹⁶ See *United States v. Nosal*, 676 F.3d 854, 861–62 (9th Cir. 2012); Kerr, *supra* note 29, at 1581.

⁹⁷ See, e.g., Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO COMM & SOC'Y 128 (2018) (finding that more than seventy percent of users never opened the agreement and those who did spent fewer than two minutes reviewing policies that should take at least fifteen minutes to read); see also Jens Grossklags & Nathan Good, *Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers*, in FINANCIAL CRYPTOGRAPHY & DATA SECURITY 341–55 (2007) (showing lack of notice and consent for software installation agreements).

⁹⁸ *Liparota v. United States*, 471 U.S. 419, 426 (1985).

⁹⁹ See, e.g., 18 U.S.C. § 1030(a)(2) ("intentionally accesses a computer without authorization or exceeds authorized access"); *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013) ("These [use contract] rulings wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use. . . . Subjective intent departs from the original view that the CFAA concerns what is 'tantamount to trespass in a computer.'" (quoting *Clinton Plumbing & Heating v. Ciaccio*, No. 09-2751, 2010 WL 4224473, at *5 (E.D. Pa. Oct. 22, 2010)); H.R. REP. NO. 98-894, at 20 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3706 ("[S]ection 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense."); David J. Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 432 (2014) ("The CFAA was aimed at 'outside hackers' who improperly access protected computers, and 'inside hackers' who have permission to use protected computers but obtain information beyond the permission that had been granted." (citation omitted)).

¹⁰⁰ Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473 § 2102, 98 Stat. 2190, 2190–91 ("Whoever . . . 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 . . .").

provides strong evidence that the CFAA does not criminalize improper use.¹⁰¹

Common law trespass has always maintained this distinction between unwelcome access (a trespass) and unwelcome behavior (not a trespass). As Blackstone explained and modern sources confirm, a patron has a general license to enter a public tavern. But if he abuses his access and “tarries there all night contrary to the inclinations of the owner[,] this wrongful act shall affect and have relation back, even to his first entry, and make the whole a trespass.”¹⁰² The same theory captures many property abuses, as jurist and scholar Thomas Street once explained:

If a lessor who enters to view for waste, damages the house, or even stays all night; if a purveyor, who takes cattle for the royal household, converts them to his own use by selling; if a commoner, who lawfully enters the common, cuts down trees; if a man who enters an inn continues all night against the will of the taverner; if the lord of a fair or market works a horse distrained for toil; or if an officer who has attached goods keeps possession of the house wherein they are taken, for an unreasonable time, without removing the goods to a place of safety; in all these cases the wrongdoer is a trespasser *ab initio*.¹⁰³

In other words, if one exercises a privilege to enter or control a property and then abuses that privilege, “the law presumes that the wrongdoer entered with the intent to commit the trespass.”¹⁰⁴ As Chief Justice Coke explained, external actions reveal secret intent: “[T]he law adjudges by the subsequent act, *quo animo*, or to what intent, he entered; for *acta exteriora indicant interiora secreta*.”¹⁰⁵ When a villain uses

¹⁰¹ See ANTONIN SCALIA & BRYAN A. GARNER, *READING LAW: THE INTERPRETATION OF LEGAL TEXTS* § 40 (2012) (“Reenactment Canon. If the legislature amends or reenacts a provision other than by way of a consolidating statute or restyling project, a significant change in language is presumed to entail a change in meaning.”); Jensen, *supra* note 59, at 125 (“Agency and contract-based interpretations are incorrect because persistent incorporation of ‘use’ flagrantly returns the CFAA to a version Congress has expressly revoked.”).

¹⁰² 2 WILLIAM BLACKSTONE, *COMMENTARIES* *213.

¹⁰³ 1 THOMAS A. STREET, *THE FOUNDATIONS OF LEGAL LIABILITY: A PRESENTATION OF THE THEORY AND DEVELOPMENT OF THE COMMON LAW* 46 (1906), <https://books.google.com/books?id=A0UzAQAAMAAJ> (footnotes omitted).

¹⁰⁴ ARCHER, *supra* note 70, at 183; *see also* 2 WILLIAM BLACKSTONE, *COMMENTARIES* *213 (“[I]f a reversioner, who enters on [pretense] of seeing waste, breaks the house, or stays there all night; or if the commoner who comes to tend his cattle, cuts down a tree; *in these and similar cases, the law judges that he entered for this unlawful purpose*, and therefore, as the act which demonstrates such his purpose is a trespass, he shall be esteemed a trespasser *ab initio*.” (first emphasis added)); 9 BACON, *supra* note 70, at 450–51 (“[T]he law intends, from the subsequent tortious act, that there was from the beginning a design to be guilty of an abuse of the authority.”).

¹⁰⁵ *The Six Carpenters’ Case*, (1610) 77 Eng. Rep. 695, 696.

the law as cover to do the illegal act they planned from the beginning, he gets punished even back to the beginning.

But when the tavern drunkard refuses to pay for his wine, that makes him a deadbeat, not a trespasser.¹⁰⁶ Only a later trespass triggers this relation back to the initial trespass.¹⁰⁷ Mere bad behavior never triggers it. This ancient division between trespassory and non-trespassory behavior demonstrates why the use contract approach—punishing behavior unrelated to access—cannot justify punishment under the CFAA.

With its non-trespassory carveout under trespass *ab initio*, the common law refused to convert a legal entry into trespass due to later non-trespassory conduct. Both *Citrin* and the use contract approach run counter to this precedent. Each treats the non-trespassory behavior as transforming the original privileged access into a trespass. This modern mistake emphasizes the need to reexamine these ancient distinctions. Whether physical or electronic, merely wrongful acts are not trespasses.

Several circuits have voiced their discomfort with the use contract approach. In its *en banc* decision in *U.S. v. Nosal (Nosal I)*, the Ninth Circuit rejected importing agency or use contract principles into the CFAA.¹⁰⁸ In *Nosal I*, the defendant used his former colleagues at executive search firm Korn/Ferry to steal trade secret files.¹⁰⁹ These colleagues had authorized access to Korn/Ferry's network and to the specific database that stored the trade secret information.¹¹⁰ Charged on CFAA violations,

¹⁰⁶ See 2 WILLIAM BLACKSTONE, COMMENTARIES *213 (“[A] bare non-feasance, as not paying for the wine he calls for, will not make him a trespasser; for this is only a breach of contract, for which the taverner shall have an action of debt or *assumpsit* against him.”); RESTATEMENT (SECOND) OF TORTS § 214 cmt. e (AM. LAW INST. 1965) (“It was also held that the subsequent act must be one which in itself would amount to a trespass, and that a mere omission, such as a failure to pay for drinks after entry, was not sufficient.”).

¹⁰⁷ See, e.g., 2 WILLIAM BLACKSTONE, COMMENTARIES *213 (“[I]f a reversioner, who enters on [pretense] of seeing waste, breaks the house, or stays there all night; or if the commoner who comes to tend his cattle, cuts down a tree; in these and similar cases, the law judges that he entered for this unlawful purpose, and therefore, *as the act which demonstrates such his purpose is a trespass*, he shall be deemed a trespasser *ab initio*.” (first emphasis added)); RESTATEMENT (SECOND) OF TORTS § 214 cmt. e (AM. LAW INST. 1965); 2 MODERN AMERICAN LAW 70 (1914), <https://books.google.com/books?id=0RMaAAAYAAJ> (“The original act must have been a trespass but for the justification, and the subsequent act must be an act of trespass”); BIGELOW, *supra* note 70, at 226 (“[O]ne who has taken possession of goods, or entered upon land, by virtue of a license of the law, becomes a trespass *ab initio* (notwithstanding the lawfulness of the levy or entry), where afterwards, while acting under the license, he commits an act which in itself amounts to a trespass.”); 2 WATERMAN, *supra* note 70, at 195–97 (“[I]t seems to be the better opinion that a man cannot become a trespass *ab initio* by any act or omission which would not itself, if not protected by a license, be the subject of trespass.”).

¹⁰⁸ See *United States v. Nosal (Nosal I)*, 676 F.3d 854, 860–61 (9th Cir. 2012) (*en banc*).

¹⁰⁹ *Id.* at 856.

¹¹⁰ *Id.*; see also *United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1031 (9th Cir. 2016) (“Searcher was hosted on the company’s internal computer network Korn/Ferry

trade secret theft, mail fraud, and other counts, the defendant moved to dismiss the CFAA counts.¹¹¹

Nosal I concluded that “without authorization” could only mean a party not authorized to access the system *at all*.¹¹² Outside hackers would fit this definition.¹¹³ By extension, “exceeds authorized access” could only mean a party authorized to use the system but not authorized for the file or function accessed.¹¹⁴ The mailroom worker who dug into the CEO’s files would fit this definition. Regardless, actions taken after the access—passing trade secret files to third parties, for example—bore no relevance to this determination.¹¹⁵ Other courts have adopted and expanded *Nosal I*’s reasoning.¹¹⁶

One commentator summed up the *Nosal I* holding with an apt analogy to the difference between theft and burglary:

If a person is invited into someone’s home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter.¹¹⁷

In trying to punish bad behavior, some courts have lost the dividing line between hacking and trade secret theft.

If the agency or contract interpretations for the CFAA win out, *Nosal I* suggests an endlessly malleable criminal law will result.¹¹⁸ Any employee that violates an employer’s trust or

issued each employee a unique username and password to its computer system; no separate password was required to access Searcher.”).

¹¹¹ *Nosal I*, 676 F.3d. at 856.

¹¹² *Id.* at 858 (“[I]t is possible to read both prohibitions as applying to hackers: ‘[W]ithout authorization’ would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and ‘exceeds authorized access’ would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files).”).

¹¹³ *See id.*

¹¹⁴ *See id.*

¹¹⁵ *See id.* at 863–64 (“This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere. Therefore, we hold that ‘exceeds authorized access’ in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.” (citation omitted)).

¹¹⁶ *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 524–27 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204–05 (4th Cir. 2012); *Diamond Power Int’l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342–43 (N.D. Ga. 2007).

¹¹⁷ Thomas E. Booms, *Hacking into Federal Court: Employee “Authorization” Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 571 (2011) (quoted with approval in *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 614 (E.D. Pa. 2013)).

¹¹⁸ *See Nosal I*, 676 F.3d at 862 (“Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without

its computer-use policy could end up behind bars. Calling a family member from their work phone, checking scores on ESPN.com, or playing Sudoku online would all result in potential trips to jail.¹¹⁹

The effect sweeps more broadly when considering website terms of service. These turgid documents, accessible only from a tiny link buried in a website's footer, are nonetheless legally binding contracts.¹²⁰ Under the agency and contract theories, the CFAA would hold visitors criminally responsible for violating these terms. Were these documents written by reasonable humans, this might not be so bad. But the internet abounds with awful terms of service. *Nosal I* points to Google's longstanding clause (from 2007 to 2012) barring minors from all Google services.¹²¹ Teenagers by the millions were committing federal crimes and didn't even know it. Facebook requires users to publish their real name, provide accurate information about themselves, avoid creating more than one account, and refrain from sharing passwords with others.¹²² Whenever a Facebook user tries to duck their ex with a fake name or present a more polished personality by using a second account for work, they expose themselves to prosecution. EHarmony's restrictions on user-posted content stretch more than a full page, including a ban on anything "objectionable."¹²³ Every single human has been found "objectionable" by another at some point. When dating in the real world, that means cutting the date short with a friend's fake phone call. With EHarmony, it could mean prison.

Criminalizing common-if-frowned-upon behavior should raise concerns. Indeed, the Supreme Court has warned against interpreting statutes to give that effect.¹²⁴ Criminalizing contract

notice. . . . Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.").

¹¹⁹ *Id.* at 860 ("Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.").

¹²⁰ Sometimes. In contract disputes, clickwrap agreements have generally been upheld, while linked agreements (sometimes called "browsewrap agreements") have seen mixed results. See Maureen A. O'Rourke, *Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act*, 2002 U. ILL. J.L. TECH. & POL'Y 295, 298 nn.12–13 (collecting cases).

¹²¹ See *Nosal I*, 676 F.3d at 861.

¹²² *Terms of Service*, FACEBOOK, <https://www.facebook.com/terms.php> [<https://perma.cc/AA2G-YFZK>].

¹²³ *Terms & Conditions*, EHARMONY, at 3, <http://static.eharmony.com/files/us/images/terms-conditions/terms-and-conditions-us.pdf> [<https://perma.cc/2VP6-ZCBF>].

¹²⁴ See, e.g., *United States v. Kozminski*, 487 U.S. 931, 949 (1988) (refusing to adopt government's position where it would "criminalize a broad range of day-to-day activity").

law is worse. Not only does it bar bad behavior; it also prevents societally desirable behavior. As mentioned above, websites often require providing truthful user information. But many legitimate professions require deception. For example, the DEA has used fake social media profiles to pursue suspects,¹²⁵ while academics have used fake profiles to root out racial discrimination.¹²⁶

Despite these concerns, the contract approach has found new life in decisions following *Nosal I*. While some courts have accepted *Nosal I*'s conclusion that the statute's plain text does not criminalize improper *use*, improper *access* falls within the CFAA's reach. Moreover, courts have generally held that system and website owners may communicate access restrictions by contract.

