ESSAY

NORMS OF COMPUTER TRESPASS

*Orin S. Kerr**

This Essay develops an approach to interpreting computer trespass laws, such as the Computer Fraud and Abuse Act, that ban unauthorized access to a computer. In the last decade, courts have divided sharply on what makes access unauthorized. Some courts have interpreted computer trespass laws broadly to prohibit trivial wrongs such as violating terms of use to a website. Other courts have limited the laws to harmful examples of hacking into a computer. Courts have struggled to interpret authorization because they lack an underlying theory of how to distinguish authorized from unauthorized access.

This Essay argues that authorization to access a computer is contingent on trespass norms—shared understandings of what kind of access invades another person's private space. Judges are unsure of how to apply computer trespass laws because the Internet is young and its trespass norms are unsettled. In the interim period before norms emerge, courts should identify the best rules to apply as a matter of policy. Judicial decisions in the near term can help shape norms in the long term. The remainder of the Essay articulates an appropriate set of rules using the principle of authentication. Access is unauthorized when the computer owner requires authentication to access the computer and the access is not by the authenticated user or his agent. This principle can resolve the meaning of authorization before computer trespass norms settle and can influence the norms that eventually emerge.

---

* Fred C. Stevenson Research Professor, George Washington University Law School. Thanks to Steve Bellovin, David Cruz, Tim Edgar, Hanni Fakhoury, David Fontana, Mary Anne Franks, Ahmed Ghappour, Robert Graham, James Grimmelmann, Stephen Henderson, Marcia Hofmann, Michael Madison, Jonathan Mayer, Janice Nadler, Paul Ohm, Michael Risch, Ken Simons, Daniel Solove, Ashkan Soltani, Peter Winn, and commenters at the Privacy Law Scholars Conference and faculty workshops at Northwestern University Law School and the University of Southern California Gould School of Law for extremely helpful comments on an earlier draft.

INTRODUCTION

The federal government and all fifty states have enacted criminal laws that prohibit unauthorized access to a computer.[1] At first blush, the meaning of these statutes seems clear.[2] The laws prohibit trespass into a computer network just like traditional laws ban trespass in physical space.[3] Scratch below the surface, however, and the picture quickly turns cloudy.[4] Courts applying computer trespass laws have divided deeply over

1. The federal law is the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030 (2012). For a summary of state laws, see generally A. Hugh Scott, Computer and Intellectual Property Crime: Federal and State Law 639–1300 (2001); Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 Richmond J.L. & Tech. 28, para. 15 n.37 (2001), http://jolt.richmond.edu/v7i3/article2.html [http://perma.cc/4YFP-KH8S].

2. See United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (concluding lower court was not required to instruct jury on meaning of "authorization" because "the word is of common usage, without any technical or ambiguous meaning").

3. See S. Rep. No. 104-357, at 11 (1996) (noting CFAA "criminalizes all computer trespass").

4. See Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1572, 1574 (2010) [hereinafter Kerr, Vagueness Challenges] (discussing uncertain application of CFAA); Note, The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation, 127 Harv. L. Rev. 751, 751–52 (2013) (noting scope of CFAA—chief federal computer crime law—"has been hotly litigated," and "the most substantial fight" is over meaning of authorization).

when access is authorized.[5] Circuit splits have emerged, with judges frequently expressing uncertainty and confusion over what computer trespass laws criminalize.[6]

Consider the facts of seven recent federal cases involving the federal unauthorized access law, the Computer Fraud and Abuse Act (CFAA).[7] In each case, the line between guilt and innocence hinged on a dispute over authorization:

1. An employee used his employer's computer at work for personal reasons in violation of a workplace rule that the computer could only be used for official business.[8]

2. An Internet activist logged on to a university's open network using a new guest account after his earlier guest account was blocked.[9]

3. Two men used an automated program to collect over 100,000 email addresses from a website that had posted the information at hard-to-guess addresses based on the assumption that outsiders would not find it.[10]

4. A man accessed a corporate account on a website using login credentials that he purchased from an employee in a secret side deal.[11]

5. A company collected information from Craigslist after Craigslist sent the company a cease-and-desist letter and blocked the company's IP address.[12]

---

5. See, e.g., United States v. Nosal, 676 F.3d 854, 865 (9th Cir. 2012) (en banc) (Kozinski, C.J.) (noting circuit split between Ninth Circuit and Fifth and Eleventh Circuits over whether employee who violates written restriction on employer's computer use engages in criminal unauthorized access under CFAA); NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *11 (N.D. Cal. Jan. 29, 2015) (noting deep division in district courts on whether copying constitutes damage under CFAA); Advanced Micro Devices, Inc. v. Feldstein, 951 F. Supp. 2d 212, 217 (D. Mass. 2013) (noting two distinct schools of thought in case law on what makes access authorized).

