A Trespass Framework for the Crime of Hacking

Josh Goldfoot & Aditya Bamzai***

ABSTRACT

Computer crime statutes prohibit accessing a computer without "authorization." In recent years, this element has attracted considerable controversy, with some courts expressing concern that "authorization" is so indeterminate that the Computer Fraud and Abuse Act ("CFAA") is void for vagueness. This Article argues that "authorization" under the CFAA has the same meaning as authorization under criminal physical trespass laws. This approach is more straightforward than the alternatives currently offer, and it aligns with Congress's announced intention to bring physical trespass law to computer networks. Although interpreting "authorization" under the CFAA can be difficult, near-identical difficulties also arise in the context of physical trespass. As a result, questions under the CFAA can be resolved by looking to the resolution of similar questions in the context of physical trespass. In addition, because both physical trespass and the CFAA require proof that the defendant knew his access was unauthorized, the merits of a void-for-vagueness challenge to computer trespass rise and fall with the merits of a similar challenge to physical trespass. Given the pedigree of the latter, a constitutional challenge to the former seems questionable.

TABLE OF CONTENTS

---

* Principal Deputy Chief (Acting), Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice; Deputy Chief for Cyber Policy, National Security Division.

** Associate Professor of Law, University of Virginia School of Law.

The Authors would like to thank Divya Bamzai, Will Baude, Matthew Berry, Adam Hickey, Orin Kerr, and the other members of *The George Washington Law Review*'s 2015 Symposium.

INTRODUCTION

"Authorization" is the key element of criminal hacking statutes. Accessing or damaging a computer "without authorization" (or, sometimes, "exceeding authorized access") is an element in almost every offense defined in the federal Computer Fraud and Abuse Act ("CFAA").[1] Authorization is also the key element of criminal physical trespass. Intruding onto someone's property without authorization—or exceeding one's authorization—is an element of trespass in every known, functioning system of property rights. That parallel naturally prompts the following question: To what degree do the "authorization" rules governing computer trespass depart from the authorization rules governing physical trespass?[2]

This Article's answer to that question can be summarized simply: not much. The text, structure, and history of the CFAA all indicate that its "without authorization" term incorporates preexisting physical trespass rules. As Justice Jackson famously put the point, "where 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."[3] Applying that prin-

---

1 18 U.S.C. § 1030 (2012); *see also id.* § 1030(e)(6) (defining "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter").

2 *Compare* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1153–54 (2016) (arguing that applying the CFAA "requires translating concepts of trespass from physical space to the new environment of computers and networks" and that computer trespass "laws inevitably rest[ ] on the identification of proper trespass norms"), *with* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 527 (2003) (arguing that courts "have shown a remarkable lack of sensitivity" to the "the differences between the Internet and physical space in a variety of contexts").

3 Morissette v. United States, 342 U.S. 246, 263 (1952).

ciple to the CFAA means that the "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.

Recognizing the parallels between the crimes of physical and computer trespass leads to three important conclusions. First, courts should require proof of the three trespass elements before concluding that there is an access "without authorization" under the CFAA. The resulting test is principled, practical, and leads to sensible results. Second, because the tests for authorization to enter property and to access computers are so similar, the difficulties that courts and commentators have experienced in defining *computer* trespass *also* exist in defining *physical* trespass. The problems associated with precisely defining the limits of the "without authorization" element in the CFAA are not novel consequences of computer trespass, but are as old as the crime of trespass itself. Put slightly differently, it is harder to define physical trespass than has been previously supposed,[4] and it is easier to define computer trespass by reference to physical trespass than some courts have supposed. Third, a number of courts and commentators have expressed concerns that uncertainty over defining the term "without authorization" may render the CFAA unconstitutionally vague.[5] But appreciating the conceptual links between computer and physical trespass should put to rest any concern that the CFAA fails to give defendants fair notice of the conduct that it prohibits. The elements of computer trespass are so similar to those of physical trespass that the two crimes must stand or fall together against a vagueness challenge. In light of the common law pedigree of laws criminalizing physical trespass, it would be hard to imagine their invalidation under the void-for-vagueness doctrine. For the same reason,

---

4 *See, e.g.*, Ben Depoorter, *Fair Trespass*, 111 COLUM. L. REV. 1090, 1090–91 (2011) (observing that "most academic commentators agree that trespass doctrine is relatively uncomplicated," but disputing the conventional wisdom that physical "trespass stands solemnly as a seemingly tranquil and uncomplicated backwater of property law").

5 *See* United States v. Nosal, 676 F.3d 854, 866 (9th Cir. 2012) (en banc) ("Other sections of the CFAA may or may not be unconstitutionally vague or pose other problems."); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1659 (2003) [hereinafter Kerr, *Cybercrime's Scope*] (arguing that "[a] contract-based approach to authorization may also render unauthorized access statutes void for vagueness"); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1572 (2010) [hereinafter Kerr, *Vagueness Challenges*] (arguing that "courts should apply the constitutional void-for-vagueness doctrine to require narrow interpretations of unauthorized access in the CFAA").

computer trespass statutes defined by reference to the elements of physical trespass pass constitutional muster.

I. A CONCEPTUAL FRAMEWORK FOR UNDERSTANDING THE CFAA'S RIGHT TO EXCLUDE

The CFAA's principal prohibitions confer on computer owners the right to regulate who may access their computer, and what those accessers may do to it.[6] Those prohibitions are best understood as creating rights to exclude that are akin, in important respects, to comparable rights in property regimes. Such property rights, in the words of a seminal paper by the economist Harold Demsetz, "derive their significance from the fact that they help a man form those expectations which he can reasonably hold in his dealings with others."[7] They are intended "to internalize externalities when the gains of internalization become larger than the cost of internalization"—in, other words, to allow a property owner to "internalize" the fruits of his labors on the property, when the benefits of doing so outweigh the costs to society.[8] That is why new property rights often arise when "[n]ew techniques, new ways of doing the same things, and doing new things" lead to "harmful and beneficial effects to which society has not been accustomed."[9]

To put the point concretely, the arrival of computer networks allowed more efficient communication than before. But using the networks required investment in technology. It also prompted the development of self-help mechanisms, such as investment in security techniques to ensure that computers are not accessed by intruders. As Demsetz explains: "[i]ncreased internalization, in the main, results from changes in economic values, changes which stem from the development of new technology[,] and the opening of new markets."[10]

Those new security techniques, however, may be inadequate to ensure optimal investment in new technology.[11] To supplement self-help mechanisms, governments can enact laws that prohibit "trespass" by giving individuals the right to "exclude" others—ranging from full-blown laws bestowing property rights to narrower laws creating a lim-

---

6 *See* 18 U.S.C. § 1030 (2012).