C. *The Access Contract Approach*

The Eleventh Circuit's opinion in *U.S. v. Rodriguez* arguably originated the access contract theory.¹²⁷ But this approach has found expanded acceptance following the Ninth Circuit's *en banc* opinion in *U.S. v. Nosal*.¹²⁸ Multiple courts have now concluded that while they may ignore use restrictions when interpreting the CFAA, they will enforce access restrictions.

In *U.S. v. Rodriguez*, the Eleventh Circuit held that Teleservice representative Rodriguez had violated the CFAA when accessing Social Security records for personal reasons.¹²⁹ Rodriguez received repeated, explicit warnings to access Social Security records only when necessary for his job.¹³⁰ He ignored those warnings.¹³¹ Again and again, he delved into files for romantic partners, friends, acquaintances, and virtual strangers.¹³² But the Eleventh Circuit did not rely on the use contract approach; indeed, it stated explicitly that this case was factually distinct from *U.S. v. John*.¹³³ Because Rodriguez had *accessed* files beyond his purview, it deemed his use irrelevant.¹³⁴

¹²⁵ *Facebook Demands DEA Stop Using Fake Profile Pages to Conduct Investigations*, FOX NEWS (Dec. 20, 2015), <https://www.foxnews.com/politics/facebook-demands-dea-stop-using-fake-profile-pages-to-conduct-investigations> [<https://perma.cc/PBS9-BH6G>].

¹²⁶ See Brian Z. Mund, Comment, *Protecting Deceptive Academic Research Under the Computer Fraud and Abuse Act*, 37 YALE L. & POL'Y REV. 385, 385–86 (2018).

¹²⁷ See *United States v. Rodriguez*, 628 F.3d 1258, 1260–63 (11th Cir. 2010).

¹²⁸ See *Nosal I*, 676 F.3d 854 (9th Cir. 2012) (*en banc*).

¹²⁹ See *Rodriguez*, 628 F.3d at 1263.

¹³⁰ *Id.* at 1260.

¹³¹ *Id.* at 1260–62.

¹³² See *id.*

¹³³ See *id.* at 1263.

¹³⁴ *Id.* at 1263 (“[Rodriguez’s] use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access.”).

Courts and scholars have grouped *Rodriguez* with *John* and even sometimes *Citrin*.¹³⁵ But these affiliations seem questionable. *Rodriguez* accessed files that his employer specifically barred him from viewing. To use an analogy, imagine *Rodriguez* as a bank teller that received a master key with instructions to access a specific safe deposit box. But while in the vault, he opened a dozen others. This does not seem like the unconstrained approach in *Citrin* and *John*. *Rodriguez* looks a lot like a situation described in *Nosal I* as exceeding authorized access, where a user logs into the system with permission, but then opens files that the system owner clearly prohibits that user from seeing.¹³⁶

On the surface, the access contract approach seems more defensible than the use contract approach. But, as Professor Patricia Bellia suggests, the result often turns principally on labeling, not substance, rendering the line between the two approaches “illusory.”¹³⁷ Revisiting the EHarmony Terms of Service that barred “objectionable” posts,¹³⁸ if EHarmony had said “Your right to access the service immediately and automatically terminates when you make an objectionable post,” then a court might consider the provision an access restriction. Indeed, the *Drew* Court considered the MySpace Terms of Service as a constraint on access and would have permitted them on that basis, even though ultimately finding that recognition of such under the statute would create unacceptable vagueness.¹³⁹ When

¹³⁵ See, e.g., *Nosal I*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) (classifying *Rodriguez* with *Citrin* and *John*); Bellia, *supra* note 48, at 1452 n.51 (classifying *Rodriguez* with *John*, but not *Citrin*).

¹³⁶ See *Nosal I*, 676 F.3d at 856–57 (“[A]ssume an employee is permitted to access only product information on the company’s computer but accesses customer data: He would ‘exceed[] authorized access’ if he looks at the customer lists.” (second alteration in original)).

¹³⁷ Bellia, *supra* note 48, at 1454–55 (“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. . . . 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. The line between ‘broad’ and ‘narrow’ views becomes illusory.” (footnotes omitted)); see also Jonathan Mayer, *The “Narrow” Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying* United States v. *Nosal*, 84 GEO. WASH. L. REV. 1644, 1659 (2016) (“That is not to say that the access-use dichotomy is a paragon of doctrinal clarity.”).

¹³⁸ See *supra* note 123 and accompanying text.

¹³⁹ See *United States v. Drew*, 259 F.R.D. 449, 462, 467 (C.D. Cal. 2009) (“Clearly, the [MySpace Terms of Service] was capable of defining the scope of authorized access of visitors, members and/or users to the website.”). Note, though, that other courts believe that the access contract approach narrows the CFAA and incorporated terms of service sufficiently to avoid vagueness problems. See *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 32 (D.D.C. 2018) (“Read to apply only to access, and not to use, restrictions, the Access Provision severely curtails both websites’ ability to define the law and prosecutors’ freedom arbitrarily to enforce it. Plaintiffs’ Fifth Amendment vagueness claim will be dismissed.”).

owners can so easily redefine use restrictions into access restrictions, adopting the access contract approach may not meaningfully narrow the statute.¹⁴⁰

Both the use and access contract approaches also raise policy concerns. For example, they eschew the traditional separation between civil and criminal law. Even where contracts for enormous sums are negotiated between sophisticated parties, with high stakes and intentional choices, we don't throw a breacher in jail.¹⁴¹

Trespass precedents also raise substantial questions about this approach. As discussed in the use contract section, finding retroactive access breaches based on a vaguely communicated policy looks a lot like trespass *ab initio*.¹⁴² This common law policy held responsible a party who entered under and then abused a privilege. Parties exercising a privilege might include landlords checking on a leak in a tenant's apartment, police officers investigating a disturbance, or patrons visiting a common purveyor like a tavern.¹⁴³ If these tolerated guests abused their privilege by staying all night, then trespass *ab initio* treated them as trespassers from the beginning.¹⁴⁴

Even when trespass *ab initio* remained viable law, the doctrine held that non-trespassory privilege abuses would not relate back.¹⁴⁵ Staying all night in a tavern was trespass *ab initio*, but failing to pay for the wine was not.¹⁴⁶ This distinction between trespassory and non-trespassory abuses constrained trespass *ab initio*. Taking this intentional distinction and drawing modern lessons from it, we concluded in the previous

¹⁴⁰ See Patterson, *supra* note 35, at 527–28 (“[I]n allowing employers to control the scope of the CFAA by merely changing the word use to access, courts adopting a narrow contract-based approach have missed the point of narrowing the CFAA’s scope.”).

¹⁴¹ See Larkin, Jr., *supra* note 3, at 275 (“[C]riminal law generally does not remedy contract violations. The law provides remedies for a contract breach because it wants to encourage parties to keep their word in order for commerce to be effective. But . . . society does not deem the parties who breach a contract to be sufficiently blameworthy to justify the moral condemnation that accompanies a criminal conviction. Like other contracts, therefore, terms-of-service agreements should be enforced only through the civil law.” (footnotes omitted)).

¹⁴² See *supra* Section II.B.

¹⁴³ See ARCHER, *supra* note 70, at 183 (constable and inn examples); 9 BACON, *supra* note 70, at 451 (landlord). Business owners are sometimes treated as granting implied consent rather than patrons having a privilege under law. See ARCHER, *supra* note 70, at 181 (“An implied license arises whenever the occupant of premises carries on a business as a tradesman or mechanic.”). Common purveyors like taverns seem the exception to this rule. See *id.* at 182 (“[L]icense of law arises whenever a public good will result from the invasion. Typical instances are seen in the right . . . of a traveler to enter an inn or conveyance of a common carrier . . .”).

¹⁴⁴ See *supra* Section II.B.

¹⁴⁵ See *supra* Section II.B.

¹⁴⁶ See *supra* Section II.B.

sections that courts should not apply the use contract approach to treat modern non-trespassory abuses as access violations.¹⁴⁷

But the law has actually abolished trespass *ab initio* entirely, which suggests that we should disfavor criminalizing even supposed access violations. When created, trespass *ab initio* was a necessary legal fiction.¹⁴⁸ In particular, it overcame medieval pleading rules that required an unlawful initial entry, or the wrongful later act would go unpunished.¹⁴⁹ But the law moved on. Punishments developed for those later wrongs, and the doctrine's importance declined. Over the late nineteenth and early twentieth centuries, it saw both increased criticism¹⁵⁰ and fewer practical applications.¹⁵¹ Eventually, the Second Restatement of Torts repudiated the doctrine entirely.¹⁵²

Yet the courts appear to have created a similar modern doctrine in the access contract approach. This is a mistake. Trespass *ab initio* was necessary to fill a gap in medieval law. No such gap exists in modern law. A system or website owner can sue for virtually any wrong committed by an unwelcome visitor. Actionable causes include contract breach, trade secret theft, and many others. There is no need to create a fiction treating later bad acts—whatever those acts are—as unauthorized access.

At the same time, the law certainly entitles property owners to both allow and forbid access.¹⁵³ Owners may turn away individuals, like a specific Met, or a group, like the hated Mets

¹⁴⁷ See *supra* Section II.B.

¹⁴⁸ See Francis H. Bohlen & Harry Shulman, *Effect of Subsequent Misconduct Upon a Lawful Arrest*, 28 COLUM. L. REV. 841, 847 (1928) (listing the bases for adopting trespass *ab initio*).

¹⁴⁹ See, e.g., SALMOND, *supra* note 70, at 168 (“The rule is primarily one of procedure, the effect of it under the old practice being that a writ of trespass would lie for the entry or seizure itself, instead of a writ of trespass or of case for the subsequent abuse only.”).

¹⁵⁰ See, e.g., McGuire v. United States, 273 U.S. 95, 98–99 (1927) (declining to apply the doctrine and explaining that its extension is disfavored); Bohlen & Shulman, *supra* note 148, at 849 (“Certainly the fiction of trespass *ab initio* ought to be banished, at least from the law of arrest.”); Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897) (“It is revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV. It is still more revolting if the grounds upon which it was laid down have vanished long since, and the rule simply persists from blind imitation of the past. I am thinking of the technical rule as to trespass *ab initio* . . .”).

¹⁵¹ See RESTATEMENT (SECOND) OF TORTS § 214 cmt. e (AM. LAW INST.1965) (“Since 1900 the weight of authority has rejected trespass *ab initio*, and there have been very few cases in which it has been applied. The decisions rejecting it have been concerned almost entirely with lawful arrest followed by tortious conduct on the part of the arresting officer; but the number of decisions which have thus rejected the doctrine, and their repudiation of the principle, indicates that it will no longer be accepted in cases of entry on land, which there is no good reason to distinguish.”).

¹⁵² *Id.* (Reporter's Notes) (“This Section has been changed from the first Restatement by reversing the position taken in Subsection (2), and rejecting the doctrine of trespass *ab initio*, as applied to privileged entries on land followed by subsequent misconduct.”).

¹⁵³ See *infra* Part III.

as a whole.¹⁵⁴ They may even condition access on behavior.¹⁵⁵ For example, an owner might welcome the Fightin' Phils to a holiday party but condition their access on not throwing anything at Santa Claus.

Unambiguous prior notice differentiates these conditions from otherwise impermissible access and use restrictions. Under the current CFAA contractual approaches, whenever an ambiguous contractual clause provides the necessary hook, system owners and the federal government each get a free-floating license to levy civil and criminal penalties.¹⁵⁶ By contrast, permissible restrictions come up-front and reasonably communicate expectations; laws governing "no trespassing" signs play some role in setting standards here, as discussed in Part III.

Of course, owners need not post up-front notices when the conduct plainly flouts authorization norms. If an intruder uses a stolen password to bypass an authentication gate, then they are "without authorization," regardless of what messages the owner has posted. Some scholars suggest that such authentication gates provide the *only* method for owners to adequately signpost their prohibition.¹⁵⁷

D. *The Code-Based Approach*

Scholars have long expressed concern with laws that would give system and website owners the ability to Balkanize the web. Some have pushed to limit owners' authority to enforce traditional rules like trespass or intellectual property infringement. To that end, some scholars argue that a user only bears liability for unauthorized access when bypassing an authentication gate like a username/password prompt. This is a mistake. It conflicts with Congress' will that system owners decide authorization. It also deprives system owners of legal tools. Paradoxically, this may push those owners to adopt technical tools that will exclude more users, rather than focusing their effort on truly bad actors.

Before the explosion in CFAA litigation, scholars first saw storm clouds in cyber-trespass litigation.¹⁵⁸ They forecasted

¹⁵⁴ See *infra* Part III.

¹⁵⁵ See *infra* Part III.

¹⁵⁶ See *supra* Sections II.B, II.C.

¹⁵⁷ See *infra* Section II.D.