6. See, e.g., CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116, 129 (3d Cir. 2015) (noting meaning of authorization "has been the subject of robust debate"); 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."); *Feldstein*, 951 F. Supp. 2d at 217 ("[T]he exact parameters of 'authorized access' remain elusive.").

7. 18 U.S.C. § 1030 (2012).

8. See *Nosal*, 676 F.3d at 863–64 (holding such acts do not violate CFAA).

9. See Indictment at 4–7, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011) (charging criminal defendant for such conduct).

10. See United States v. Auernheimer, 748 F.3d 525, 534–35 (3d Cir. 2014) (reversing conviction on venue grounds but not reaching whether it violated CFAA).

11. See Brief of Appellant at 10–14, United States v. Rich (4th Cir. Mar. 2, 2015) (No. 14-4774), 2015 WL 860788 (arguing such conduct does not violate CFAA).

12. See Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 968–70 (N.D. Cal. 2013) (concluding such conduct violates CFAA).

> 6. A company used an automated program to purchase tickets in bulk from Ticketmaster's website despite the website's use of a barrier designed to block bulk purchases by automated programs.[13]
>
> 7. A former employee continued to access his former employer's computer network using a backdoor account that the former employer had failed to shut down.[14]

On the surface, there are plausible arguments on both sides of these cases. The prosecution can argue that access was unwanted, at least in some sense, and therefore was unauthorized. The defense can argue that access was allowed, at least in some sense, and therefore was authorized.[15] Liability hinges on what concept of authorization applies. However, courts have not yet identified a consistent approach to authorization. Authorization is not defined under most computer trespass statutes, and the statutory definitions that exist are generally circular.[16] Violating computer trespass laws can lead to severe punishment, often including several years in prison for each violation.[17] And yet several decades after the widespread enactment of computer trespass statutes, the meaning of authorization remains remarkably unclear.

This Essay offers a framework to distinguish between authorized and unauthorized access to a computer. It argues that concepts of authorization rest on trespass norms. As used here, trespass norms are broadly shared attitudes about what conduct amounts to an uninvited entry into another person's private space.[18] Relying on the example of physical-world trespass, this Essay contends that the scope of trespass crimes follows from identifying trespass norms in three ways: first, characterizing the nature of the space; second, identifying the means of permitted access; and third,

---

13. See United States v. Lowson, Crim. No. 10-114 (KSH), 2010 WL 9552416, at *6–7 (D.N.J. Oct. 12, 2010) (discussing but not resolving CFAA liability for such facts).

14. See United States v. Steele, 595 F. App'x 208, 210–11 (4th Cir. 2014) (holding this violates CFAA).

15. 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 [http://perma.cc/YYP8-A8A5] ("In any CFAA case, the defendant can argue, 'You say I shouldn't have done it, but the computer said I could!'").

16. For example, the CFAA does not define "without authorization," and the related term "exceeds authorized access" is defined circularly 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." 18 U.S.C. § 1030(e)(6) (2012).

17. See generally Orin S. Kerr, Computer Crime Law 328–75 (3d ed. 2013) (discussing sentencing under CFAA).

18. The word "norms" has been used to mean many different things, ranging from practices that are common and expected among members of a society to practices that are perceived as morally obligated within that group. See generally Richard H. McAdams & Eric B. Rasmusen, Norms and the Law, *in* 2 Handbook of Law and Economics 1575, 1576–78 (A. Mitchell Polinsky & Steven Shavell eds., 2007) (defining "norms"). In this Essay, I use the term "trespass norms" to focus specifically on norms that relate to perceptions of invasion of private space.

identifying the context of permitted entry. These three steps can be used to identify the norms of computer trespass and to give meaning to criminal laws on unauthorized access.

Interpreting computer trespass laws raises an important new twist. Although trespass norms in physical space are relatively settled and intuitive, computer trespass norms online are often unsettled and contested. The Internet is new and rapidly changing. No wonder courts have struggled to apply these laws: Doing so requires choosing among unsettled norms in changing technologies that judges may not fully understand. In that context, courts cannot merely identify existing norms. Instead, they must identify the best rules to apply from a policy perspective, given the state of technology and its prevailing uses. Published court decisions can then help establish norms consistent with those rules.