7 Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 347 (1967).

8 *Id.* at 350.

9 *Id.*

10 *Id.*

11 *See* Douglas Lichtman, *How the Law Responds to Self-Help*, 1 J.L. ECON. & POL'Y 215, 229–30 (2005).

ited right to exclude others.[12] The "development of [such] private rights permits the owner to economize on the use of those resources from which he has the right to exclude others."[13]

But there is a downside: when the right to exclude is granted to one party, "third parties must expend time and resources to determine the attributes of these rights, both to avoid violating them and to acquire them from present holders."[14] Just as physical trespass laws require pedestrians to discern where a sidewalk ends and a neighbor's lawn begins, the creation of exclusion rights for computer users runs the risk of imposing costs on internet users who may stumble into legal jeopardy. The situation is further complicated by the fact that "owners" with the right to exclude commonly want to exclude some parties while at the same time admitting others—with the distinction between the two sets of parties drawn through consensual side agreements rather than enacted law. The appropriate level of government protection requires a balance between the benefits provided by government trespass sanctions and the costs of enforcement, including costs innocent parties bear by unwittingly violating the new protections.

In the CFAA, Congress sought to strike the appropriate balance between the exclusion rights of computer owners and the costs imposed on casual network users by tying computer trespass to the law of physical trespass.[15] The CFAA allows owners to connect their computers to networks while preserving some control over what will happen as a result. The statute was passed during an era when computer users were slowly beginning to realize that the long-distance computer networks created during the 1970s could now be used against them.

---

12 *Id.*; *see also* Henry E. Smith, *Self-Help and the Nature of Property*, 1 J.L. ECON. & POL'Y 69, 94–104 (2005).

13 Demsetz, *supra* note 7, at 356; *see also id.* at 355 ("If a single person owns land, he will attempt to maximize its present value by taking into account alternative future time streams of benefits and costs and selecting that one which he believes will maximize the present value of his privately-owned land rights.").

14 Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 8 (2000) [hereinafter Merrill & Smith, *Optimal Standardization*]; *see also id.* at 26–34; Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 359, 387 (2001) (noting that, because "property rights create duties that attach to 'everyone else,'" they can "impose[ ] an informational burden on large numbers of people" and "[t]o avoid violating property rights, a large and indefinite class of dutyholders must know what constraints on their behavior such rights impose").

15 *Cf.* Merrill & Smith, *Optimal Standardization*, *supra* note 14, at 58 (arguing that "legislated changes in property forms produce information to third parties at less cost than judicially mandated changes").

"[E]very computer which is connected to a modern computer network can be reached from any of the 100 million telephones in the United States," testified a witness at a House hearing in 1983, but "[i]t is this very capability which has also enabled the recent flurry of electronic trespassing incidents."[16] Yet, according to the 1984 House Report, "traditional legal machinery . . . in many cases may be ineffective against unconventional criminal operations. Difficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft."[17]

To solve that problem, the CFAA established that "trespassing" violated computer owners' rights.[18] The 1986 House Report equated hackers to "trespassers, just as much as if they broke a window and crawled into a home while the occupants were away."[19] When the statute was amended in 1996, the accompanying Senate Report expressly drew the parallel with common law trespass by noting that the CFAA "criminalizes all computer trespass."[20] And when courts began to interpret the CFAA's terms, they viewed its "without authorization" language through a physical trespass framework, relying on the general principle that "[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."[21] In one well-

16 H.R. REP. NO. 98-894, at 10 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3696.

17 *Id.* at 9.

18 Kerr, *supra* note 2, at 1153–54 (describing statutes like the CFAA as "computer trespass statutes" that apply the same "concepts of trespass from physical space to the new environment of computers and networks").

19 H.R. REP. NO. 99-612, at 5–6 (1986).

20 S. REP. NO. 104-357, at 11 (1996).

21 Field v. Mans, 516 U.S. 59, 69 (1995) (quoting Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 739 (1989)). To be sure, there are exceptions to this general principle. As one statutory interpretation treatise puts it, the question raised where Congress incorporates a common law term can be framed as whether courts should "identify [the term's] meaning simply by reference to" a general common law understanding "at the time that the federal statute was enacted," or rather "devise a statute-specific definition of the term that is influenced more by the apparent purposes behind the federal statute" than by background principles. CALEB NELSON, STATUTORY INTERPRETATION 599 (2011). A paradigm illustration of the more policy-driven approach is the Supreme Court's opinion in *NLRB v. Hearst Publications, Inc.*, 322 U.S. 111 (1944), discussed for this proposition in NELSON, *supra*, at 613–23. In *Hearst*, the Court rejected the argument that the meaning of the statutory term "employee" "must be determined by reference to common-law standards" that "the courts have applied in distinguishing between 'employees' and 'independent contractors' when working out various problems unrelated to the . . . purposes and provisions" of the National Labor Relations Act, which was the statute at issue in the case. *Hearst*, 322 U.S. at 120. "It will not do," the Court reasoned, "to import wholesale the

known example, the Second Circuit understood the term "without authorization" as being "of common usage, without any technical or ambiguous meaning."[22] But although these cases correctly recognized the connection between the CFAA and physical trespass, they failed to specify—and indeed, courts have yet to specify—the elements of physical trespass that the CFAA incorporates.

II. THE MEANING OF "AUTHORIZATION" UNDER THE CFAA

Under the CFAA, "authorization" (or exceeding authorization) to access a computer,[23] or "authorization" to "cause damage" to a computer,[24] is equivalent to authorization to enter property under criminal trespass law. By extension, the three elements that have traditionally been required to establish unauthorized entry into property are also necessary to establish unauthorized access to a computer under the CFAA. Those elements are: (1) the entry (or access) violates an express or implied prohibition; (2) the violator knew, or should have known, of the prohibition's existence; and (3) the prohibition is material or related to the underlying policy of trespass.