¹⁵⁸ See, e.g., Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 32 (2000) (detailing the mixed experience with using trespass to chattels for computer misuse) ("[T]he claim of 'trespass' is mutating from an innovative claim to deter commercial spam into a more general claim to deter unwanted messages."); O'Rourke, *supra* note 120, at 304–05 ("[S]ome courts have mutated the traditional

that aggressive website owners would strangle internet speech and commerce, creating an “anti-commons,” in which property rights are so finely divided that it becomes essentially impossible to conduct any type of business.”¹⁵⁹ Even though that prediction has not been borne out, recent articles have raised similar concerns about the CFAA.¹⁶⁰ Others have raised the concern that broad controls for user behavior under the CFAA turn the statute into a malleable mess that regulates everything from employee laziness to trade secret theft.¹⁶¹

To prevent these problems, some scholars suggest that users should only be deemed “without authorization” where they bypass a code-based barrier like a username/password gate.¹⁶² Any more ambiguous barrier—like terms of service, IP blocks,¹⁶³ or even

trespass to chattels tort into a strict liability regime that allows Web site owners to enjoin harmless intrusions.”).

¹⁵⁹ Burk, *supra* note 158, at 49.

¹⁶⁰ See, e.g., Kerr, *supra* note 13, at 1163 (“Sellers who want to keep people out, backed by the authority of criminal trespass law, shouldn’t set up shop at a public fair. Similarly, companies that want to keep people from visiting their websites shouldn’t connect a web server to the Internet and configure it so that it responds to every request. By choosing to participate in the open Web, the website owner must accept the open trespass norms of the Web.”); Marissa Boulanger, Note, *Scraping the Bottom of the Barrel: Why It Is No Surprise That Data Scrapers Can Have Access to Public Profiles on LinkedIn*, 21 S.M.U. SCI. & TECH. L. REV. 77, 85 (2018) (“[I]t seems to be a rather common sense conclusion that was never explicitly touched upon by courts—what is public is public.”).

¹⁶¹ See, e.g., Patterson, *supra* note 35, at 528 (“All theories of interpreting authorization under the CFAA other than code-based theory will create opportunities for employers or prosecutors to use the CFAA to cover misappropriation-type claims as well as potential employee frolic claims under the CFAA.”).

¹⁶² See, e.g., Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2173 (2004) (“I . . . demonstrate that courts should apply the [CFAA] only when a system owner uses strong technical measures to control access, and argue that courts have too broadly interpreted that statute by allowing system owners to invoke it to enforce terms of use and other weak forms of notice.”); Bellia, *supra* note 48, at 1475 (“[A] code-based approach to the CFAA offers a number of advantages.”); Kerr, *supra* note 13, at 1164 (“In my view, an authentication requirement draws the proper line.”); Patterson, *supra* note 35, at 528 (“[C]ourts should expressly adopt a code-based approach to [the CFAA’s] interpretation.”). *But see* Mayer, *supra* note 137, at 1670 (“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. . . . Much as the code-based test holds appeal, it simply cannot be squared with the statute.”).

¹⁶³ IP addresses are (very loosely) like phone numbers for the internet. At any given time, they tell another computer how to get a message to you. See *IP Address*, WIKIPEDIA, https://en.wikipedia.org/wiki/IP_address [https://perma.cc/57H8-J793]. IP blocks are like caller ID blocks. If your IP address matches an entry on a website’s block list, then you can’t visit that website. See *IP Address Blocking*, WIKIPEDIA, https://en.wikipedia.org/wiki/IP_address_blocking [https://perma.cc/ZUQ5-YRD8].

CAPTCHAs¹⁶⁴ designed to turn away bots—“should be construed as insufficient to overcome the open nature of the Web.”¹⁶⁵

Until very recently, no court had accepted the code-based approach for the CFAA.¹⁶⁶ The Ninth Circuit just changed that, though it took a circuitous path to this point. Back in 2012, the Ninth Circuit’s *en banc* opinion in *Nosal I* first nodded toward the code-based approach by suggesting in dicta that only circumventing restrictions like password gates would suffice to trigger CFAA liability.¹⁶⁷ But without a clear holding to that effect, several lower courts broadened CFAA liability, adopting roughly the access contract approach.¹⁶⁸ When the Ninth Circuit’s later

¹⁶⁴ CAPTCHAs are (very easy) puzzles designed to deter bots. They often require typing the letters or numbers that appear in an image. If you can’t complete the test, the website assumes you are a bot and turns you away. See *CAPTCHA*, WIKIPEDIA, <https://en.wikipedia.org/wiki/CAPTCHA> [<https://perma.cc/JJ7A-NA9Y>].

¹⁶⁵ Kerr, *supra* note 13, at 1164. The code-based approach draws its legitimacy from clarity; it seems that everyone should understand when they have bypassed a code-based barrier. But as Professor James Grimmelmann points out, not all code-based barriers are so straightforward. He points to a fascinating case from Australia where a defendant obtained money from the ATM despite having insufficient funds in his account. Because the ATM was offline and could not check balances, it was hard-coded not to withhold funds. The defendant argued that either the ATM itself or the developers that programmed it had consented by permitting the withdrawal even though they could not know whether the balance was sufficient. See James Grimmelmann, *Computer Crime Law Goes to the Casino*, LABORATORIUM (May 2, 2013), http://laboratorium.net/archive/2013/05/02/computer_crime_law_goes_to_the_casino [<https://perma.cc/75H6-U5P7>].

¹⁶⁶ See *The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, BERKLEY TECH. L.J. BLOG (Mar. 31, 2014), <http://btlj.org/2014/03/the-computer-fraud-and-abuse-act-circuit-split-and-efforts-to-amend/> [<https://perma.cc/B3HP-4PXG>] (“No court has adopted the code-based interpretation of the CFAA.”). While interpreting state statutes, some lower courts have adopted code-based positions. See, e.g., *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715–16 (N.D. Cal. 2011); *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780-JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010). But see *Weingand v. Harland Fin. Sols., Inc.*, No. C-11-3109, 2012 WL 2327660, at *5 (N.D. Cal. June 19, 2012) (declining to adopt the code-based approach for the same statute at litigation’s outset, though not foreclosing later motions based on a more developed record). And it has been argued that one of the earliest computer trespass cases—*United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)—“invoked a close analogue to the code-based interpretation.” Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees’ Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 825 (2009). But the *Morris* holding is difficult to analogize because it dealt with a computer worm or virus. See *Morris*, 928 F.2d at 505.

¹⁶⁷ See *Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012) (*en banc*) (“[The CFAA’s] general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets . . .”).

¹⁶⁸ See, e.g., *Craigslist, Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) (acknowledging that access restrictions in terms of use might validly trigger the CFAA, but declining to resolve the question because the terms at issue were not “true” access restrictions, but only use restrictions); *Weingand v. Harland Fin. Sols., Inc.*, No. C-11-3109, 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 also *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 597 (E.D. Pa. 2016) (“[T]he Court can plausibly infer that the QVC Publisher Agreement prohibits web-crawling and that Resultly was alerted to that prohibition. . . . Accordingly, . . . the Court can plausibly infer that Resultly acted ‘without authorization’ when it crawled QVC’s website.”).

opinions in *Nosal II* and *Power Ventures* each found liability beyond authentication circumvention, it appeared that the Court of Appeals had ratified these lower-court interpretations.¹⁶⁹ But in a very recent opinion from *HiQ Labs, Inc. v. LinkedIn Corp.*, the Ninth Circuit has tightened its standard for CFAA liability, adopting the position that liability only attaches when one bypasses an authentication gate.¹⁷⁰

HiQ Labs reinterprets both *Nosal II* and *Power Ventures*, concluding that when a system owner notifies a user that its access has been revoked, the system owner does not (and seemingly cannot) prohibit access to portions of the website located *outside* an authentication gate.¹⁷¹ Rather, the system owner's cease-and-desist prohibits the user from creating new accounts or using an existing account to reach *through* an authentication gate.¹⁷² Indeed, it appears that the authentication gate becomes virtually the *only* relevant fact, without regard to whether the pages are *actually* accessible to the public. In *Power Ventures*, Facebook placed pages behind an authentication gate that any person could circumvent with a free, easy-to-create account;¹⁷³ the Ninth Circuit permitted a cease-and-desist to bar circumventing even that ephemeral gate.¹⁷⁴ Apparently the (questionable) authentication gate is the only thing that matters.

But despite the Ninth Circuit's recent endorsement, Congress never intended the CFAA to focus so narrowly. In drafting the statute, Congress could have used the word "authentication," or they could have mentioned username/password gates. Those concepts were well understood and broadly accepted in computer

¹⁶⁹ See *Nosal II*, 844 F.3d 1024, 1033–41 (9th Cir. 2016); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067, 1067 n.1 (9th Cir. 2016) ("distill[ing] two general rules": system owners may revoke access and terms of use violations are not enough, and acknowledging but declining to resolve tension between these principles where "an automatic boilerplate revocation follows a violation of a website's terms of use"). *But see* Jamie L. Williams, *Automation Is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. SCI. & TECH. L. 416, 427 (2018) ("[B]ecause both [*Power Ventures* and *Nosal II*] involved conduct the respective panels did not like, they contorted *Nosal II*'s clear holding to ensure that the defendants did not escape CFAA liability . . ." (footnote omitted)).

¹⁷⁰ See *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019) (suggesting that "authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information").

¹⁷¹ *Id.* at 1002–03.

¹⁷² *Id.*

¹⁷³ *Id.* at 1002 ("Power Ventures was gathering user data that was protected by Facebook's username and password authentication system . . .").

¹⁷⁴ *Id.* ("After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent IP barriers and gain access to password-protected Facebook member profiles. We held that after receiving an individualized cease-and-desist letter, Power Ventures had accessed Facebook computers 'without authorization' and was therefore liable under the CFAA." (internal citations omitted)).

security, even in 1984 and certainly as the CFAA was later amended.¹⁷⁵ But code-based barriers go unmentioned in the statute. Furthermore, neither “without authorization” nor “exceeds authorized access” tends naturally to suggest a code-based approach. As the Ninth Circuit explains in *Brekka*, the dictionary defines “authorization” as “permission or power granted by an authority.”¹⁷⁶ In *WEC*, the Fourth Circuit gives another dictionary definition as “formal warrant, or sanction.”¹⁷⁷ Neither definition requires that the system owner communicate authorization in any particular manner.

Trespass precedents also counsel against this rigid rule.¹⁷⁸ Physical enclosure with a fence or locked door would provide the equivalent to the electronic authentication gate. But the common law permitted owners to recover for trespass not only to their enclosed land, but also their adjacent unenclosed land.¹⁷⁹ Modern statutes do not require enclosing land; they permit reasonable notice in other forms.¹⁸⁰ In particular, statutes often detail how an owner may post their land with “no trespassing” signs to provide notice.¹⁸¹

¹⁷⁵ See, e.g., *A Short History of the Computer Password*, WELIVESECURITY (May 4, 2017), <https://www.welivesecurity.com/2017/05/04/short-history-computer-password/> [<https://perma.cc/WA9S-5PLG>] (discussing MIT developing the computer security password in the 1960s). But at least one contemporaneous dictionary ties “authorization” to usernames and passwords, which raises the plausible though unlikely suggestion that Congress had such gates in mind when using that language. See JERRY M. ROSENBERG, *DICTIONARY OF COMPUTERS DATA PROCESSING AND TELECOMMUNICATIONS* 30 (1984) (defining “authorization code” as “a code made up of user identification and password used to protect against unauthorized access to data and system facilities”).

¹⁷⁶ *LVRC Holdings LCC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (quoting *RANDOM HOUSE UNABRIDGED DICTIONARY* 139 (2001)); see also *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015) (same).

¹⁷⁷ *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (quoting *OXFORD ENGLISH DICTIONARY* (2d ed. 1989, online version 2012)).

¹⁷⁸ See, e.g., *Goldfoot & Bamzai*, *supra* note 13, at 1490 (“[T]hat meaning of ‘authorized’ [under the code-based approach] contradicts its recognized meaning in the context of physical trespass, where barriers short of physical ones are nonetheless capable of putting a would-be trespasser on notice.”).

¹⁷⁹ *BIGELOW*, *supra* note 70, at 213 (“A man’s close includes not only his actually enclosed land, but also all adjoining unenclosed lands held by him; and, if he is in possession of any part of his premises, he is in possession of the whole The owner has the ‘power of control’ and the ‘purpose to exercise the same’ for himself; he is therefore in a proper position to recover damages for trespasses committed in any part of his premises, the unenclosed as well as the enclosed. For example: The defendant, without permission, enters and cuts timber in an open woodland of the plaintiff, adjoining a farm upon which the plaintiff resides. The plaintiff is in possession of the woodland, and is entitled to recover.” (footnotes omitted)); *id.* at 219 (“Any entry upon land in the rightful possession of another, without license or permission, is a breach of duty to the possessor; and this too though the land be unenclosed.”).

¹⁸⁰ See, e.g., *State v. Dixson*, 766 P.2d 1015, 1024 (Or. 1988) (“[I]f land is fenced, posted or otherwise closed off, one does not enter it without permission”); *Rayburn v. State*, 300 S.E.2d 499, 500 (Ga. 1983) (holding that repeated warnings by police not to enter train station conveyed required notice).

¹⁸¹ See *infra* Section III.B.