After first identifying the conceptual challenges of applying computer trespass laws, this Essay argues that the principle of authentication provides the most desirable basis for computer trespass norms. Authentication requires verifying that the user is the person who has access rights to the information accessed.[19] Under this principle, the open norm of the World Wide Web should render access to websites authorized unless it bypasses an authentication gate. This approach leaves Internet users free to access websites even when their owners have put in place virtual speed bumps that can complicate access, such as hidden addresses, cookies-based limits, and IP address blocks.[20] Further, when access requires authentication, whether access is authorized should hinge on whether it falls within the scope of delegated authority the authentication implies. Access to canceled accounts should be unauthorized, and access using new accounts may or may not be authorized depending on the circumstances.[21] Finally, the lawfulness of access using a shared password should depend on whether the user intentionally acts outside the agency of the account holder.

The authentication principle advocated in this Essay best captures the competing policy goals of modern Internet use in light of the blunt and severe instrument of criminal law. Norms based on this principle give users wide berth to use the Internet as the technology allows, free from the risk of arrest and prosecution, as long as they do not contravene mechanisms of authentication. On the other hand, the norms give computer owners the ability to impose an authentication requirement and then control who accesses private information online. The result establishes both public and private virtual spaces online using a relatively clear and stable technological standard.

---

19. See infra section III.C (explaining authentication).

20. See infra Part III (discussing open nature of Web and mechanisms used by site owners to restrict access).

21. See infra Part IV (discussing distinction between canceled accounts, blocked accounts, and new accounts).

This Essay contains four parts. Part I shows how trespass norms apply in physical space. Part II argues that courts should apply the same approach to computer networks but that they must identify the best trespass norms rather than simply identify existing norms. Part III considers the trespass norms that courts should identify in the many difficult cases involving the Web. Part IV explains how the norms of computer trespass should apply to the complex problems raised by canceled, blocked, and shared accounts.

I. TRESPASS IN PHYSICAL SPACE

Imagine a suspicious person is lurking around someone else's home or office. The police are called, and officers watch the suspect approach the building. Now consider: When has the suspect committed a criminal trespass that could lead to his arrest and prosecution? This section shows how the answer comes from trespass norms in physical space—shared understandings of obligations surrounding access to different physical spaces. The rules are not written down in trespass statutes. Instead, those called on to interpret physical trespass laws make intuitive conclusions based on the nature of that space and the understood purposes of different means of accessing it. From those intuitions, shared understandings emerge about whether and when access to a physical space is permitted. By unpacking our intuitions that govern physical trespass, we can then appreciate why courts have struggled to interpret computer trespass laws.

A. *Authorization and Social Norms*

The concept of trespass implies signals sent by property owners about what uses of that property are permitted. In some cases, the signals are clear and direct. Recall the childhood game "red light, green light."[22] In the game, the game master barks out orders to the players. Green light, they can run. Red light, they must stop. The control is direct and in realtime, with the game master watching the players in person. In this environment, notions of authorization are obvious. The leader monitors and maintains complete control.

The more common and interesting problems arise when control of authorization is implicit. In most cases, permission is deduced from the circumstances based on signals that draw on shared understandings about the world. A Martian who landed on Earth for the first time would find the results deeply puzzling. Having never experienced human social interaction, it would miss the signals and see the human understandings as arbitrary. From our perspective, however, the signals are intuitive and usually seem obvious.

22. See Red Light/Green Light, Games Kids Play, http://www.gameskidsplay.net/games/sensing_games/rl_gl.htm [http://perma.cc/3JVF-NZWM] (last visited Jan. 26, 2016).

Importantly, the text of criminal trespass statutes doesn't provide these answers.[23] Consider New York's trespass law, § 140.05. The language is brief: "A person is guilty of trespass when he knowingly enters or remains unlawfully in or upon premises."[24] What does "unlawfully" mean? The statutory definition tries but fails to answer that question. "A person 'enters or remains unlawfully' in or upon premises," the definition says, "when he is not licensed or privileged to do so."[25] That's no help. When are you "licensed" to enter? What gives you a "privilege"? The text doesn't say.

Criminal trespass law can retain this textual ambiguity because the real meaning of trespass law comes from trespass norms that are relatively clear in physical space.[26] The written law calls on the norms, and the norms tell us, at an intuitive level, when entry to property is forbidden and when it is permitted. Although identifying social norms is often difficult generally, the specific nature of trespass norms allows greater clarity. Trespass norms are relatively specific: They are about shared intuitions about what is a trespass, not what is appropriate or inappropriate behavior generally. And those norms provide relative clarity about what is a physical trespass.