A. *Element 1: The Computer's Owner Objectively Prohibited Access, Express or Implied*

The CFAA incorporates physical trespass's requirement that a computer owner manifest an express or implied prohibition on access. In the case of physical trespass, express prohibitions may be easy to spot, such as the traditional "no trespassing" sign available at most local hardware stores. But they may not be, such as a "no trespassing" sign obscured by overgrown shrubs. The same is true of implied prohibitions. A straightforward implied prohibition is a lock on a front door, which tells a passerby as surely as a "no trespassing" sign that entry is not permitted. A slightly less straightforward implied

---

traditional common-law conceptions" into the statutory scheme. *Id.* at 125. *Hearst*'s approach on this issue, however, represents a distinct minority position on how to interpret terms familiar from the common law. *See* NELSON, *supra*, at 613–23.

22 United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991); *see* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (citing *Morris* and finding that "without authorization" is a non-technical term); United States v. Nosal (*Nosal II*), 828 F.3d 865, 876–77 (9th Cir. 2016) (same).

23 The difference between acting without authorization and in excess of authorization has been described as "paper thin" and, at any rate, is not central to this Article's thesis. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); *see* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (citing *Citrin* for the proposition that the distinction is "arguably minute").

24 18 U.S.C. § 1030(a)(5)(A) (2012).

prohibition is the custom that express permission to enter a business ordinarily does not include permission to enter the private back room and to rifle through desk drawers.

The latter examples show how express and implied prohibitions can interact in technically confusing, but practically intuitive, ways. An express authorization ("come into my restaurant") comes with implied limitations. An implied invitation to enter (a neon sign advertising a "restaurant" hanging above a street doorway) may be trumped by express or implied prohibition ("you can't enter because we have no open tables" or a simple lock on the door).

To the extent that a rule may be gleaned from the many different settings in which these issues are presented, it is this: express trumps implied.[25] Where permission may be impliedly prohibited ("you can't enter my house through an open window"), express permission allows it ("come on in that way, if you must"). By the same token, where permission may be impliedly given, it can be expressly revoked. The intent of the property owner, objectively manifested, governs authorization.

The same set of rules holds true for the CFAA. The owner of a computer may impliedly permit access to the computer, for example by running a mail server.[26] Authorization, also, can be limited and selective. Just as a store might welcome all members of the general public except for shoplifters specifically told they may not return,[27] a computer owner can limit access to only some users, and then limit what they may do with the computer.[28] For example, in *United States v. Phillips*,[29] the Fifth Circuit held that though the defendant "was authorized to use his UT [University of Texas] email account and engage in other activities defined by UT's acceptable computer use policy, he was never authorized to access" an application hosted on the same server that required login with "a valid Social Security number pass-

25 *See, e.g.*, 2 MODEL PENAL CODE § 221.2(2)(a) (AM. LAW INST., Official Draft and Revised Comments 1962) (punishing as a "Defiant Trespasser" a person who stays in a place when notice of trespass has been provided by "actual communication to the actor"); RESTATEMENT (SECOND) OF TORTS § 160 cmt. d (AM. LAW INST. 1965) (stating that "termination of consent creates a duty to remove" even when consent had originally been given).

26 Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011).

27 *See, e.g.*, People v. Ramnarain, 861 N.Y.S.2d 6, 8 (App. Div. 2008).

28 *See Nosal II*, 828 F.3d 865, 870 (9th Cir. 2016) (contending that employee "had no authority from [employer] to provide her password to former employees whose computer access had been revoked" and that an alternative interpretation "would render meaningless the concept of authorization").

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

word to which UT has affirmatively granted authorization."[30] As with other kinds of property, permission objectively withheld by a computer owner prohibits others from using the computer in the specified manner.

Trespass law can also provide a framework for determining *who* may authorize use of a computer: the company that owns the server, the company that leases space on that server to publish a website, a user of that website, or someone else entirely? In the case of physical trespass, a property owner may authorize access to property by a single user, or class of users, while limiting the right of those users to authorize *others* to access the property.[31] Likewise, in the case of computer trespass, the ability to authorize access to a computer originates with the person who owns the computer, but that authority can be delegated—with the scope of one user's ability to consent to use by another dependent on the scope of the authority delegated by the owner. A computer owner can thus choose not only to authorize users, but to delegate to those users the right to authorize others.[32] An example of such a delegation is Netflix's agreement to grant its customers a limited right to share their passwords with others: "[a]s long as they aren't selling them, members can use their passwords however they please."[33] Yet it goes too far to say, in every case, that "the permission of *either* the system owner *or* a legitimate account holder [that is, a user]" is sufficient to authorize access.[34] Just as owners of physical property can control the scope of the delegation to property users—granting a limited scope of authority barring those users from granting permission to authorize others—so too computer owners may authorize access to a user while prohibiting that user from authorizing access by the rest of the world.

---

30 *Id.* at 220–21.

31 RESTATEMENT (SECOND) OF TORTS § 891 (AM. LAW. INST. 1979).

32 *Cf.* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1077 (9th Cir. 2016) (reasoning that a party "reasonably could have thought that consent from *Facebook users* . . . was permission . . . to access *Facebook's* computers").

33 Kim LaCapria, *Sharing Netflix Passwords Hasn't Become a Felony*, SNOPES (July 12, 2016), http://www.snopes.com/2016/07/12/sharing-netflix-passwords-hasnt-become-a-felony/. By contrast, the legal principle that "the permission of *either* the system owner *or* a legitimate account holder" may authorize access, notwithstanding the scope of the delegation to the account holder, *see Nosal II*, 828 F.3d at 891 (Reinhardt, J., dissenting), would depart from the background understanding permitting property owners to control the scope of the delegation to users.

34 *Nosal II*, 828 F.3d at 891 (Reinhardt, J., dissenting).