Having considered how trespass precedents inform the overall approaches currently considered by courts and scholars, we can turn to how trespass precedents inform specific, frequently encountered situations in the case law.

III. APPLYING TRESPASS PRECEDENT IN SPECIFIC CASES

Admittedly, difficulties arise in analogizing common law trespass to modern electronic trespass. We must acknowledge that trespass at common law referred to a broad “constellation of related ideas.”¹⁸² In Blackstone’s words, it could encompass “any transgression or offence against the law of nature, of society, or of the country in which we live; whether it relates to a man’s person or his property.”¹⁸³ Treatises confirm that this broad trespassory definition survived in American law. Treatise authors devoted numerous chapters to trespass on the person, which included assault, battery, and false imprisonment.¹⁸⁴ They devoted similar space to trespass on personal property,¹⁸⁵ which included hunting animals belonging to another and taking goods belonging to another.¹⁸⁶ At some point, this broad trespass definition contracted. By the time the CFAA was adopted in 1984, it appears that courts primarily used “trespass” to refer to trespass upon land.¹⁸⁷

In that vein, Josh Goldfoot and Professor Aditya Bamzai have recently presented evidence suggesting that Congress intended to incorporate physical trespass law into CFAA “authorization.”¹⁸⁸ Based on that conclusion, they construct a workable general rule for authorization under the CFAA:

¹⁸² Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 90.

¹⁸³ 2 WILLIAM BLACKSTONE, COMMENTARIES *208.

¹⁸⁴ See, e.g., 1 WATERMAN, *supra* note 70, at vi–vii.

¹⁸⁵ See, e.g., *id.* at vii–ix.

¹⁸⁶ See *id.* at 355, 358.

¹⁸⁷ See, e.g., *Oliver v. United States*, 466 U.S. 170, 175 (1984) (“In this case, the officers had trespassed upon [the] defendant’s property . . .”); *Porras v. Craig*, 675 S.W.2d 503, 504 (Tex. 1984) (“In a suit for permanent damage to land, . . . the measure of damages is the difference in the market value of the land immediately before and immediately after the trespass.”); *State v. Brechon*, 352 N.W.2d 745, 747 (Minn. 1984) (“Appellants were arrested at Honeywell corporate headquarters in Minneapolis and charged with trespassing.”); *People v. Leonard*, 62 N.Y.2d 404, 407 (1984) (“Defendant was . . . charged . . . with criminal trespass in the third degree for his allegedly unlawful presence on campus.”); *State v. Ohling*, 688 P.2d 1384, 1385 (Or. Ct. App. 1984) (“[T]he officers intruded onto the curtilage of defendant’s dwelling. Their action was a trespass unless it was privileged or had defendant’s express or implied consent.”).

¹⁸⁸ See Goldfoot & Bamzai, *supra* note 13, at 1478–79, 1482. As they point out themselves, this is not the first time this suggestion has arisen. *Id.* at 1482–83, 1483 n.22. Indeed, in the earliest significant CFAA case, the Second Circuit referred repeatedly to the CFAA as punishing “trespass.” See *United States v. Morris*, 928 F.2d 504, 511 (2d Cir.

[T]he “without authorization” trespass element is met when, as in the case of physical trespass, a defendant (1) violates an express or implied prohibition on entry or access (2) about which he knew or should have known, and that (3) is material or related to access and the underlying policy of trespass.¹⁸⁹

Thus far, though, neither scholars nor the courts have taken up the work to apply trespass precedents to individual CFAA cases. Indeed, Professor Orin Kerr has suggested that such precedents are unworkable, and new precedents need to develop that specifically address CFAA scenarios.¹⁹⁰

But the law has dealt for centuries with disputes over open fields, public lands, and proprietor’s shops. The web imposes new wrinkles, shifting traditional trespass paradigms, but not nearly so far that they become inapplicable.¹⁹¹ And even if the fit proves imperfect, the courts have an obligation to try. As the Supreme Court explains, Congress often mandates that courts incorporate settled common-law principles into new packages: “[W]here Congress uses terms that have accumulated settled meaning under . . . the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms.”¹⁹²

The CFAA has most frequently been invoked in two situations: (1) to punish trade secret theft by disloyal employees, sometimes working with outside actors; and (2) to punish website misuse in various forms.

1991). But for no clear reason, CFAA jurisprudence quickly wandered away from this fundamental base.

¹⁸⁹ Goldfoot & Bamzai, *supra* note 13, at 1479.

¹⁹⁰ See Kerr, *supra* note 13, at 1157 (“Amidst this rapid technological change, courts cannot merely invoke existing trespass norms to interpret authorization to access a computer. It’s not clear any widely shared norms exist yet.”); see also Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 393 (2014) (“The broad language of the CFAA is a result of out-dated Internet philosophies from before the Internet’s omnipresence in society. Congress rooted the statute in common-law trespass doctrines However, common law property doctrine is difficult to apply in situations such as the recent *Auernheimer* case.”).

¹⁹¹ See Goldfoot & Bamzai, *supra* note 13, at 1499 (“Precedents on physical trespass provide a richer and more nuanced set of doctrines than has been previously appreciated. They allow courts to interpret the CFAA in a fair, predictable, and principled manner.”).

¹⁹² *Field v. Mans*, 516 U.S. 59, 69 (1995) (quoting *Cnty. For Creative Non-Violence v. Reid*, 490 U.S. 730, 739 (1989)); see also *Morissette v. United States*, 342 U.S. 246, 263 (1952) (“[W]here Congress borrows terms of art in which are accumulated the legal tradition and meaning of centuries of practice, it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed.”).

A. *The Disloyal Employee*

The disloyal employee scenario provokes strong emotions.¹⁹³ It strikes a traditional trust relationship when a worker sneaks around and steals valuable files, seeking to enrich themselves while still drawing a paycheck from their victim. But courts should refuse to bend the CFAA to punish disloyal employees. As discussed previously regarding *Citrin*, trespass law provides no basis for enforcing a duty of loyalty.¹⁹⁴ Adequate protections already exist to remedy contracts breached and trade secrets stolen. If an employee confines their trespass to systems they can already access, then the CFAA should probably not apply.

Certainly, prosecutable cases exist. The CFAA could punish an employee that lacks even a login for a particular system, entering through a technical flaw or by stealing another employee's credentials.¹⁹⁵ The statute embraces punishing an employee who accesses a confidential internal database that they have no legitimate reason to use.¹⁹⁶ Trespass law agrees, as "consent . . . to the actor's presence on a part of the land does not create a privilege to enter or remain on any other part."¹⁹⁷ Preferably employers would festoon databases with pop-up warnings or similar prohibition. Even better, employers could put them behind authentication gates. But such warnings are probably unnecessary. Employees know they shouldn't be poking around in the CEO's files or in other workers' pay records.

Three difficult scenarios crop up in the case law. The first scenario arises when an employee passes confidential information to the outsider. If the employee can normally access that data, then the circuits split on whether the employee has violated the CFAA.¹⁹⁸ Trespass precedents would hold the employee liable

¹⁹³ See, e.g., *United States v. Agrawal*, 726 F.3d 235, 237 (2d Cir. 2013) ("The question on this appeal is . . . not whether Agrawal is a thief. He is.").

¹⁹⁴ See *supra* Section II.A.

¹⁹⁵ Despite their employee status, there seems no reason to treat them differently than any outside hacker that behaves similarly. Thus, they should be liable not just for "exceed[ing] authorized access," but for access "without authorization." 18 U.S.C. § 1030(a)(2).

¹⁹⁶ See *Nosal I*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc) ("[E]xceeds authorized access' would refer to data or files on a computer that one is not authorized to access").

¹⁹⁷ RESTATEMENT (SECOND) OF TORTS § 169 (AM. LAW INST. 1965); see also *McCusker v. Mitchell*, 36 A. 1123, 1124 (R.I. 1897) ("It is very clear that a license to go upon one's land for a certain distance gives the licensee no right to go beyond that distance, or to do anything not specified in the license."); *Taylor v. Whitehead* (1781) 99 Eng. Rep. 475, 475 ("It is not a good justification in trespass, that the defendant has a right of way over part of the plaintiff's land, and that he had gone upon the adjoining land, because the way was impassable from being overflowed by a river.").

¹⁹⁸ Compare *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (employee liable), and *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (employee liable), with *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (employee not liable), and *Nosal I*, 676 F.3d 854 (9th Cir. 2012) (en banc) (employee not liable).

under at least some circumstances. As the Restatement explains, a person licensed to enter cannot circumvent prohibitions levied against others:

A grants permission to B, his neighbor, to enter A's land and draw water from A's spring for B's own use. A has specifically refused permission to C to enter A's land and draw water from the spring. At C's instigation, B enters A's land and obtains for C water from the spring. B's entry is a trespass.¹⁹⁹

But applying this trespass precedent to the CFAA would destroy the distinction between access and use. As discussed above, at least the Second, Fourth, and Ninth Circuits have concluded that the CFAA prohibits only improper access, not improper use.²⁰⁰ These statutory arguments are persuasive; when clearly contrary, the statute overrides common law understandings.

The second difficult scenario arises when an employee uses a database in their day-to-day duties but veers into prohibited territory by accessing records they shouldn't. No easy answer exists. Prohibitions on access and use blur into each other. Warnings may or may not give sufficient notice, depending on the individual case. *United States v. Rodriguez* provides a good example for punishment under the CFAA.²⁰¹ Rodriguez received ample warning that he should not access Social Security files for personal purposes. He was told repeatedly that he should access only files related to his official obligations, through "mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily."²⁰² One can also infer that the files were clearly separated, presumably by Social Security number or similar identifier. Further, Rodriguez's duties, which "included answering questions of the general public about social security benefits," presumably provided clear boundaries about which files he needed to access.²⁰³ A call might trigger Rodriguez to pull up the caller's file or a file about their dependents or others in their household. It would not reasonably require pulling up a file for someone in the next building, street, or town.

The third difficult scenario questions whether to punish an outside actor that induces the disloyal employee to steal secrets. Again, this splits the circuits. The principal split falls as expected: Courts willing to punish the employee have had little

¹⁹⁹ RESTATEMENT (FIRST) OF TORTS § 168 cmt. d, illus. 3 (AM. LAW INST. 1934); see also 9 BACON, *supra* note 70, at 492 ("If A command or request B to take the goods of C, and B do it, this action lies as well against A as against B.").

²⁰⁰ See *supra* Section II.B.

²⁰¹ *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).

²⁰² *Id.* at 1260.

²⁰³ *Id.*

difficulty punishing their puppeteer,²⁰⁴ while courts declining to punish the employee have likewise refused to punish the outside instigator.²⁰⁵ But the Ninth Circuit has proven a surprising outlier in this split. Even though it declined to punish the disloyal employees in *Nosal II*, it had no trouble punishing the outside actor pulling their strings.²⁰⁶ Surprisingly, this final position seems most consistent with trespass precedent. As suggested above, licenses can be personal, with authorization that does not chain from party to party.²⁰⁷ Courts can punish parties for inducing others to trespass.²⁰⁸ Indeed, by accepting stolen goods, one can even ratify the trespass after the fact, which results in trespass liability.²⁰⁹ Taken together, these

²⁰⁴ See, e.g., *Se. Mech. Servs., Inc. v. Brody*, No. 8:08-CV-1151-T-30EAJ, 2008 WL 4613046, at *14 (M.D. Fla. Oct. 15, 2008) (“Although Babcock, TEI, Maliszewski, and Naughton may not have accessed SMS’s computers, the e-mail communications among the Defendants supports SMS’s assertions that Babcock, TEI, Maliszewski and Naughton implicitly induced and/or encouraged Brody, Sherouse, and Smith to access and use SMS’s information without authorization.”).

²⁰⁵ See *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012) (holding that the outsider “cannot be liable under the statute for any role it played in encouraging such conduct”).

²⁰⁶ See *Nosal II*, 844 F.3d 1024, 1031, 1038 (9th Cir. 2016); see also *Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 671 (E.D. Pa. 2018) (“[B]ecause [insider] Sandhu did not obtain the information at issue without authorization or beyond her authorized access, we shall dismiss the CFAA claim against her. Outsiders, like Apotex and Desai, are not treated the same as insiders. Rather, they are akin to hackers, those the CFAA aimed to hold criminally and civilly liable. They did not have authority to access the computers. But, they indirectly accessed Teva’s protected computers through one who had the authority.”).

²⁰⁷ See RESTATEMENT (FIRST) OF TORTS § 168 cmt. e (AM. LAW INST. 1934) (“Although ordinarily one to whom consent is given to enter land for a particular purpose may delegate his privilege to a servant or deputy, the license may be a purely personal one. In such case, if the licensee causes a third person to enter the land, both he and the third person are trespassers.”).

²⁰⁸ See 9 BACON, *supra* note 70, at 492 (“If A command or request B to take the goods of C, and B do it, this action lies as well against A as against B.”); 1 WILLIAM BLACKSTONE, COMMENTARIES *429–30 (“[I]f the servant commit a trespass by the command or encouragement of his master, the master shall be guilty of it: though the servant is not thereby excused, for he is only to obey his master in matters that are honest and lawful.”); 1 WATERMAN, *supra* note 70, at 42 (“[T]he liability of the master for the acts of his servant depends upon whether the servant at the time, and in the particular in question, was acting under and in execution of authority from the master; in which case the master is responsible.”).