Relative clarity doesn't mean absolute clarity, of course. Criminal trespass law is rarely litigated. Physical trespass tends to be a low-level offense,[27] and it typically extends to those who unlawfully remain in place after being told by the homeowner to leave.[28] As a practical matter, the crime may be used primarily as a way to arrest and remove someone who won't leave where he is not wanted rather than as a tool for criminal pun-

---

23. Trespass is an accordion-like concept that can mean different things in different contexts. See, e.g., 3 William Blackstone, Commentaries *208–09 (discussing variations of trespass at common law). Because computer trespass laws are primarily criminal statutes, the discussion focuses on liability under criminal trespass statutes. I am therefore excluding consideration of other kinds of trespass claims such as the scope of the common law tort of trespass to chattels. See generally eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000) (applying common law tort of trespass-to-chattels analysis in computer context).

24. N.Y. Penal Law § 140.05 (McKinney 2010).

25. Id. § 140.00(5).

26. See Richard H. McAdams, The Origin, Development, and Regulation of Norms, 96 Mich. L. Rev. 338, 340 (1997) ("Sometimes norms govern behavior irrespective of the legal rule, making the choice of a formal rule surprisingly unimportant."); see also Cass R. Sunstein, Social Norms and Social Roles, 96 Colum. L. Rev. 903, 914 (1996) (defining social norms as "social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done").

27. For example, under New York law, trespass only carries an offense level of a violation. N.Y. Penal Law § 140.05. A violation carries a maximum punishment of fifteen days. Id. § 10.00(3).

28. See, e.g., id. § 140.05 ("A person is guilty of trespass when he knowingly enters *or remains* unlawfully in or upon premises." (emphasis added)).

ishment on conviction.[29] As a result, some ambiguities may exist but remain latent in the statute.

But even if ambiguities remain, they are substantially narrowed by the three ways that trespass norms inform the meaning of criminal trespass laws. First, trespass norms provide a general set of rules that govern entrance based on the nature of the space. Second, they help resolve which means of access are permitted. And third, they explain the context in which the permitted means become authorized.

B. *The Nature of the Space*

The first way that trespass norms guide notions of license and privilege is by providing informal rules based on the nature of each space. Different spaces trigger different obligations. Private homes trigger one set of rules. Commercial stores would trigger another. A public library might trigger a third. A public park a fourth. Life experience with common social practices creates shared understandings about what kinds of entry are permitted for different kinds of spaces.

Start with the home. The home triggers a robust set of assumptions about privacy and permission.[30] A person's home is his castle, the common law tells us.[31] And the principle of the common law remains deeply and widely held today. Everyone knows that you stay out of another's home unless there is an express invitation. If you break those norms, trouble will follow. You can expect a frightened homeowner to call the police, if not to emerge with a twelve gauge pointed in your direction. And trespass case law reflects the strong default presumption of the home: The slightest overstep or intrusion into the home, or even just entry based on false pretenses, has been held to be a trespass.[32]

But what is true for the home is not true for other physical spaces. Contrast the home with a commercial store. Imagine it's a weekday afternoon and you find a flower shop in a suburban strip mall. The norms governing access to the shop are very different from those governing ac-

---

29. In general, probable cause to arrest a suspect for criminal trespassing can justify the suspect's arrest and removal so long as the offense—typically, the refusal to leave—is occurring in the officer's presence. See, e.g., N.Y. Crim. Proc. Law § 140.10 (McKinney 2004) (describing arrest powers).

30. See generally Stephanie M. Stern, The Inviolate Home: Housing Exceptionalism in the Fourth Amendment, 95 Cornell L. Rev. 905, 912 (2010) (discussing special status of home in Fourth Amendment law).

31. See Semayne's Case (1604) 77 Eng. Rep. 194, 198; 5 Co. Rep. 91 a, 93 a ("[T]he house of any one is not a castle or privilege but for himself.").