B. *Element 2: The Defendant Knew or Should Have Known of the Express or Implied Access Prohibition*

In a similar vein, the CFAA parallels criminal trespass law's intent requirement. Most states criminalize physical trespass only when the defendant knew, or should have known, his entry onto the property was unauthorized.[35] This "knowledge requirement is designed primarily to exclude from criminal liability both the inadvertent trespasser and the trespasser who believes that he has received an express or implied permission to enter or remain."[36]

Congress expressly wrote an equivalent rule into the CFAA's "without authorization" elements. For example, one of the CFAA's most frequently charged provisions, § 1030(a)(2)(C), conditions liability on the defendant "*intentionally* access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[37] The word "intentionally" must modify both "access" and "without authorization" because of the "presumption [that] . . . a scienter requirement should apply to each of the statutory elements that criminalize otherwise innocent conduct."[38] As the 1986 House Report put it, the "intentionally" standard was "meant to focus Federal criminal prosecutions . . . on those who evince a clear intent to enter, without authorization, computer files belonging to another."[39]

Thus, to prove a defendant is liable or culpable under the CFAA, the plaintiff or prosecution must prove that the defendant not only accessed the computer without authorization, but also knew, or should have known, of facts that would establish his access was unauthorized.

There are at least three ways to do so.

---

35 *See* 75 AM. JUR. 2D *Trespass* § 151 (2007) ("[T]he common requirement of criminal trespass offenses is that the actor be aware of the fact that he is making an unwarranted intrusion, and, in general, criminal trespass statutes require that the trespass be knowingly committed." (footnote omitted)); 3 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 21.2(c) (2d ed. 2003); *see also, e.g.*, 2 MODEL PENAL CODE § 221.2 cmt. 2(c) (AM. LAW INST., Official Draft and Revised Comments 1962) ("knowing that he is not licensed or privileged to do so"). By contrast, the civil tort of trespass does not require intent. 87 CORPUS JURIS SECUNDUM *Trespass* § 4 (2010).

36 Herd v. State, 724 A.2d 693, 701 (Md. Ct. Spec. App. 1999) (quoting 2 MODEL PENAL CODE § 221.2 cmt. 2(a) (AM. LAW INST., Official Draft and Revised Comments 1962)).

37 18 U.S.C. § 1030(a)(2)(C) (2012) (emphasis added).

38 United States v. X-Citement Video, Inc., 513 U.S. 64, 72 (1994) (citing Morissette v. United States, 342 U.S. 246 (1952)). *But see* United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) ("We adopt the reasoning of the *Morris* court and hold that the computer fraud statute does not require the Government to prove that the defendant intentionally damaged computer files.").

39 H.R. REP. NO. 99-612, at 10 (1986).

1. *Code-Based Restrictions*

First, if the computer owner attempted to configure his computer to prevent or limit some kind of access, and the defendant knows about that attempt, then the defendant knows that kind of access is unauthorized. Code-based restrictions are attempts to enforce an owner's desire to limit authorization, through the use of software or other computer configuration. Code that demands a password before accessing an email account is one example.

Code-based restrictions are examples of the self-help mechanisms alluded to in the discussion of exclusion rights above[40]: the computer owner's attempt to internalize the cost of excluding others. When they work as intended, code-based barriers are better than analogous fences and walls: if a computer is properly configured to exclude access, then it is impossible to get in. But hacking would not be possible—and the CFAA would not be necessary—if it was both possible and cost-effective for computer owners to perfectly implement their intended authorization restrictions in code. Imperfect, insecure code leads to many unauthorized intrusions.[41]

Imperfect code-based restrictions are nonetheless relevant to the CFAA because the unsuccessful *attempt* to restrain access might still *communicate* to defendants the owner's (frustrated) intent to exclude. To communicate that intent effectively, code-based barriers need not be insurmountable barriers. A web server that relies on an easily forged "user agent" string to block conventional browsers and permit access only from a custom browser application, for example, still communicates an intent to limit access, even though an attacker could forge a user agent string.[42] So, too, does a "CAPTCHA"—code that tests whether the user is human by requiring the user to recognize text that would be difficult, but not impossible, for a computer to recognize.[43] Though a CAPTCHA can be defeated, it nonetheless communicates the owner's intent to block automated access.[44]

---

40 *See supra* notes 6–10 and accompanying text.

41 *See* U.S. Dep't of Homeland Sec., *Top 30 Targeted High Risk Vulnerabilities* (May 6, 2015), https://www.us-cert.gov/ncas/alerts/TA15-119A [https://perma.cc/MK3J-MPVU] ("Cyber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations.").

42 *See* United States v. Auernheimer, 748 F.3d 525, 530 (3d Cir. 2014) (describing such a technique).

43 *See* Kerr, *supra* note 2, at 1169–70.

44 *See id.* at 1169 (noting that "[t]he purpose of the CAPTCHA . . . is to allow humans in but to block computer 'bots' that can make thousands of automated requests at once," but nonetheless concluding automated access that bypasses a CAPTCHA is not unauthorized).

One way to think about the issue is that it is not really accurate to speak of "circumventing" a code-based barrier. As Professor Grimmelmann has noted, if a computer's flawed code permits an attacker to access something, then that code arguably was not a barrier to access in the first place.[45] For example, suppose a programmer hopes to write a simple password barrier: the code asks for a password, and permits access if it is correct. But, the code has a flaw—it suffers from what is known as a SQL injection vulnerability.[46] Because of the vulnerability, the code permits access if one enters the correct password, *or* if one enters a string ending with "' OR 1=1/*". Does that buggy code constitute a "code-based barrier" that demands a password but is "circumvented" when someone exploits the SQL injection vulnerability? Or, does that code constitute a more limited code-based barrier that is not "circumvented" by "' OR 1=1/* " but rather accepts either that or the password as correct?

The programmer's intent, objectively understood, should settle this question: although the code permits access two different ways, the second way was an accident, not an authorization. Users figure that out not from a "code-based barrier," but from intuitions about what the programmer meant to do. They know, in other words, that the imperfect password barrier was still meant to be a barrier, not because the code effectively enforced a restriction, but because the owner communicated the intent to restrict through the imperfect code.

Contrary to this analysis, some writers have placed enormous importance on code-based restrictions, going so far as to say that *only* those restrictions that were "code[d] . . . so that the particular user has a limited set of privileges on the computer," would be enforceable under the CFAA.[47] It is argued that the alternative—"contract-based" barriers—would base "criminal liability on violations of private computer use" policies, thus transforming "otherwise innocuous

---

45 *See* James Grimmelmann, *Computer Crime Law Goes to the Casino*, CONCURRING OPINIONS (May 2, 2013), http://concurringopinions.com/archives/2013/05/computer-crime-law-goes-to-the-casino.html ("In every interesting case, the defendant will have been able to make the program do something objectionable. If a program conveys authorization whenever it lets a user do something, there would be no such thing as 'exceeding authorized access.' Every use of a computer would be authorized.").