²⁰⁹ 75 AM. JUR. 2D *Trespass* § 58, Westlaw (database updated Aug. 2019) (“A person may be liable for causing someone else to commit a trespass. All persons who command, instigate, promote, encourage, advise, countenance, cooperate in, aid, or abet the commission of a trespass, or who approve of it after it is done, if done for their benefit, are cotrespassers [sic]”); 9 BACON, *supra* note 70, at 492 (“If J S agree to a trespass which has been committed by J N for his benefit, this action lies against J S, although it was not done in obedience to his command, or at his request.”); 1 WATERMAN, *supra* note 70, at 27 (“A thing done for another by a person not assuming to act for himself, but for such other person, though without any precedent authority whatever, becomes the act of the principal, if subsequently ratified by him. . . . Sir Edward Coke says: ‘He that receiveth a trespasser and agrees to a trespass after it is done, is no trespasser, unless

principles indicate that the courts should hold liable an outsider who induces an insider with access to trespass on his behalf.

B. *General Rules for Website Trespass*

One would think that websites would prove difficult to analogize to centuries-old trespass law. But precedents applying to public resources rank among the oldest and most well-established. Even the near-absolute property rights in English common law yielded to established public norms. English courts declaimed *cujus est solum, ejus est usque ad caelum et ad inferos*²¹⁰: “To whomsoever the soil belongs, he owns also to the sky and to the depths.”²¹¹ With absolute ownership came absolute right to exclude. Under English common law, “[e]very entry upon the land of another without lawful authority is a trespass, though only the grass be trodden.”²¹² Yet those opening their establishments to the public must accept that the public would enter them. As Blackstone explains: “[A] man may justify entering into an inn or public house without the leave of the owner first specially asked, because when a man professes the keeping such inn or public house he thereby gives a general license to any person to enter his doors.”²¹³ Modern law agrees;²¹⁴ the Supreme Court has held that even private homes bear an

the trespass was done for his use, or for his benefit, and then his agreement subsequent amounteth to a precedent commandment.” (citations and footnotes omitted).

²¹⁰ See, e.g., *Doe v. Burt*, (1787) 99 Eng. Rep. 1330, 1330; see also John G. Sprankling, *Owning the Center of the Earth*, 55 UCLA L. REV. 979, 982–90 (2008) (tracing maxim’s history). Modern law has stepped away from this approach. See *United States v. Causby*, 328 U.S. 256, 260–61 (1946) (“[The *cujus est solum*] doctrine has no place in the modern world.”).

²¹¹ BLACK’S LAW DICTIONARY 304 (2d ed. 1910), <https://books.google.com/books?id=R2c8AAAAIAAJ>.

²¹² 2 WATERMAN, *supra* note 70, at 219.

²¹³ 2 WILLIAM BLACKSTONE, COMMENTARIES *212; see also BIGELOW, *supra* note 70, at 221–25 (“The term ‘license of the law’ has reference to cases in which a permission is given regardless of the will of the owner or occupant, and includes all other cases in which the entry or taking possession was lawful. It includes, therefore, certain cases in which, in point of fact, there may at the same time be a license of the party; as e.g. in the case of an innkeeper, who both invites, and, generally speaking, must receive guests.”); 1 WATERMAN, *supra* note 70, at 154 (“As an innkeeper holds out his house as a public place to which travelers may resort, he cannot prohibit persons who come in that character, in a proper manner, and at suitable times, from entering, so long as he has the means of accommodation for them.”).

²¹⁴ See, e.g., 75 AM. JUR. 2D *Trespass* § 40, Westlaw (database updated Aug. 2019) (“Opening an establishment to transact business with the public is permission to enter, unless forbidden.”); *St. Louis County v. Stone*, 776 S.W.2d 885, 888–89 (Mo. Ct. App. 1989) (“In such instance where a person enters a public or common area, there is no intrusion or trespass because the person is clothed with the implied consent of the owner or possessor of the property. It would be ludicrous for a member of the public to seek out the expressed consent of the owner to enter an area already open to the public.” (internal citations omitted)).

implied license “to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave.”²¹⁵

Inevitably, business owners will wish that certain patrons had never darkened their doorstep. The hotel guest destroys their room. The diner cannot pay for their meal. They are unwelcome. They may even bear liability under other criminal or civil laws. They are not trespassers.²¹⁶

Trespass laws do not leave business owners defenseless. Guests must enter in a reasonable manner and leave when the owner asks.²¹⁷ The right to walk in a shop’s front door does not imply the right to drive through it in a tank.²¹⁸ If the owner posts a sign saying “You may not enter without wearing a funny hat,” you’d better work on your haberdashery.²¹⁹ The right to enter

²¹⁵ Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013).

²¹⁶ 2 WILLIAM BLACKSTONE, COMMENTARIES *213 (“[A] bare non-feasance, as not paying for the wine he calls for, will not make him a trespasser; for this is only a breach of contract, for which the taverner shall have an action of debt or *assumpsit* against him.”); see Goldfoot & Bamzai, *supra* note 13, at 1495 (“[F]or a violation of an express or implied prohibition to constitute a criminal trespass, it must advance the rationale for the crime of trespass.”).

²¹⁷ See, e.g., 75 AM. JUR. 2D *Trespass* § 40, Westlaw (database updated Aug. 2019) (“Once the proprietor requests that a person leave, that individual has no legal right to remain.”).

²¹⁸ See RESTATEMENT (SECOND) OF TORTS § 214(1) (AM LAW INST. 1965) (“An actor who has in an unreasonable manner exercised any privilege to enter land is subject to liability for any harm to a legally protected interest of another caused by such unreasonable conduct.”); 75 AM. JUR. 2D *Trespass* § 40, Westlaw (database updated Aug. 2019) (“An invitation to conduct business presupposes that the conduct of persons coming to the premises will be in keeping with that purpose.”); 75 AM. JUR. 2D *Trespass* § 51, Westlaw (database updated Aug. 2019) (“Although a person who enters an area open to the public at a reasonable time and in a reasonable manner has the implied consent of the owner to enter the premises under a limited privilege, substantial evidence of the stay being prolonged, boisterous conduct, breach of the peace, blocking the entranceways, interference with the public, picketing, or other conduct which would revoke the implied consent of the owner by acts inconsistent with the purposes of the business or facility, causes a trespass.”); 75 AM. JUR. 2D *Trespass* § 53, Westlaw (database updated Aug. 2019) (“An actor who has, in an unreasonable manner, exercised any privilege to enter land is subject to liability for any harm to a legally protected interest of another caused by that unreasonable conduct.”).

²¹⁹ See RESTATEMENT (FIRST) OF TORTS § 168 (AM. LAW INST. 1934) (“A conditional or restricted consent to enter land creates a privilege to do so only in so far as the condition or restriction is complied with.”); 75 AM. JUR. 2D *Trespass* § 51, Westlaw (database updated Aug. 2019) (“A trespass may occur if the party, entering pursuant to a limited consent, i.e., limited as to purpose or place, proceeds to exceed those limits by divergent conduct on the land of another, as a conditional or restricted consent to enter land creates a privilege to do so only in so far as the condition or restriction is complied with.”); Lothar Determann, *Internet Freedom and Computer Abuse*, 35 HASTINGS COMM. & ENT. L.J. 429, 443–44 (2013) (“[P]roperty owners were always able to some degree to define limitations on authorizations in a number of different ways, including the following: They can grant authorization subject to conditions precedent. . . . They can also grant authorization subject to continued conditions. . . . The property owner can also grant authorization subject to limitations”); Gideon Parchomovsky & Alex Stein, *Reconceptualizing Trespass*, 103 N.W. U. L. REV. 1823, 1855 (2009) (“The right to exclude entitles the owner not only to block another person’s entry to her property entirely but also to grant her conditional entry. The

does not prevent an owner from ejecting you and barring your future entry.²²⁰

From these precedents, this article suggests three general rules. First, access methods substantially out of step with web norms²²¹ or explicitly banned by the website owner²²² would lack authorization. On the norms side, bypassing authentication gates, as under the code-based approach, would obviously lack authorization.²²³ Denial-of-service attacks—designed to slow or crash a site and thereby render it inaccessible—would likewise lack authorization.²²⁴ On the website owner’s side, communicating prohibited access methods could be accomplished through a robots.txt file (for scrapers),²²⁵ a pop-up (for regular users), or a cease-and-desist letter (for either).

Second, an owner can tell specific users they are unwelcome in the first place. The owner can accomplish this through a pop-up, a cease-and-desist letter,²²⁶ an IP block combined with another

owner can set countless conditions for another person’s entry to her property, as well as notify any entrant, expressly or implicitly, that violation of any of those conditions would make him an unwanted trespasser.”).

²²⁰ See, e.g., *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1024 (S.D. Ohio 1997) (“[Defendants argue] that because an establishment invites the public to enter its property for business purposes, it cannot later restrict or revoke access to that property, a proposition which is erroneous under Ohio law.”); 1 WATERMAN, *supra* note 70, at 152 (“[I]f a person . . . refuses to leave the shop, after being requested by the shopkeeper or his servants, he may be ejected.”); *id.* at 154 (“[An innkeeper] is not obliged to make his house a common receptacle for all comers, whatever may be their character or condition. He is not obliged to receive one who is not able to pay for his entertainment. . . . [H]e is not bound to admit one whose notorious character as a thief furnishes good reason to suppose that he will purloin the goods of his guests, or his own. . . . [H]e may exclude common brewers, and any one who comes with intent to commit an assault or make an affray. . . . He has a right to prohibit idle persons and common drunkards from entering, and to require them and the others before mentioned to depart if they have already entered.”).

²²¹ See *supra* note 218 and accompanying text.

²²² See *supra* note 219 and accompanying text.

²²³ See 75 AM. JUR. 2D *Trespass* § 51, Westlaw (database updated Aug. 2019) (“[L]eaving the public premises of a business to venture into a posted nonpublic area changes an invitee into a trespasser.”).

²²⁴ See, e.g., *Tyco Int’l (US) Inc. v. Does*, No. 01 Civ. 3856, 2003 WL 23374767, at *2–3, *7 (S.D.N.Y. Aug. 29, 2003) (recommending injunction and nominal damages under CFAA for denial-of-service attack); see also *United States v. Morris*, 928 F.2d 504, 510–11 (2d Cir. 1991) (affirming CFAA violation for exploiting bugs and bypassing password gates that also had a denial-of-service effect).

²²⁵ For an explanation of scrapers and their configuration, see *infra* notes 271–277 and accompanying text.

²²⁶ See *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1062 (9th Cir. 2016) (“We also hold that Power violated the CFAA and California Penal Code section 502 only after it received Facebook’s cease and desist letter and nonetheless continued to access Facebook’s computers without permission.”).

more definite notice method,²²⁷ or a suspended or disabled account combined with another more definite notice method.²²⁸

Finally, the owner can turn users away any time they want. This rule plainly accords with trespass precedent. The owner “has the right to determine whom to invite, the scope of the invitation, and the circumstances under which the invitation may be revoked.”²²⁹ They can do so by providing reasonable notice to the user that they are unwelcome. As with the up-front prohibition, this can be accomplished through a pop-up, a cease-and-desist letter, an IP block combined with another more definite notice method, or a suspended or disabled account.

The question is not whether a property owner *may* restrict access, but *how* they provide sufficient notice that they *have* restricted access. In the real property context, revoking permission often means telling someone directly that they must leave.²³⁰ That occasionally happens in the CFAA context, usually with cease-and-desist letters. IP blocks and similar methods may communicate the same intent. But generally, the web’s open nature makes it difficult to single out specific trespassers to uninvite.

In the real property context, owners can also revoke permission by posting a “No Trespassing” sign.²³¹ States

²²⁷ See *id.* at 1068 n.5 (“Simply bypassing an IP address, without more, would not constitute unauthorized use. Because a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user’s roommate or co-worker.”).

²²⁸ See Kerr, *supra* note 13, at 1174 (“[S]uspending an account withdraws authorization to access the account. . . . [A] suspension may or may not signal that access to additional accounts is prohibited.”).

²²⁹ 75 AM. JUR. 2D *Trespass* § 40, Westlaw (database updated Aug. 2019).

²³⁰ See, e.g., *id.* (“Once the proprietor requests that a person leave, that individual has no legal right to remain.”); ALASKA STAT. § 11.46.350 (criminalizing “fail[ing] to leave premises or in a propelled vehicle that is open to the public after being lawfully directed to do so personally by the person in charge”); ARIZ. REV. STAT. § 13-1502 (criminalizing remaining “after a reasonable request to leave by a law enforcement officer, the owner or any other person having lawful control”); ARK. CODE ANN. § 5-39-101(3)(B)(i) (“A person who enters or remains in or upon premises that are at the time open to the public does so with license and privilege, regardless of his or her purposes, unless he or she defies a lawful order not to enter or remain . . .”).