32. See, e.g., People v. Bush, 623 N.E.2d 1361, 1364 (Ill. 1993) ("If . . . the defendant gains access to the victim's residence through trickery and deceit and with the intent to commit criminal acts, his entry is unauthorized and the consent given vitiated because the true purpose for the entry exceeded the limited authorization granted."); People v. Williams, 667 N.Y.S.2d 605, 607 (Sup. Ct. 1997) (concluding "person who gains admittance to premises through intimidation or by deception, trick or artifice, does not enter with license or privilege" for purposes of criminal trespass liability).

cess to a home. You can approach the store and peer through the window. If you see no one inside, you can try to enter through the front door. If the door is unlocked, you can enter the store and walk around. The shared understanding is that shop owners are normally open to potential customers. An unlocked door during work hours ordinarily signals an invitation. That openness is not unlimited, of course. You can't go into the back of the store, marked "Employees Only," without an invitation.[33] And if the store owner tells you to leave, you have to comply.[34] But in contrast to the closed default at a private home, the default at a commercial store is openness absent special circumstances indicating closure.

Even open spaces can have trespass norms, and those norms can differ from the norms governing entry into enclosed structures such as homes or stores. In a recent Fourth Amendment case, *Florida v. Jardines*,[35] the Supreme Court considered the trespass norms that apply to a front porch. Officers suspected that Jardines might be growing marijuana in his home, so they walked a drug-sniffing dog up to his front porch and had him give the front door a good, hard sniff.[36] The dog alerted to drugs, creating probable cause for a warrant and a search.[37]

The Justices ruled that walking up to the front door with the dog was a trespass that violated the Fourth Amendment because it exceeded the implied social license governing approach to the home.[38] According to Justice Scalia, some entry onto the front porch was permitted by social custom. Any visitor could "approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave."[39] On the other hand, bringing a drug-sniffing dog to the front door violated that customary understanding:

> To find a visitor knocking on the door is routine (even if sometimes unwelcome); to spot that same visitor exploring the front path with a metal detector, or marching his bloodhound into

33. See, e.g., State v. Cooper, 860 N.E.2d 135, 138 (Ohio Ct. App. 2006) (entering portion of store marked "Employees Only" was trespass because sign "put the defendant on notice that by entering the room, he was in violation of restriction against access that applied to him").

34. See, e.g., Model Penal Code § 221.2(2)(a) (Am. Law Inst. 2015) (punishing as "defiant trespass" a person who stays in a place when notice of trespass has been provided by "actual communication to the actor").

35. 133 S. Ct. 1409 (2013).

36. Id. at 1413.

37. Id.

38. See id. at 1417 ("[W]hether the officers had an implied license to enter the porch . . . depends upon the purpose for which they entered. Here, their behavior objectively reveals a purpose to conduct a search, which is not what anyone would think he had license to do.").

39. Id. at 1415.

> the garden before saying hello and asking permission, would inspire most of us to—well, call the police.[40]

The lesson is that different spaces have different trespass norms. Some spaces are open, others are closed, and still others are open to some but closed to others. The text of trespass laws is often misleadingly simple—just the simple prohibition against unlicensed entry. Meanwhile, the real work of distinguishing culpable invasions from nonculpable explorations comes from space-specific norms.

C. *Means of Access*

The second role of trespass norms is to identify means of permitted access. Permission to enter often is implicitly limited to specific methods of entrance. And we know which means of entry are permitted, and which are forbidden, by relying on widely understood social understandings.

Consider entrance to a commercial store. The trespass norm governing a commercial store might be that entrance is permitted when a ready means of access is available that can be read in context as an open invitation. That principle implies limits on which means of access are allowed. An open window isn't an invitation to jump through the window and go inside. If there's an open chimney or mail drop, that's not an invitation to try to enter the store. Barring explicit permission from the store owner, the only means of permitted access to a commercial store is the front door.

The source of these principles seems to be a socially shared understanding of the intended function of walls, windows, chimneys, and doors. Windows are there to let in light, not people. Chimneys exist to let out smoke, not admit guests (Santa excepted). We know from life experience that these ways in are not authorized. In contrast, entry through the unlocked front door is authorized. The front door is intended for customer entrance and exit. That's why it's there.

D. *Context of Access*

Trespass norms play a third role by governing the context in which entrance can occur. Entry through the front door might be authorized, but the front door isn't for everyone. Doors usually come with locks, and locks are designed to let some people in and keep other people out. Locks are an example of access control by which we recognize a means of access but limit it to specific people with specific rights.[41] To complete

---

40. Id. at 1416. According to Justice Scalia, the norms were readily grasped even though they were not written down: "Complying with the terms of that traditional invitation does not require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters." Id. at 1415.

41. See Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, Handbook of Applied Cryptography 3 (1996) (defining "access control" as means of "restricting access to resources to privileged entities").

the picture of how norms govern authorization to enter a home, we need to consider how those norms apply to locks and keys.