46 *See generally* William G.J. Halfond, Jeremy Viegas & Alessandro Orso, *A Classification of SQL Injection Attacks and Countermeasures*, *in* INT'L SYMPOSIUM ON SECURE SOFTWARE ENG'G (2006).

47 Kerr, *Cybercrime's Scope*, *supra* note 5, at 1644; *see also* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2258 (2004) ("Courts would better serve both the statutory intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access.").

behavior into federal crimes simply because a computer is involved."[48] But, the distinction between "code-" and "contract-" based restrictions was never so clear. As Lawrence Lessig noted, both the term of service, "[b]y using this site you agree not to use the print-screen command," and the JavaScript code that attempts to disable the print-screen command, are "just words, words on both sides."[49] Neither set of words prevents printing; circumventing the JavaScript barrier is only slightly harder than ignoring the contractual restriction. It is a mistake to attach enormous importance to code and no importance to other authorization restrictions.[50]

Focusing exclusively on code-based restrictions ignores relevant social and ethical contexts, yielding definitions of "authorized" that do not reflect common understandings of the term. Take the example of the 2003 Senate Judiciary Committee memo affair. After watching a system administrator perform some work on his computer, a Republican staffer discovered that he could access Democratic staffers' files without a password; he only had to access "My Network Places" and "Entire Network."[51] Thousands of sensitive, internal Democratic memos discussing strategy were downloaded, and some later leaked to the press.[52] The Sergeant at Arms investigated and suggested that charges under the CFAA were a possibility.[53]

One defender at the time argued that the Republican staffers had authorization to access the Democratic memos, because "[n]o one exceeds their authority when they log on and access files on their own computer's desktop. Democrats, in other words, were the ones who disclosed their own documents, which were in fact entirely unrestricted."[54] That argument proceeded directly from the flawed premise that code, alone, defines authorization: the lack of a code-based

---

48 United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc). Notably, the Ninth Circuit has rejected the argument that "the CFAA only criminalizes access where the party circumvents a technological access barrier." *Nosal II*, 828 F.3d 865, 878 (9th Cir. 2016).

49 Transcript of Lawrence Lessig, *Aaron's Laws - Law and Justice in a Digital Age*, CORRENTE (Feb. 19, 2013, 5:00 PM), http://www.correntewire.com/transcript_lawrence_lessig_on_aarons_laws_law_and_justice_in_a_digital_age.

50 *See* Kerr, *Cybercrime's Scope*, *supra* note 5, at 1651–52.

51 WILLIAM PICKLE, REPORT ON THE INVESTIGATION INTO IMPROPER ACCESS TO THE SENATE JUDICIARY COMMITTEE'S COMPUTER SYSTEM 22 (Mar. 4, 2004), https://www.judiciary.senate.gov/imo/media/doc/The%20Computer%20Report%20Testimony%20030404.pdf.

52 *Id.* at 9.

53 *See id.* at 59–60.

54 C. Boyden Gray, Letter to the Editor, *Faulty Judiciary Network: Let's Establish the Facts*, WALL ST. J. (Dec. 23, 2003, 12:01 AM), http://www.wsj.com/articles/SB107215138165655600.

barrier between Republican staffers and Democratic files means that Republicans were "authorized" to access Democratic files under the CFAA.

Yet, that meaning of "authorized" 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. Setting aside how the computers were configured, no one believed that anyone intended to authorize Republican staffers to access, read, and publish confidential memos between Democratic staffers and their senators. Senator Kennedy compared the incident to the Watergate scandal, and Senator Hatch—a Republican and the Committee's chairman—was "mortified" by "this improper, unethical, and simply unacceptable breach of confidential files."[55] To argue that the documents were "entirely unrestricted," or that Democratic staffers "disclosed their own documents" to Republican staffers,[56] ignores patterns of conduct, social norms, and other indicia of what people actually believed was permitted. The CFAA, a statute crafted to imitate trespass law,[57] embraces those considerations.

Code is important not because it defines authorization limits, but because it is a way to communicate the computer owner's intent to exclude or limit authorization. It is not the only way, but rather one form of "words" used to express intent.[58]

2. *Policies, Terms of Service, and Other Human-Language Restrictions*

A second way to prove that the defendant knew his access was unauthorized is to point to a clear and authoritative human-language notification that certain accesses are unauthorized. In other words, a defendant will know his access is not authorized if someone tells the defendant his access is not authorized. For example, conspicuous notices (such as "Only our employees may access this site") and cease-and-desist letters both communicate to users that their access to a website is unauthorized, even if the site is otherwise public and unsecured.[59] So long as there is sufficient proof that this notification

---

55 Charlie Savage, *GOP Downplays Reading of Memos*, BOS. GLOBE (Jan. 23, 2004), http://archive.boston.com/news/politics/us_senate/articles/2004/01/23/gop_downplays_reading_of_memos/.

56 Gray, *supra* note 54; *see also* Savage, *supra* note 55.

57 *See supra* notes 18–20 and accompanying text.

58 *See* Lessig, *supra* note 49.