²³¹ See, e.g., ALASKA STAT. § 11.46.350(b); ARIZ. REV. STAT. § 13-1502; ARK. CODE ANN. § 5-39-101(3)(B)(i); CAL. PENAL CODE § 602.8(a); HAW. REV. STAT. § 708-814; IDAHO CODE § 18-7008; IND. CODE § 35-43-2-2(c) & (d); 17 ME. REV. STAT. ANN. tit. 17-A, § 402(4)(A).

sometimes specify size,²³² content,²³³ cluster density,²³⁴ and other considerations. Florida provides a particularly detailed example, with land considered posted where:

Signs are placed not more than 500 feet apart along, and at each corner of, the boundaries of the land, upon which signs there appears prominently, in letters of not less than 2 inches in height, the words “no trespassing” and in addition thereto the name of the owner, lessee, or occupant of said land. Said signs shall be placed along the boundary line of posted land in a manner and in such position as to be clearly noticeable from outside the boundary line.²³⁵

But states rarely regulate signs with such detail. States often permit posting in any reasonably conspicuous manner.²³⁶

Similar notice rules should apply in the CFAA context. Because neither the federal government nor the states have legislated in this area, courts must apply some reasonable boundaries. A simple, unambiguous message establishing that an individual or recognizable group may not use the site should bar access to those listed.²³⁷ The message should require affirmative acknowledgment (e.g., a click-thru) from the user. The message should be provided with the acknowledgment button, rather than on a separate, linked page. The website owner should record the message content, the acknowledgment, and pertinent details about the visitor (e.g., IP address, cookie content, account name). A certified cease-and-desist letter would provide similar assurance that notice was received. As discussed below, other methods like IP blocks provide some evidence that notice was received, but courts should not attach criminal liability to these unless the website owner supplements them with other methods.

²³² See, e.g., FLA. STAT. § 810.011(5)(a)(1); HAW. REV. STAT. § 708-814(1)(d)(ii) (“letters no less than two inches in height”).

²³³ See, e.g., FLA. STAT. § 810.011(5)(a)(1); HAW. REV. STAT. § 708-814(1)(d)(ii) (“Private Property – No Trespassing”, ‘Government Property – No Trespassing’, or a substantially similar message”); IDAHO CODE § 18-7008(2)(a) (“conspicuous ‘no trespassing’ signs or bright orange or fluorescent paint”); IND. CODE § 35-43-2-2(c), (d) (prescribed sign, sign likely to come to public’s attention, or purple marks); 17 ME. REV. STAT. tit. 17-A, § 402(4)(A) (“Signs must indicate that access is prohibited, that access is prohibited without permission of the landowner or the landowner’s agent, or that access for a particular purpose is prohibited. . . . [Specified paint marking may also be used].”).

²³⁴ See, e.g., CAL. PENAL CODE § 602.8 (“not less than three to the mile”); HAW. REV. STAT. § 708-814(1)(d)(ii) (“no less than three signs to a mile”); IND. CODE § 35-43-2-2 (purple marks on trees no more than a hundred feet apart or posts no more than thirty-six feet apart); 17 ME. REV. STAT. tit. 17-A, § 402(4)(C) (“intervals no greater than 100 feet”).

²³⁵ FLA. STAT. § 810.011(5)(a)(1).

²³⁶ See, e.g., ALASKA STAT. § 11.46.350 (“a reasonably conspicuous manner under the circumstances”); ARIZ. REV. STAT. § 13-1502 (“reasonable notice prohibiting entry”); ARK. CODE ANN. § 5-39-101(3)(C)(ii) (“posting in a conspicuous manner”).

²³⁷ Obviously, the recognizable group cannot be a class protected by federal or state anti-discrimination laws.

This notice approach generally accords with an early CFAA case.²³⁸ In *EF Cultural Travel Corp. BV v. Zefer Corp.*, the First Circuit declined to hold that a website owner could forbid scrapers under the CFAA absent clear notice:

[The website owner] could easily include . . . a sentence on its home page or in its terms of use stating that “no scrapers may be used,” giving fair warning and avoiding time-consuming litigation

. . . .

. . . [W]ith rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid.²³⁹

The approach advocated here would differ from *Zefer* in that website owners should not bury these vital notices in terms of service.

With these principles in mind, we can address some scenarios repeatedly encountered by the courts.

1. The Denial-of-Service Attacker

Denial-of-service attacks make computer systems unavailable to legitimate users.²⁴⁰ These attacks take many forms, including spam e-mail barrages or webpage request deluges.²⁴¹ Several cases have tried to apply the CFAA to denial-of-service attacks, generally under two theories: unauthorized damage and unauthorized access. The damage theory arises from 18 U.S.C. § 1030(a)(5)(A), which prohibits “knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.”²⁴² The access theory arises from the familiar 18 U.S.C. § 1030(a)(2), which prohibits “intentionally access[ing] a protected computer without authorization.”²⁴³ Notably, these provisions differ in

²³⁸ In any other legal area, a case coming almost two decades after the statute’s enactment would not be considered an “early” case, but CFAA development has been surprisingly slow.

²³⁹ *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63–64 (1st Cir. 2003).

²⁴⁰ See NCCIC, U.S. Comput. Emergency Response Team, Dep’t of Homeland Sec., *Security Tip (ST04-015) Understanding Denial-of-Service Attacks*, (June 28, 2018), <https://www.us-cert.gov/ncas/tips/ST04-015> [<https://perma.cc/52RK-C78N>] (“A denial-of-service (DoS) attacks occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.”).

²⁴¹ See *id.* (“A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes.”).

²⁴² 18 U.S.C. § 1030(a)(5)(A).

²⁴³ 18 U.S.C. § 1030(a)(2).

what requires authorization. While (a)(2) prohibits access without authorization, (a)(5)(A) prohibits *damage* without authorization.²⁴⁴

The limited precedent uniformly treats denial-of-service attacks as unauthorized damage.²⁴⁵ For example, in *United States v. Carlson*, the Third Circuit affirmed an (a)(5)(A) conviction against a Philadelphia Phillies fan that used spoofed e-mail addresses to flood the team's front office with messages criticizing their management decisions.²⁴⁶ He clogged inboxes, caused delays, and sometimes required purging both spam and legitimate e-mails to solve the problem.²⁴⁷ Similarly, in *Pulte Homes*, a labor union mounted a protest by employing both automated systems and union members to spam employer Pulte Homes with e-mail and phone calls.²⁴⁸ The calls clogged Pulte's voicemail system and cut it off from customers.²⁴⁹ "The e-mails wreaked more havoc: they overloaded Pulte's system . . . and . . . stalled normal business operations because Pulte's employees could not access business-related e-mails or send e-mails to customers and vendors."²⁵⁰ The Sixth Circuit held this sufficient for an (a)(5)(A) claim.²⁵¹

But the Sixth Circuit rejected the companion (a)(2) claim. While concluding the damage was unauthorized, it held the access authorized because the phone and e-mail systems were open to the public.²⁵² The Sixth Circuit concluded that the statute mandated

²⁴⁴ See ORIN S. KERR, *COMPUTER CRIME LAW* 108 (4th ed. 2018) ("Note that the absence of authorization does not refer to the access, but rather to causing damage."). One may reasonably ask why anyone would grant authorization for damage. Obviously, penetration testers and other security professionals may need permission for potentially destructive testing to confirm system or network security. But because damage is defined by the statute as "any impairment to the integrity or availability of data," 18 U.S.C. § 1030(e)(8), it could also include routine maintenance tasks like encrypting files or modifying their permissions.

²⁴⁵ See, e.g., *Pulte Homes, Inc. v. Laborers' Int'l Union N. Am.*, 648 F.3d 295, 301–03 (6th Cir. 2011); *United States v. Carlson*, 209 F. App'x 181, 185 (3d Cir. 2006); *United States v. Mitra*, 405 F.3d 492, 493, 497 (7th Cir. 2005); *BHRAC, LLC v. Regency Car Rentals, LLC*, No. CV 15-865, 2015 WL 3561671, at *1–4 (C.D. Cal. June 4, 2015); *Tyco Int'l (US) Inc. v. Does*, No. 01 Civ. 3856, 2003 WL 23374767 (S.D.N.Y. Aug. 29, 2003); see also *Ebates, Inc. v. Does*, No. 16-cv-01925, 2016 WL 2344199 (N.D. Cal. May 3, 2016) (declining to decide whether Ebates pleaded a plausible CFAA claim for DDOS attack, but finding a *prima facie* showing).

²⁴⁶ See *Carlson*, 209 F. App'x at 182–83.

²⁴⁷ *Id.* at 184.

²⁴⁸ See *Pulte Homes*, 648 F.3d at 298–99, 301–03.

²⁴⁹ *Id.* at 299.

²⁵⁰ *Id.* at 299.

²⁵¹ *Id.* at 301–03.

²⁵² *Id.* at 304 ("LIUNA used unprotected public communications systems, which defeats Pulte's allegation that LIUNA accessed its computers 'without authorization.' Pulte allows all members of the public to contact its offices and executives: it does not allege, for example, that LIUNA, or anyone else, needs a password or code to call or e-mail its business.").

this view.²⁵³ While Congress never defined “without authorization,” Congress did define “exceeds authorized access.” That definition—“access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter”²⁵⁴—necessarily captures all the cases where an intruder has authorization but does something untoward. And it regulates only “obtain[ing] or alter[ing] information.” It does not regulate the methods used.²⁵⁵

Absent this statutory limit, trespass precedents favor treating situations like *Carlson* and *Pulte* as unauthorized access. Even those with authorization must behave reasonably in exercising it.²⁵⁶ In *United States ex rel. Horelick v. Criminal Court of New York*, the Second Circuit explained that a teacher authorized to “go in the front door” does not gain a license “to enter surreptitiously through a basement window.”²⁵⁷ In *Moonin v. Nevada ex rel. Department of Public Safety*, the District of Nevada held that a privilege to remove a dog kennel did not justify destroying the backyard fence in the process.²⁵⁸ In *Brutsche v. City of Kent*, the Washington Supreme Court held that when “officers executing a search warrant unnecessarily damage the property while conducting their search . . . liability in trespass can result.”²⁵⁹ Numerous other cases attest to this.²⁶⁰ But the statute reigns supreme.

There is no question that a denial-of-service attack is an unreasonable method for accessing a website, and one could argue that entering in an unreasonable manner taints the initial authorization, making access unreasonable from the beginning. But this seems a creative way to get around Congress’ textual limitation on “exceed[ing] authorized access.” Trespass precedent counsels a broad reading, but that reading can never

²⁵³ See *id.* at 303–04.

²⁵⁴ 18 U.S.C. § 1030(e)(6).

²⁵⁵ See *Pulte Homes*, 648 F.3d at 303–04; see also *Oracle USA, Inc. v. Rimini St., Inc.* 879 F.3d 948, 962 (9th Cir. 2018) (“We hold that taking data using a *method* prohibited by the applicable terms of use, when the taking itself generally is permitted, does not violate the [California CFAA]. Because the same reasoning applies to the [Nevada CFAA] claim, we reverse the judgment as to both claims.”).

²⁵⁶ See RESTATEMENT (SECOND) OF TORTS § 214(1) (AM. LAW INST. 1965) (“An actor who has in an unreasonable manner exercised any privilege to enter land is subject to liability for any harm to a legally protected interest of another caused by such unreasonable conduct.”); 75 AM. JUR. 2D *Trespass* § 40, Westlaw (database updated Aug. 2019) (“An invitation to conduct business presupposes that the conduct of persons coming to the premises will be in keeping with that purpose.”).

²⁵⁷ *United States ex rel. Horelick v. Crim. Ct. N.Y.*, 507 F.2d 37, 41 (2d. Cir. 1974).

²⁵⁸ *Moonin v. Nev. ex rel. Dep’t Pub. Safety*, 960 F. Supp. 2d 1130, 1145 (D. Nev. 2013).

²⁵⁹ *Brutsche v. City of Kent*, 193 P.3d 110, 116 (Wash. 2008).

²⁶⁰ See RESTATEMENT (SECOND) OF TORTS § 214 (AM. LAW INST. 1965) (collecting cases).

exceed the statutory text. Denial-of-service attacks clearly deserve punishment under the CFAA. But addressing them under the damage provision accomplishes the right result. It fits the offense better than mere access. And through its intent, damage, and loss requirements, it likely forecloses applying the CFAA to accidents (like a misconfigured scraper bot) that never rise to real denial-of-service attacks.

2. The Web Scraper

The modern internet requires scrapers, automated bots that play countless roles, including capturing websites for search engines like Google and surveying prices for travel sites like Kayak. Because they access many sites, sometimes for competing companies, scrapers feature regularly in CFAA litigation. As Andrew Sellars details in a comprehensive article, their treatment has evolved along with CFAA precedent.²⁶¹ Early cases suggested that virtually “*any* mechanism could be used to determine that the scraper’s access was unauthorized.”²⁶² These included use restrictions, terms of service violations, and express warnings.²⁶³ Then *Brekka* and *Nosal I* held that violating use restrictions did not garner CFAA liability.²⁶⁴ These decisions catalyzed a shift toward a narrower reading, giving less weight to website terms of service.²⁶⁵ But CFAA plaintiffs adjusted their aim and tried again, this time arguing that those failing to comply with terms of service were not merely *using* the data improperly, but had *no right to access the site at all*.²⁶⁶ As Judge Breyer summarizes in *Craigslis, Inc. v. 3Taps Inc.*: “[C]omputer owners have the power to revoke the authorizations they grant.”²⁶⁷

This accords with trespass precedent. Property owners can revoke the licenses they grant.²⁶⁸ The law should punish scraper owners that ignore targeted cease-and-desist requests.