The starting point is simple enough. The property owner owns the door, lock, and keys, so the owner presumptively is in charge. If the lock breaks, the owner has to buy another one. The owner has the power to decide who gets a key and who is permitted to use it. As a result, authorization of entrance by key depends on whether that entrance was within the zone of authority delegated by the owner.

Imagine you are walking down the street and you see and pick up a lost house key. Possession of the key doesn't entitle you to use the key and enter the house. You have the key, but you lack permission to use it. And you lack permission because there's no chain of authorization coming from the owner. Picking a lock is unauthorized for the same reasons, at least unless you're a locksmith who the owner hired to open the door after being locked out.[42] If the owner grants you permission but later revokes it, your authorization expires with the revocation. If the homeowner gives someone else the key but places limits on access, those limits govern authorization.[43]

The lesson of these examples is that authorization rests on trespass norms. In a world of indirect communication, familiarity with the social signals of what entry is permitted or forbidden makes the law clear enough that most people don't fear arrest in their everyday activity. The nature of the space provides one set of messages, norms about the intended purpose of different means of access provide even more detailed guidance, and access controls within the zone of permission delegated by property owners provide an additional layer of rules.

II. THE NORMS OF COMPUTER TRESPASS

The Internet has its own kind of trespass law that closely resembles its physical-world cousin. In cyberspace, the relevant law is found in computer misuse statutes such as the CFAA.[44] The CFAA and its state equivalents ban unauthorized access to a computer.[45] At a broad level, the purpose of those statutes is easy to describe: Unauthorized access statutes are computer trespass statutes.[46] Applying the new statutes requires translat-

42. Cf. Taha v. Thompson, 463 S.E.2d 553, 557 (N.C. Ct. App. 1995) (holding evidence that individual sent locksmith onto property to change locks without homeowner's permission establishes trespass).

43. See Douglas v. Humble Oil & Ref. Co., 445 P.2d 590, 591 (Or. 1968) (en banc) (holding employee who was given key to employer's home to feed employer's pets committed trespass when employee used key to enter home for different reason).

44. 18 U.S.C. § 1030 (2012).

45. For an overview, see generally Scott, supra note 1, at 639–1300. In this Essay, I include both "access without authorization" and conduct that "exceeds authorized access" as within the general ban on unauthorized access. See infra section III.B (discussing unauthorized access).

46. See supra notes 2–5 (discussing court applications of computer trespass laws).

ing concepts of trespass from physical space to the new environment of computers and networks. But as courts have found, understanding the concept of authorization to computers ends up being surprisingly hard.[47] The courts are divided, with many courts struggling to apply this simple-seeming concept.[48]

The norms-driven nature of physical trespass law explains why courts have struggled to interpret computer trespass laws. The trespass norms of physical space are relatively clear because they are based on shared experience over time. The Internet and its technologies are new, however, and the trespass norms surrounding its usage are contested and uncertain. When faced with an authorization question under a computer trespass law, today's judges bring to mind the Martian from outer space considering how traditional trespass laws might govern trespass into a home. Without established norms to rely on, the application of a seemingly simple concept like "authorization" becomes surprisingly hard.

This section develops three lessons for interpreting authorization in computer trespass statutes that follow from the norms-based nature of trespass law. First, the meaning of authorization will inevitably rest on the identification of trespass norms, which will in turn rest on models and analogies. Second, Internet technology is sufficiently new, and the norms of computer trespass sufficiently unsettled, that judges applying computer trespass law must not just identify existing trespass norms, but must identify as a policy matter the optimal rules that should govern the Internet. And third, despite these challenges, trespass provides a sensible framework for regulating computer misuse and courts have the ability to identify and apply the norms for computer trespass within the framework of existing laws.

A. *The Inevitability of Norms in Computer Trespass Law*

The first lesson is that the meaning of authorization in computer trespass laws inevitably rests on the identification of proper trespass norms. Like their physical-world cousins, computer trespass laws feature unilluminating text. They prohibit unauthorized access to computers just like physical trespass laws prohibit unlicensed entry to physical spaces. In both contexts, the meaning of the law must draw from social understandings about access rights drawn from different signals within the relevant spaces. Courts must identify the rules of different spaces based on understandings of the relevant trespass norms.

It's no surprise that litigation over computer trespass laws often triggers a battle of physical-space analogies. The government, seeking a broad reading of the law, will push analogies to physical facts that trigger strict norms. The defense, seeking a narrow reading of the law, will push analo-

47. See supra notes 2–5.

48. See supra notes 4–5 (providing examples of disagreements among courts over concept of authorization in CFAA).

gies to physical facts that implicate loose norms. The battle of analogies happens not because it is inevitable that we analogize cyberspace to physical space,[49] but rather because authorization inevitably rests on trespass norms. Litigants will use analogies from physical spaces with the trespass norms that best aid their side.