59 *See* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1078 (9th Cir. 2016) (reasoning that "consent . . . received from Facebook users was not sufficient to grant continuing author-

reached the defendant, and that the defendant read it or otherwise knew of the access limitation it conveyed, the defendant's access contrary to these limitations was unauthorized.[60]

Human-language restrictions as a basis for CFAA liability have drawn considerable criticism. Several commentators argue that allowing authorization to hang on obscure, often unread website terms of service or employer rules fails to ensure fair notice under the Due Process Clause, because "regulated parties should know what is required of them so they may act accordingly." Thus, they argue, the CFAA should be held void for vagueness if liability turns on human-language rules.[61] One court expressed concern that users will not know what the rules are if they are not contained in enacted law.[62] Relatedly, in *United States v. Nosal*,[63] the Ninth Circuit held that "the CFAA does not extend to violations of use restrictions," because doing so could lead to terrifying results such as criminalizing lying on dating websites, or convicting children for using websites that authorize only adults to access them.[64]

The critical point, however, is that the very same issue can arise in the context of physical trespass. There, too, an express condition on entry into physical space might be contained in written text and might be vague or obscure. As noted above, property-rights scholars have long recognized that a consequence of granting the right to exclude is that third parties must expend time and resources to determine what the rules are.[65] The response of criminal trespass regimes has not been to eliminate the possibility that a property owner may limit entry subject to certain conditions, but rather to exclude inadvertent tres-

---

ization to access Facebook's computers after Facebook's express revocation of permission" through a "cease and desist letter" and "IP barriers"); *Nosal II*, 828 F.3d 865, 868–69 (9th Cir. 2016) ("[O]nce authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door."); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969–70 (N.D. Cal. 2013).

60 *See id.*

61 *See* United States v. *Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) ("Not only are the terms of service vague and generally unknown . . . but website owners retain the right to change the terms at any time and without notice."); Kerr, *Vagueness Challenges*, *supra* note 5, at 1572 ("In both cases [of violations of website terms of service and employer rules], the void-for-vagueness doctrine should force the conclusion that neither conduct is prohibited by the CFAA."); Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 752 (2013).

62 United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

63 United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

64 *Id.* at 861–63.

65 *See supra* note 14 and accompanying text.

passers from liability.[66] In other words, physical trespass laws criminalize conduct only when the defendant knew, or should have known, his entry onto the property was unauthorized.[67] Similarly, the CFAA requires proof not just that access was unauthorized, but that a defendant knew or should have known that his access was unauthorized.[68] In this respect, computer trespass poses an ancient analytical problem rather than a novel one. The solution to the problem is the same: the CFAA's mental-state requirement "blunts any notice concern" by requiring that the prosecution prove that the defendant had notice.[69]

Thus, the mental-state requirement tends to negate the possibility that obscure or vague access restrictions could form the basis for criminal liability. Consider, for example, concerns raised by the en banc Ninth Circuit in *Nosal* that an employer policy prohibiting a "nonbusiness purpose" use of a computer leaves it unclear whether using that computer to "check the weather" is authorized.[70] If "minor personal uses are tolerated," the court asked, "how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?"[71] That is exactly the point: if the employee is not on notice of when a policy withdraws authorization to access a work computer, then the CFAA does not punish that access because the employee lacked criminal intent.

Not every violation of a user agreement or employer policy results in intentional unauthorized access. For defendants to have notice of access restrictions, the terms must have unambiguously conditioned the right to "access" the computer on a particular promise or term. As one court found, "use" restrictions are not the same as "access" restrictions under the CFAA.[72] This distinction answers hy-

---

66 *See* 2 MODEL PENAL CODE § 221.2(1)–(2) (AM. LAW INST., Official Draft and Revised Comments 1962) (limiting the liability of inadvertent trespassers by imposing a "knowing" requirement).

67 *See id.*

68 *Cf.* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) ("when the user knows or reasonably should know that he or she is not authorized to access a computer").

69 Skilling v. United States, 561 U.S. 358, 412 (2010); United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009) ("[T]he Supreme Court 'has made clear that scienter requirements alleviate vagueness concerns.'").

70 United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

71 *Id.*

72 Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) ("Craigslist's TOU contain only 'use' restrictions, not true 'access' restrictions as the term is used in *Nosal*."); *see also Drew*, 259 F.R.D. at 467 ("It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization.").

potheticals about CFAA liability for violations of terms of use on dating sites and search engines. Although Match.com's membership agreement reads "[y]ou represent and warrant that all information that you submit upon registration is accurate and truthful," it does not say that access is withdrawn and the user becomes a trespasser if that promise is broken. Instead, the agreement suggests that the penalty is just "terminating or suspending the membership of such violators."[73] When well-written terms do withdraw authorization to "access," they say so: for example, Google's 2007 terms said, "[y]ou agree not to access (or attempt to access) any of the Services by any means other than through the interface that is provided by Google."[74]

3. *Social Norms*

A third (but not necessarily final) way to prove that the defendant knew his access was unauthorized is to show that social norms or conventions, with which the defendant was familiar, demand that conclusion.

As the Fifth Circuit noted in *United States v. Phillips*, "[c]ourts have . . . typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."[75] Some social norms authorize; others withdraw authorization.[76] For example, web servers, as a default rule, "inherently" authorize anyone to access them.[77] In *Phillips*, however, the court cited "the understanding of any reasonable computer user"—a norm, in other words—to hold that a brute-force attack of a website's authentication page was unauthorized.[78]

Social norms conceptually overlap with the common law notion of implied permission.[79] And as with physical property, implied permission to access a computer may be either expressly or impliedly negated.[80]

---

73 *Match.com Terms of Use Agreement*, MATCH.COM ¶ 9(a), (d) (Feb. 5, 2014), http://www.match.com/registration/membagr.aspx.

74 *Google Terms of Service*, GOOGLE.COM ¶ 5.3 (Apr. 16, 2007), https://www.google.com/intl/en/policies/terms/archive/20070416/.

75 United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).

76 *See* Kerr, *supra* note 2, at 1164–65.

77 *See id.* at 1161–62.

78 *Phillips*, 477 F.3d at 220; *see also* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580 (1st Cir. 2001) (accepting a district court finding that the defendant "used EF's website in a manner outside the 'reasonable expectations' of both EF and its ordinary users").

79 *See* Kerr, *supra* note 2, at 1151.

80 *See supra* Section II.A.

The key question is whether the social norms for computer trespass are relevantly different from the social norms of physical trespass. Under the CFAA, they are not. By incorporating the rules of physical trespass in the CFAA, Congress also incorporated the relevant norms of trespass. Suppose the opposite: that a court had the authority to announce a new "norm" that carves out the specific case from the scope of the CFAA's prohibition.[81] By rendering the analysis of the CFAA a case-by-case one, the interpretive approach would make it that much more difficult to treat like cases alike, thereby raising vagueness problems under the Due Process Clause.[82]

As discussed at the beginning of this Article, the key empirical question posed by trespass laws is the following: whether the greater internalization of benefits (and concomitant greater investment in computer technology) is outweighed by the costs imposed on third parties who must make efforts to inform themselves about legal rules and avoid trespassing on others' property.[83] In our common law system, the "social norms" of physical trespass have developed over centuries in an effort to reflect this fundamental empirical point.[84] From this perspective, the "social norms" framework is another way of expressing a crucial, ultimately *empirical*, question: in the law of computer trespass, when and where do third-party costs outweigh internalization benefits?[85] Under the CFAA, Congress sought to incorporate the social norms of physical trespass.[86] For legal purposes, those are now the norms of computer trespass, unless and until Congress says otherwise.