²⁶¹ See Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372 (2018).

²⁶² *Id.* at 393.

²⁶³ *Id.* at 394.

²⁶⁴ See *Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (“[W]e continue to follow in the path blazed by *Brekka*, 581 F.3d 1127, and the growing number of courts that have reached the same conclusion. These courts recognize that the plain language of the CFAA ‘target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.’” (second alteration in original) (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008))).

²⁶⁵ See Sellars, *supra* note 261, at 398–400.

²⁶⁶ See *id.* at 402–04.

²⁶⁷ *Craigslis, Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1183 (N.D. Cal. 2013).

²⁶⁸ See *supra* notes 218–220 and accompanying text.

Similar warnings like IP blocks may also suffice, depending on the circumstances.²⁶⁹

But what about the general rule advocated by this article that brief, unambiguous pop-up messages can provide reasonable notice? Problems arise when applying this approach to web scrapers. Scrapers view websites differently than people.²⁷⁰ Unlike humans, scrapers often cannot distinguish such notice messages from other website content. Absent very specific, unusual, and likely error-prone programming, scrapers cannot parse these terms to distinguish permitted actions from prohibited actions. For this reason, courts should not normally treat click-thru messages as a notice to scrapers. (An exception may apply if the scraper was specifically designed to bypass or acknowledge the click-thru message.) But websites can use methods to provide unambiguous notice to scrapers. These include robots.txt usage and user-agent monitoring.

Robots.txt is a file placed at a website's root directory.²⁷¹ It follows a standard format that automated systems can understand.²⁷² It specifies what if any parts of the site automated systems can access.²⁷³ Because developers designed these conventions for automated systems to understand, they are unambiguous.²⁷⁴ Scraper designers are encouraged to abide by these rules.²⁷⁵ Tech companies adhere to them.²⁷⁶ Because they provide unambiguous notice, courts might reasonably treat a scraper that ignores them as operating without authorization.²⁷⁷

²⁶⁹ See *infra* Section III.B.

²⁷⁰ See Sellars, *supra* note 261, at 387.

²⁷¹ See M. Koster, *A Method for Web Robots Control* (Internet Eng'g Task Force, Working Paper, Dec. 4, 1996), <http://www.robotstxt.org/norobots-rfc.txt> [<https://perma.cc/HH4W-4HFN>].

²⁷² See *id.*

²⁷³ See *id.*

²⁷⁴ See Bellia, *supra* note 162, at 2215 (“The [robot exclusion] standard nevertheless serves as a means to provide technical but very specific notice about permissible uses of a system.”)

²⁷⁵ See KEVIN HEMENWAY & TARA CALISHAIN, SPIDERING HACKS 46 (2003) (“If you’re planning on releasing your scraper or spider into the wild, it’s important that you make every possible attempt to support robots.txt.”).

²⁷⁶ See Barry Schwartz, *Robots.txt Celebrates 20 Years of Blocking Search Engines*, SEARCH ENGINE LAND (June 30, 2014), <https://searchengineland.com/robots-txt-celebrates-20-years-blocking-search-engines-195479> [<https://perma.cc/B78J-9YAP>] (“All major search engines [in 1994], including WebCrawler, Lycos and AltaVista, quickly adopted it; and even [twenty] years later, all major search engines continue to support it and obey it.”).

²⁷⁷ Cf. Bellia, *supra* note 162, at 2215 (“The [robot exclusion] standard nevertheless serves as a means to provide technical but very specific notice about permissible uses of a system.”); Sellars, *supra* note 261, at 414 (discussing robots.txt and encouraging its further consideration in the CFAA context, but acknowledging that no courts “have gone so far as to suggest that it can be used to demonstrate authorized access to a website”).

Websites can also control access with user-agent monitoring. User-agents are text strings that contain identifying information, sent by a browser or scraper when connecting to a website.²⁷⁸ In response, websites can block the connection or send back specific error messages.²⁷⁹ Like robots.txt, these error messages follow unambiguous programming conventions. They include “401 Unauthorized” and “403 Forbidden.”²⁸⁰ Scrapers need not always provide an honest user-agent string. There are legitimate reasons—like quality-control testing—why someone might provide a spoofed (false) user-agent string. But if a scraper receives an Unauthorized or Forbidden message, then modifies the user-agent string to bypass that message, courts should consider their access without authorization.

Robots.txt and HTTP error messages provide owners with certain unambiguous conventions to communicate to scrapers that they lack CFAA authorization. But it should give anyone pause that “a tremendous number of [CFAA opinions involving web scrapers] concern claims brought by direct commercial competitors or companies in closely adjacent markets.”²⁸¹ The CFAA should not provide companies with a tool to lock out their competitors in ways that hurt the free market. For example, by preventing bots from surveying comparable prices, companies keep prices artificially high.²⁸² Executive agencies like the FTC and DOJ could punish scraper exclusion as unfair competition or an antitrust violation. Alternatively, Congress could craft a safe harbor that exempts scraping from the CFAA.

²⁷⁸ See *User-Agent*, MOZILLA, <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent> [<https://perma.cc/WH22-B9RL>] (“The User-Agent request header contains a characteristic string that allows the network protocol peers to identify the application type, operating system, software vendor or software version of the requesting software user agent.”); see also *QVC, Inc. v. Resultly, LLC*, 99 F. Supp. 3d 525, 530 (E.D. Pa. 2015) (“A user agent is a ‘string’ that is passed by a browser or other device, to a website, to identify what software is being used by that device to access the site.”).

²⁷⁹ See Jeff Starr, *Example of a Spoofed Search Engine Bot*, PERISHABLE PRESS, <https://perishablepress.com/spoofed-search-engine-bot/> [<https://perma.cc/FF6J-H45F>] (explaining how to review user agent and related information and block bots).

²⁸⁰ *10 Status Code Definitions*, W3C, <https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html> [<https://perma.cc/6VV3-HBNL>].

²⁸¹ Sellars, *supra* note 261, at 390 (footnote omitted).

²⁸² Some companies sell technical tools to filter and block scrapers, and they freely admit that scrapers generally pull down prices overall, which they want to avoid. See, e.g., Elias Terman, *Five Ways Your Competition Is Using Price Scraping Bots on Your E-Commerce Site*, DISTIL NETWORKS, <https://resources.distilnetworks.com/all-blog-posts/price-scraping> [<https://perma.cc/JYB7-WSJE>] (“[B]ad actors seek to scrape information from legitimate online retail sites to gain product and pricing intelligence that can be used to undercut their pricing or position against their offerings.”).

3. The IP-Blocked User

IP Address blocking also makes regular appearances in CFAA cases. “IP Address blocking is a security measure that prevents a connection between a specific or group of IP addresses and a mail, web or Internet server.”²⁸³ Websites use IP blocking to exclude undesirable visitors.²⁸⁴ Unfortunately, blocking messages frequently provide no real information to the user. And the IP addresses on which blocks operate can refer to multiple computers or change over time.²⁸⁵ This means that more people than intended could get hit with a block.²⁸⁶ Alternatively, visitors can “circumvent” blocks without realizing it.

Courts generally hold that IP address blocks provide some evidence demonstrating that users are without authorization.²⁸⁷ This cuts both ways; when a website owner files a CFAA complaint without terminating the offending accounts or blocking their IP addresses, that indolence undermines the owners’ claims.²⁸⁸

Others have been more reticent about punishing IP block evaders. Jamie Williams at the Electronic Frontier Foundation puts her position bluntly: “How Does Ignoring a Cease and Desist Letter and an IP Address Block Add Up to a Computer Break-

²⁸³ *IP Address Blocking*, TECHOPEDIA, <https://www.techopedia.com/definition/3991/ip-address-blocking> [<https://perma.cc/FK5D-LW2B>].

²⁸⁴ See Kerr, *supra* note 13, at 1168–69 (“To be sure, an IP block indicates that the computer owner does not want at least someone at that IP address to visit the website.”).

²⁸⁵ See *id.* at 1168 (“For some users, turning on and off their modems at home will lead their IP addresses to change.”).

²⁸⁶ See *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1068 n.5 (9th Cir. 2016) (“[E]ven if [a blocked user] does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user’s roommate or co-worker.”).

²⁸⁷ See, e.g., *Power Ventures*, 844 F.3d at 1067 (“Facebook then imposed IP blocks in an effort to prevent Power’s continued access. The record shows unequivocally that Power knew that it no longer had authorization to access Facebook’s computers, but continued to do so anyway.”); *CouponCabin LLC v. Savings.com, Inc.*, No. 2:14-CV-39-TLS, 2017 WL 83337, at *3 (N.D. Ind. Jan. 10, 2017) (“Plaintiff alleged that . . . Defendants knowingly and intentionally circumvented the Plaintiff’s security measures after it blocked their access from certain cloud computing/internet service providers . . . [This] would have been sufficient to give the Defendants constructive notice that they were without authorization . . .”); *Oracle USA, Inc. v. Rimini St., Inc.*, 191 F. Supp. 3d 1134, 1149 (D. Nev. 2016) (IP blocking put defendants “on notice that their conduct was improper”); *Craigslist, Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013) (“Craigslist affirmatively communicated its decision to revoke 3Taps’ access through its cease-and-desist letter and IP blocking efforts.”); see also *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1062–63, 1069–70 (N.D. Cal. 2000) (citing repeated blocks and warnings from eBay as supporting trespass case).

²⁸⁸ See *Ticketmaster LLC v. Prestige Entm’t, Inc.*, 306 F. Supp. 3d 1164, 1175–76 (C.D. Cal. 2018) (“Ticketmaster’s Complaint is wholly devoid of any allegations suggesting that Ticketmaster took steps to prevent Defendants from future access. For example, Ticketmaster did not allege that they shut down Defendants’ accounts or attempted to block their IP addresses.”).

In?”²⁸⁹ This position proceeds from an incorrect assumption. Despite its anti-hacking origins, the CFAA prohibits more than break-ins. It prohibits access “without authorization” and it prohibits “exceed[ing] authorized access.” But we can fairly question whether an IP address block provides notice sufficiently unambiguous to revoke the presumed open access inherent in every website. Professor Orin Kerr thinks not, comparing bypassing an IP block to “bending your neck to see around someone who has temporarily blocked your view.”²⁹⁰

This article respectfully disagrees. Certainly, an IP address block standing *alone* should not suffice.²⁹¹ Often, IP blocks never get communicated to the website user.²⁹² Users might see a Connection Refused error, which can arise from numerous innocent causes.²⁹³ And while the website could modify the error to something more pointed,²⁹⁴ like “401 Unauthorized” or “403 Forbidden,”²⁹⁵ even this might not be enough. A reasonable user might conclude that the message is not targeted at him.²⁹⁶ Given the web’s technical realities, website owners cannot accurately aim IP blocks at a single, static target. For example, to prevent Aaron Swartz from downloading copyrighted journal articles, JSTOR “block[ed] all of MIT’s access for a few days.”²⁹⁷ This ban was neither aimed at every MIT student, nor would every MIT student be held liable for evading it. But Swartz had notice. He next escalated his actions by breaking into a basement wiring closet while covering his face to evade cameras.²⁹⁸

IP address blocks should put others on notice. Are they enough standing alone? No. But combined with other signals—certainly a cease-and-desist letter, perhaps a click-thru or prominent homepage message referring to disallowed activities—

²⁸⁹ Williams, *supra* note 169, at 429.

²⁹⁰ Kerr, *supra* note 13, at 1168.

²⁹¹ *Power Ventures*, 844 F.3d at 1068 n.5 (“Simply bypassing an IP address, without more, would not constitute unauthorized use.”).

²⁹² *See id.* (“Because a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked.”).

²⁹³ *See Sellars, supra* note 261, at 405–06 (“The website might be down due to a server error or technical bug with the user’s ISP. It might instead be due to a site-imposed block—in which case the next attempt to load the page is grounds for CFAA liability.”).

²⁹⁴ *See* Damon, *Customizing Cloudflare Error Pages*, CLOUDFLARE, (Aug. 28, 2019, 5:16 AM), <https://support.cloudflare.com/hc/en-us/articles/200172706-How-do-I-customize-Cloudflare-error-pages> [<https://perma.cc/CS2D-ZWKM>] (showing how to customize pages appearing for IP-blocked users).

²⁹⁵ *10 Status Code Definitions, supra* note 280.

²⁹⁶ *See Power Ventures*, 844 F.3d at 1068 n.5 (“[E]ven if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user’s roommate or co-worker.”).

²⁹⁷ KERR, *supra* note 244, at 11.

²⁹⁸ *See id.*

an IP block should reasonably communicate the explicit revocation expected by trespassing precedent.