Consider the recent litigation in *United States v. Auernheimer*.[50] Auernheimer had been convicted of unauthorized access for using a software program that collected information from an AT&T website at hard-to-guess addresses intended to be kept private.[51] On appeal to the Third Circuit, the government's brief analogized the website to a home where trespass norms are at their zenith. Use of the program was a computer trespass, the government argued, because a physical trespass occurs "when an unauthorized person enters someone else's residence, even when the front door is left open or unlocked."[52] In contrast, the defense analogized the website to a public space where trespass norms are at their nadir. Use of the program was not a trespass, the defense argued, because putting information on a website "ma[d]e the information available to everyone and thereby authorized the general public to view the information."[53] Each analogy aimed to import a set of physical-world norms.[54]

B. *Because Computer Trespass Norms Are Unsettled, Courts Should Identify the Best Norms to Apply*

The conflicting analogies found in computer trespass cases highlight the biggest difference between applying physical trespass and computer trespass laws: Computer trespass norms remain uncertain. Understandings of access rights surrounding the home are ancient, while understandings of access rights in computer networks are not. The statutes came first, and the statutory prohibition on unauthorized access has remained fixed while computer network technology has advanced at astonishing speed. In this environment, courts cannot merely identify existing norms. Instead, they should make a normative policy decision about what understandings should govern the Internet. Judicial decisions will then shape future computer trespass norms, allowing appropriate norms to emerge with the help of the courts.

---

49. See Mark Lemley, Place and Cyberspace, 91 Calif. L. Rev. 521, 523–26 (2003) ("[E]ven a moment's reflection will reveal that the analogy between the Internet and a physical place is not particularly strong.").

50. 748 F.3d 525 (3d Cir. 2014). Full disclosure: I represented Auernheimer.

51. Id. at 530–31.

52. Brief for Appellee at 34, *Auernheimer*, 748 F.3d 525 (No. 13-1816), 2013 WL 5427839.

53. Brief for Appellant at 15, *Auernheimer*, 748 F.3d 525 (No. 13-1816), 2013 WL 3488591.

54. The Third Circuit did not reach this issue, as it reversed on the ground that venue was lacking in the district where the prosecution was brought. *Auernheimer*, 738 F.3d at 541.

To appreciate the problem, consider the rapid evolution of Internet technologies. The Internet itself is less than fifty years old.[55] The World Wide Web is only about twenty years old.[56] The experience of using the Internet morphs quickly. Fifteen years ago, connecting to the Internet meant logging on from a desktop computer at work or perhaps using a dial-up connection from home. Today, connecting to the Internet is very different. Wireless connections have become the norm, allowing anyone to access the Internet from almost anywhere. And in just the last five years, the rise of the "smart phone" has brought the Internet to a light hand-held device that most adults leave on 24/7 and carry with them in their pockets and purses.[57]

The programs we use to access the Internet also change rapidly. A majority of Americans now have a Facebook account, and about seventy percent of account holders visit Facebook every day.[58] But Facebook wasn't even invented until 2004,[59] and it already has become passé among teenagers who have moved on to Instagram (launched in 2010[60]) and Snapchat (launched in 2011[61]).[62] Or consider the popular Apple iPhone introduced in 2007.[63] The iPhone popularized the phrase "there's an app for that"[64] for the new applications, or "apps," that the phone can run. Apple's

---

55. See Reno v. ACLU, 521 U.S. 844, 849–50 (1997) (tracing history of Internet from ARPANET in 1969).

56. See Tim Berners-Lee with Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor 69 (1999) (describing February 1993 release of first popular web browser).

57. See Riley v. California, 134 S. Ct. 2473, 2484 (2014) (recognizing "modern cell phones . . . are now such a pervasive and insistent part of daily life" but were "unheard of ten years ago").

58. Elizabeth Weise, Your Mom and 58% of Americans Are on Facebook, USA Today (Jan. 9, 2015, 5:22 PM), http://www.usatoday.com/story/tech/2015/01/09/pew-survey-social-media-facebook-linkedin-twitter-instagram-pinterest/21461381/ [http://perma.cc/QNK9-N5WZ].

59. Company Info: Our History, Facebook, http://newsroom.fb.com/timeline/company-info/ [http://perma.cc/9J9R-H2BT] (last visited Jan. 26, 2016).