---

81 *See, e.g.*, Kerr, *supra* note 2, at 1159 ("I am optimistic that courts can identify and apply computer trespass norms using existing statutes.").

82 A limiting construction that introduces indeterminacy into statutory meaning may itself give rise to a vagueness challenge. *See, e.g.*, Bond v. United States, 134 S. Ct. 2077, 2097 (2014) (Scalia, J., dissenting) (claiming that "[n]o one should have to ponder the totality of the circumstances in order to determine whether his conduct is a felony" and arguing that narrowing construction of a statute may give rise to due process problems because "[t]hanks to the Court's revisions, the Act, which before was merely broad, is now broad and unintelligible"). *But see* Kerr, *Vagueness Challenges*, *supra* note 5, at 1572 (arguing that "[o]nly a narrow construction of the [CFAA] can save its constitutionality" against the void-for-vagueness doctrine).

83 *See supra* Part I.

84 *See* Kerr, *supra* note 2, at 1148–49.

85 Indeed, without further elaboration on how such norms would be derived, a "social norms" interpretive approach could suffer from some of the same conceptual arguments about circularity that have been levied at the "reasonable expectation of privacy" test in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 511 n.34 (2007). A "social norms" interpretive approach prompts the question: what are the appropriate "social norms," other than the ones that courts have announced?

86 *See* Kerr, *supra* note 2, at 1153–54.

C. *Element 3: Punishing the Unauthorized Access Would Advance the Rationale for the CFAA*

The third element, although perhaps less well defined, forms a core part of the law of physical trespass and is therefore, under our approach, incorporated into the CFAA's "without authorization" concept: for 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.[87]

Two illustrations, one ancient and one modern, demonstrate the principle's meaning. In the Commentaries, Blackstone expresses the rule of implied licenses in the following way: "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 of such inn or public house, he thereby gives a general licence to any person to enter his doors."[88] He further appears to acknowledge that express prohibition trumps implied consent, by remarking that "every entry" on private property "if contrary to [an owner's] express order, is a trespass or transgression."[89] But he acknowledges a wrinkle in the application of this principle. A trespass occurs "if one comes into a tavern, and will not go out in a reasonable time, but tarries there all night contrary to the inclinations of the owner."[90] But a trespass does not occur for "a bare non-feasance, as not paying for the wine he calls for . . . for this is only a breach of contract, for which the taverner shall have an action of debt or *assumpsit* against him."[91] Blackstone's point, it seems, is that alternative remedies exist for nonpayment of a dinner bill, thus ensuring that a "deceiver is . . . deterred without any resort to [a] trespass" claim.[92]

A modern application of this general principle can be found in Judge Posner's opinion for the Seventh Circuit in *Desnick v. American*

---

87 *See* WARD FARNSWORTH & MARK F. GRADY, TORTS: CASES AND QUESTIONS 28 (Aspen 2004). Several recent articles have noted a connection between the principle that we discuss in the text and the concept of a Fourth Amendment "search." *See, e.g.*, William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1823, 1877 (2016) (stating that "[u]nder the positive law model" Fourth Amendment issues should be resolved "by looking to underlying rules of property and agency law"); Laurent Sacharoff, *Trespass and Deception*, 2015 BYU L. REV. 359, 391 (arguing that deceptive practices should vitiate consent when they "relate to the interests the underlying right protects").

88 4 WILLIAM BLACKSTONE, COMMENTARIES *212.

89 *Id.* at *209.

90 *Id.* at *213.

91 *Id.*

92 Saul Levmore, *A Theory of Deception and then of Common Law Categories*, 85 TEX. L. REV. 1359, 1364 (2007).

Broadcasting Cos.[93] That case concerned undercover television reporters who carried concealed cameras into eye examination centers, thereby deceiving the owner of the clinic (to whom they had promised no undercover reporting).[94] After the television network used some of the footage obtained by the undercover reports in a negative exposé, the centers sued for common law trespass.[95] In analyzing that claim, Judge Posner recognized that "[t]o enter upon another's land without consent is a trespass" and that, although a privilege or implied consent was sufficient to allow a party to enter someone else's property, "there can be no implied consent in any nonfictitious sense of the term when express consent is procured by a misrepresentation or a misleading omission."[96] Yet Judge Posner still concluded that no trespass had occurred, because in certain cases consent will be deemed "effective even though it was procured by fraud."[97] Whether consent procured by fraud is effective, Posner reasoned, depends on whether there is an "invasion . . . of any of the specific interests that the tort of trespass seeks to protect."[98] Without this principle, Judge Posner observed, "a restaurant critic could not conceal his identity when he ordered a meal, or a browser pretend to be interested in merchandise that he could not afford to buy."[99]

This "relation to trespass" element may, at first blush, appear to be an ad hoc exception to the otherwise bright-line rules of trespass. But there are deeper principles at work. First, recall that trespass, both physical and computer, quite often turns on the terms of an agreement between an owner and a user, with the owner agreeing to

---

93 Desnick v. Am. Broad. Cos., 44 F.3d 1345 (7th Cir. 1995).

94 *Id.* at 1348.

95 *Id.* at 1347.

96 *Id.* at 1351 (reasoning that the eye center "would not have agreed to the entry of the test patients into its offices had it known they wanted eye examinations only in order to gather material for a television exposé").

97 *Id.*

98 *Id.* at 1352 (observing that the "lines" in this area "are not bright" and "not even inevitable" and have "resulted in a multitude of artificial distinctions in modern law").