4. The Terms of Service Violator

Terms of service are the internet user's *bête noire*—or would be, if anyone bothered to read them.²⁹⁹ Courts and scholars have regularly criticized using them as a source for CFAA deauthorization.³⁰⁰ As suggested above in discussing the use contract approach, trespass precedents resolve this relatively easily.³⁰¹ We should only treat trespasses as trespasses, not bad behavior.³⁰² Prosecute Lori Drew for harassment. Castigate her in the court of public opinion. But she isn't a hacker.

C. Ignoring an Owner's Wishes

This article offers one final and controversial suggestion: In some circumstances, trespass norms *might* override even an owner's express prohibitions. The inquisitive reader might ask how this could happen, when the statute clearly requires "authorization," and the article earlier emphasized that norms can guide but not supplant statutory text.³⁰³

Authorization is really a conclusion that flows from the owner's consent, which is a tricky topic. There are actually *two* kinds of consent:

Factual consent . . . is a state of the world; it exists when a person acquiesces in conduct by another that affects her. But legal consent . . . is a conclusion of law: it exists where the law decides to treat a person as acquiescing in another's conduct. Legal consent is defined in terms of factual consent, but factual consent is neither necessary nor sufficient for legal consent.³⁰⁴

When factual consent is not necessary for legal consent—in other words, when we ignore what the owner thinks—we still

²⁹⁹ See *infra* Section III.C.

³⁰⁰ See *infra* Section III.C.

³⁰¹ See *supra* Section III.B.

³⁰² See 2 WILLIAM BLACKSTONE, COMMENTARIES *169 (“[A] bare nonfeasance, as not paying for the wine he calls for, will not make him a trespasser: for this is only a breach of contract, for which the taverner shall have an action of debt or *assumpsit* against him.”); Goldfoot & Bamzai, *supra* note 13, at 1495 (“[F]or a violation of an express or implied prohibition on entry to constitute a criminal trespass, it must advance the rationale for the crime of trespass.”).

³⁰³ See *supra* notes 175–177, 200 and accompanying text.

³⁰⁴ James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1503 (2016).

have authorization. But the authorization flows from the law, not from the owner.³⁰⁵

1. The Public Protector

In rare circumstances, using a system without authorization may prevent a worse harm. The WannaCry worm provides a good example. This particularly vicious worm spreads quickly, “locking up critical systems like the UK’s National Health Service, a large telecom in Spain, and other businesses and institutions around the world.”³⁰⁶ The worm’s designers built in a kill switch; when a website with a domain name composed of particular gibberish went live, the worm would stop propagating.³⁰⁷ With quick thinking and some luck, a security researcher registered the domain name.³⁰⁸ The worm stopped.³⁰⁹ So far so good. But what if the worm would instead stop when a major website went *down*? And what if the website owner balks? This situation seems tailor made for the necessity doctrine, which imputes consent where required to avoid “public disaster.”³¹⁰ Indeed, the necessity defense under common law appeared to require even less justification, explaining that “[a] person may enter the premises of another to save a life; to rescue an animal in danger; to abate a nuisance; or to escape assault or injury.”³¹¹

From its roots in the common law,³¹² the necessity doctrine has found acceptance in at least some states (though

³⁰⁵ See, e.g., BIGELOW, *supra* note 70, at 221–25 (“The term ‘license of the law’ has reference to cases in which a permission is given regardless of the will of the owner or occupant, and includes all other cases in which the entry or taking possession was lawful. . . . The law licenses an entry upon the land of another, or the taking possession of another’s goods, in many cases; and in these the license cannot be revoked by the party affected.”); 2 WATERMAN, *supra* note 70, at 182–83 (“There are cases where an authority to enter is given by law; as, to execute legal process; to distrain for rent; to a landlord or reversioner to see that his tenant does no waste, and keeps the premises in repair according to his covenant or promise; to a creditor, to demand money payable there; or to a person entering an inn for the purpose of getting refreshment.”).

³⁰⁶ Lily Hay Newman, *How an Accidental ‘Kill Switch’ Slowed Friday’s Massive Ransomware Attack*, WIRED (May 13, 2017), <https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/> [<https://perma.cc/6Q4X-RZRM>].

³⁰⁷ See *id.*

³⁰⁸ See *id.*

³⁰⁹ See *id.*

³¹⁰ RESTATEMENT (FIRST) OF TORTS § 196 (AM. LAW. INST. 1934) (“One is privileged to enter land in the possession of another, if necessary, or if it reasonably appears to the actor to be necessary, for the purpose of averting a public disaster.”); see also *id.* § 262 (“One is privileged to use or otherwise intentionally intermeddle with a chattel in the possession of another when such intermeddling is or is reasonably believed to be necessary for the purpose of averting a public disaster.”).

³¹¹ ARCHER, *supra* note 70, at 183.

³¹² See, e.g., *id.* at 182 (“Although the law jealously guards the right of an individual to undisturbed possession of real estate, yet there are circumstances when for the welfare of the public the law gives permission to enter his premises, even against his consent. This is called license of law.”).

how many remains debatable).³¹³ But substantial doubt arises about whether the federal common law has adopted a general necessity defense. Though the Supreme Court has taken up the issue several times, it has never squarely resolved it, and the lower courts have split.³¹⁴ Nonetheless, assuming the defense's availability, the Ninth Circuit's definition is typical, requiring a defendant satisfy four elements: "(1) they were faced with a choice of evils and chose the lesser evil; (2) they acted to prevent imminent harm; (3) they reasonably anticipated a direct causal relationship between their conduct and the harm to be averted; and (4) they had no legal alternatives to violating the law."³¹⁵

A choice-of-evils analysis will necessarily depend on the scope and severity of the worm being combated and the methods necessary to stop it. But, taking WannaCry as an example, it is likely the lesser evil to take down one website rather than permit a worm to cripple national health care systems.³¹⁶ Security researchers would act to prevent its spread and reasonably anticipate that their actions would have that result. But they run into a roadblock with legal alternatives. In most situations, they could negotiate with the website owner, convince the website owner's host or ISP to sever their connection, or involve law enforcement. Nonetheless, one can certainly envision circumstances where a researcher could satisfy all four elements.

Note that this approach never alters the factual definition of "authorization." Instead, it interposes a different doctrine—necessity—which concludes that the perpetrator should not receive punishment for their crime. By contrast, cyber-tenants ejected from a system might suggest that owners can't always withdraw authorization at a whim.

³¹³ See Adav Noti, Note, *The Uplifted Knife: Morality, Justification, and the Choice-of-Evils Doctrine*, 78 N.Y.U. L. REV. 1859, 1861 (2003) ("Most states recognize the justification defense in a form similar to the statutes proposed by the Model Penal Code." (footnote omitted)). *But see* Michael H. Hoffheimer, *Codifying Necessity: Legislative Resistance to Enacting Choice-of-Evils Defenses to Criminal Liability*, 82 TUL. L. REV. 191, 196 (2007) ("[M]ost states do not codify the necessity defense in any form.").

³¹⁴ See Stephen S. Schwartz, Comment, *Is There a Common Law Necessity Defense in Federal Criminal Law?*, 75 U. CHI. L. REV. 1259, 1259 (2008) ("[T]he question of whether the [necessity] defense exists in modern federal criminal law remains an open question. The Supreme Court has avoided deciding the question squarely, and lower courts have addressed it inconsistently.").

³¹⁵ *United States v. Schoon*, 971 F.2d 193, 195 (9th Cir. 1991).

³¹⁶ See Newman, *supra* note 306 ("WannaCry swept Europe and Asia quickly yesterday, locking up critical systems like the UK's National Health Service, a large telecom in Spain, and other businesses and institutions around the world, all in record time.").

2. The Unjustly Ejected

One final category is the unjustly ejected cyber-tenant. Trespass law traditionally forbids owners from using their right to exclude to acquire another's property. Assume, for example, you own a set of lockers and provide the public with free use to secure their possessions. You can bar future users and even shut down your service, forcing current users to promptly remove their possessions, but you can't simply confiscate them.³¹⁷ The same would apply to a private campground. If you invite hikers to park their RVs, you can kick them off whenever you want. But you can't use your exclusion right to prevent them from returning to the land to claim their RVs.³¹⁸

This principle flows from several sources. First, property ownership almost always involves the right to control that property. As Thomas Waterman wrote in his 1875 treatise, "[t]he right of property . . . draws after it the right of possession."³¹⁹ To effectuate that possessory right without infringing on the *landowner's* right to control, the law resorts to a fiction. It determines that the landowner has consented even when the landowner insists they have done no such thing. It does so by making irrevocable the initial license granted by the landowner.³²⁰ In a thoughtful and important article, Professor James Grimmelmann links this concept of constructive consent with CFAA authorization.³²¹ He explains that a system

³¹⁷ See RESTATEMENT (FIRST) OF TORTS § 255 (AM. LAW INST. 1934) ("Upon termination of consent to the use or occupancy of a chattel in the possession of another, the actor is privileged to continue such use or occupancy so long as it is reasonably necessary to safely effect egress from or discontinuance of his use of the chattel or to remove his personal belongings therefrom.")

³¹⁸ See RESTATEMENT (FIRST) OF TORTS § 177 (AM. LAW INST. 1934) ("Upon termination or suspension of consent as to the presence on land of a thing which was placed there with the consent of the then possessor of the land to its removal thereafter, one entitled to the immediate possession of the thing is privileged . . . to be on the land for the purpose of removing the thing in a reasonable manner and with reasonable promptness, unless he knew or had reason to know the time of such termination or suspension a reasonable period in advance thereof."); BIGELOW, *supra* note 70, at 221–25 ("The term 'license of the law' has reference to cases in which a permission is given regardless of the will of the owner or occupant A fourth case is where goods have been placed upon a man's land under a tenancy [Generally,] the owner may go upon the premises and take them. For example: The plaintiff lets premises to the defendant at will, on the terms that the defendant shall have reasonable time to remove his goods, after notice to quit. The defendant enters accordingly after termination of the lease, to get his goods, against the plaintiff's refusal to allow him. This is no breach of duty." (footnotes omitted)).

³¹⁹ 2 WATERMAN, *supra* note 70, at 207.

³²⁰ See *id.* at 206–07 ("[I]f the owner of personal property, by virtue of a contract with, or the permission of the owner of land, places his property on the land, the license to enter upon it for the purpose of removing the property, is irrevocable.")

³²¹ See Grimmelmann, *supra* note 304, at 1514 ("The most important species of imputed consent for CFAA purposes is *constructive* consent, in which S is irrebuttably regarded as having consented to conduct *x* by virtue of having consented to some other conduct *y*.")

owner irrefutably consents to certain conduct, e.g., removing items, by consenting to certain other conduct, e.g., granting access in the first place.³²²

While this idea has garnered little attention in CFAA litigation, it seems only a matter of time, because relevant fact patterns regularly recur. The most common seems to be the work laptop that gets wiped.³²³ If done after termination to cover up workplace misconduct, then that might be a CFAA violation. But what if it's done to cover up an unfortunate but not criminal web browsing history? While the laptop belongs to the employer, some files on it belong to the employee.³²⁴ Just like an employer can't simply confiscate the employee's coffee mug and family photos from the physical desk, it seems reasonable that the employee should get an irrevocable license to clean up their personal files from their virtual desk without risking criminal penalties.

CONCLUSION

The law has always benefited from forebears' wisdom and slow, incremental refinement over the centuries. Writing in 1818 on bailment law, Sir William Jones drew not only from English sources, but Jewish, Athenian, Roman, Visigoth, ancient Briton, and Indian.³²⁵ As he explained: "[I]n questions of *rational* law, no cause can be assigned, why we should not shorten our own labor by resorting occasionally to the wisdom of ancient jurists, many of whom were the most ingenious and sagacious of men."³²⁶

The analogies between physical and electronic trespass will not always be perfect. But as Professor Richard Epstein suggested, the similarities are greater than the differences, and cyberspace's brave new world "is neither as brave nor as new as it first appears."³²⁷ The endless splits in CFAA jurisprudence have persisted long enough. Even if Congress tried to clarify the

³²² *See id.*

³²³ *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

³²⁴ If an employee has signed an explicit agreement that any files created or placed on the laptop become the employer's property, then obviously they would be the employer's property.

³²⁵ SIR WILLIAM JONES, AN ESSAY ON THE LAW OF BAILMENTS 12, 13, 130, 131, 132 (1818), <https://books.google.com/books?id=0hgzaAAAIAAJ>.

³²⁶ *Id.* at 16.

³²⁷ Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 87–88 (2003) ("In some circumstances we do need to modify traditional right situations to deal with new forms of property rights. But that proposition is not some unarticulated but universal truth. Sometimes the old analogies work just fine. So long as we keep our eye on the ball, we do not have to be fearful of the imagined consequences that will follow by taking the older rules of trespass and carrying them over to the brave new world of cyberspace, which, when all is said and done, for legal purposes at least, is neither as brave nor as new as it first appears.").

ambiguous statutory terms, doubt would remain about applying the law to concrete cases.³²⁸ It is past time to build a broad, durable structure for future use. Trespass law provides the foundation. Hopefully, this article has laid the first course of brick.

³²⁸ Cf. Mayer, *supra* note 137, at 1661 (“[R]ecognizing 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.”).