99 *Id.* at 1351. The point, as Judge Posner notes, is a general one, with the "law's willingness to give effect to consent procured by fraud . . . not limited to the tort of trespass." *Id.* at 1352; *see also* RESTATEMENT (SECOND) OF TORTS § 892B, illus. 9 (AM. LAW. INST. 1979); Depoorter, *supra* note 4, at 1093 (speculating that "courts would probably not protect owners from a restaurant critic eating in a restaurant under a borrowed identity, from a browser in a store pretending to be interested in merchandise he cannot afford, or from customers in a car dealership's showroom who aggressively bargain with a salesperson by falsely claiming to have been offered a cheaper price by another vendor"). For a significant case following *Desnick*, see *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505 (4th Cir. 1999).

waive the right to exclude for some users or uses.[100] In that respect, just as an owner may contractually set the *scope* of access, so too may an owner be able to contractually set the proper *remedies* for a violation of the terms of access.[101] An owner, *ex ante*, may desire different consequences for a violation of different contractual terms, with only some terms being so crucial that the very right to access the system is conditioned on them.[102] As the Match.com example illustrates, website owners can explicitly attach a minor penalty, such as account deletion, to an infraction of the terms of service.[103] The site might frown on the prohibited conduct, but still decide as a business matter not to restrict access on that basis—in part so as not to inhospitably threaten valued customers.[104] The "relation to" element could be viewed as an attempt by courts to read remedial terms into otherwise silent contracts.

Second, it may be that this element reflects views about the judicial administrability of certain contractual terms. Authorization to access is determined at the time of access—if a person or business grants authorization conditioned on an understanding or conditioned on a promise, then the act is *still authorized* even if the understanding proves false or the promise is not kept.

Recognizing this parallel between physical and computer trespass does not definitively resolve the issues that Judge Kozinski raised in the Ninth Circuit's en banc *Nosal* decision—but it does provide analytical clarity on how to approach the case. *Nosal* addressed a circumstance where employees of one company used log-in credentials to

---

100 *See supra* Part I.

101 *Cf.* Saul Levmore, *Judging Deception*, 74 U. CHI. L. REV. 1779, 1789 (2007) (noting connection between approach to deception and the problem "of choosing an appropriate remedy").

102 *See id.* at 1785 ("One idea worth trying here concerns the likely ex ante agreement that would be reached between investigator and subject. . . . In the aftermath of a stinging review, a disappointed restaurateur might well claim that the critic gained access through fraudulent and thus tortious means. But viewed earlier in time, the critic offers the restaurant the potential of a positive, or even rave, review, followed by the patronage of many new customers. It is, therefore, safe to say that the overwhelming majority of restaurants would agree in advance to an undercover visit by a critic masquerading as a mere patron."); Levmore, *supra* note 92, at 1366 ("The hypothetical bargain idea is surely the source of the common intuition that a restaurant critic's deceit and apparent trespass is to be entirely forgiven.").

103 *See supra* notes 72–73 and accompanying text.

104 *See* Levmore, *supra* note 101, at 1787–88 (noting that an "emphasis on hypothetical contract or consent raises the obvious question of less convenient cost self-assessments, or simply of idiosyncratic reactions," such as a restaurant that expressly announces that reviewers will be deemed trespassers—but arguing that such an "inhospitable" reaction by a restaurant is "unrealistic" because it "would surely chase away a large number of patrons").

access the company's confidential database in order to help start a competing business, thereby violating a company policy forbidding the disclosure of confidential information. [105] The court held that the CFAA did not criminalize company policies that prohibited access to information for a particular use.[106]

One way of assessing whether *Nosal* was correctly decided is by looking to comparable instances in the realm of physical trespass. The same problem addressed in *Nosal* can arise in the context of physical trespass, if an employment agreement restricts the use of confidential files on company premises to legitimate, company purposes. Arguably, those precise applications of common law trespass were similarly incorporated into computer trespass. If so, *Nosal* may well have reached the wrong result because physical trespass prohibits (in Judge Posner's words) "a competitor [from] gain[ing] entry to a business firm's premises posing as a customer but in fact hoping to steal the firm's trade secrets."[107]

Another way of assessing *Nosal* is by reference to the CFAA's purposes, as reflected in, for example, the Act's legislative history. Here, too, the preliminary evidence is that *Nosal* takes a too narrow view of the CFAA.[108] At any rate, while this Article does not claim to fully resolve the proper scope and application of the "relation to" element, it does resolve one aspect of the debate surrounding *Nosal*: the same problem that the court confronted in the context of computer trespass also exists in the context of physical trespass.

CONCLUSION

The crimes of physical and computer trespass have parallels, and those parallels teach us three things. First, "authorization" under the CFAA has the same meaning as authorization under criminal physical trespass laws because Congress intended to incorporate the law of physical trespass into the CFAA.[109] Second, although interpreting "authorization" under the CFAA can be difficult, identical difficulties exist in the application of physical trespass laws—and the very same

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

106 *Id.* at 863–64.

107 Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1352 (7th Cir. 1995); *see also* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991); E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1014 (5th Cir. 1970).

108 *See* William A. Hall, Jr., *The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in* United States v. Nosal, 84 GEO. WASH. L. REV. 1523, 1542–43 (2016).

109 *See* S. REP. NO. 104-357, at 11 (1996); *supra* Part I.

resolutions of these problems in the context of physical trespass should, as a first approximation, apply in the context of computer trespass. 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. Third, because both physical trespass and the CFAA require proof that the defendant knew his access was unauthorized, the merits of a void-for-vagueness challenge to computer trespass rises and falls with the merits of a similar challenge to physical trespass. The elements being the same, the result should likewise be the same. Given the pedigree of the latter, a constitutional challenge to the former seems questionable.

Whatever may be said against applying the rules of physical trespass to computer trespass, one thing must be said in its favor: this approach is more straightforward than the alternatives currently on offer, and it aligns with Congress's announced intention to bring trespass law to computer networks. In the context of a statute enacted against a property-rights backdrop—and enforced by criminal penalties, no less—that simplicity should be viewed as a significant virtue.[110]

110 *Cf.* Johnson v. United States, 135 S. Ct. 2551, 2558 (2015) (reasoning that "this Court's repeated attempts and repeated failures to craft a principled and objective standard . . . confirm [the statute's] hopeless indeterminacy"); *see also* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 247 (2012) ("A statute should be interpreted in a way that avoids placing its constitutionality in doubt.").