60. MG Siegler, Instagram Launches with the Hope of Igniting Communication Through Images, TechCrunch (Oct. 6, 2010), http://techcrunch.com/2010/10/06/instagram-launch/ [http://perma.cc/T7E2-YNU3].

61. J.J. Colao, Snapchat: The Biggest No-Revenue Mobile App Since Instagram (Nov. 27, 2012, 1:36 PM), http://www.forbes.com/sites/jjcolao/2012/11/27/snapchat-the-biggest-no-revenue-mobile-app-since-instagram/ [http://perma.cc/P6LY-7J73].

62. See Joanna Stern, Teens Are Leaving Facebook and This Is Where They Are Going, ABC News (Oct. 31, 2013), http://abcnews.go.com/Technology/teens-leaving-facebook/story?id=20739310 [http://perma.cc/4S6G-ZHYE] (noting migration of teen users from Facebook to Instagram and Snapchat).

63. See Press Release, Apple, Apple Reinvents the Phone with iPhone (Jan. 9, 2007), http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html [http://perma.cc/L937-DHP4]; see also Steve Jobs, iPhone Introduction in 2007, YouTube (Jan. 10, 2014), http://www.youtube.com/watch?v=9hUIxyE2Ns8.

64. The phrase comes from a commercial for the iPhone 3G in 2009. Apple, There's an App for That, YouTube (Feb. 4, 2009), http://www.youtube.com/watch?v=szrsfeyLzyg.

iTunes App Store has more than 1.5 million apps available already,[65] and about 1,000 new apps are submitted for approval every day.[66] Even the specific programs we use change over time. Regular updates and improvements are the norm, with new versions often adding features that can substantially change the user experience.

The problem is not just technological. The lawyers have stepped in, too. Companies often hire counsel to write detailed terms of use that purport to say when access is permitted.[67] These written contractual limitations can be extremely restrictive,[68] often creating a clash between what the technology allows a user to do and what the language of the terms says is allowed. In that case, what governs: the technology or the language? 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.

Deferring to jury verdicts is not workable, either. Trial courts have often used jury instructions that either leave authorization undefined or else tell the jury, unhelpfully, that access is unauthorized when it is without permission.[69] A study by Matthew Kugler suggests that this leads to verdicts far beyond whatever trespass norms may emerge.[70] Kugler surveyed 593 adult Americans by asking them to review short descriptions of the facts of several CFAA cases.[71] Respondents were asked to what extent the computer user had "authorization to use the computer" in the way

---

65. Number of Available Apps in the Apple App Store from July 2008 to June 2015, Statista, http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/ [http://perma.cc/CVH8-P4J5] (last visited Jan. 26, 2016).

66. Number of Newly Developed Applications/Games Submitted for Release to the iTunes App Store from 2012 to 2014 (Fee Based), Statista, http://www.statista.com/statistics/258160/number-of-new-apps-submitted-to-the-itunes-store-per-month/ [http://perma.cc/YN4W-7FM4] (last visited Jan. 26, 2016).

67. See Judith A. Powell & Lauren Sullins Ralls, Best Practices for Internet Marketing and Advertising, 29 Franchise L.J. 231, 235 (2010) (advising franchise operators to protect themselves by creating terms of use that allow franchisors to effectively control sites' content).

68. See United States v. Nosal, 676 F.3d 854, 860–63 (9th Cir. 2012) (providing examples of ways computer-use policies prohibit common activity).

69. See, e.g., United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (agreeing with lower court that "it was unnecessary to provide the jury with a definition of 'authorization' . . . [s]ince the word is of common usage"); United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009) (noting no evidence Congress intended to give specialized meaning to "authorization" and "authorized" in CFAA and citing dictionary definition); Transcript for Trial at 26–27, United States v. Auernheimer, Crim. No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Oct. 26, 2012), rev'd, 748 F.3d 525 (3d Cir. 2014) ("To access without authorization is to access a computer without approval or permission.").

70. See Matthew B. Kugler, Measuring Computer Use Norms (unpublished manuscript) (manuscript at 25) (Oct. 19, 2015), http://ssrn.com/abstract=2675895 (on file with the *Columbia Law Review*) [hereinafter Kugler, Measuring Norms] (noting participants' willingness to find common behavior blameworthy and, in some cases, criminal).

71. Id. (manuscript at 6).

he did, measured on a scale of one (not at all) to six (very much).[72] The study then asked respondents to assign the proper punishment for the act, with respondents choosing among four options: no punishment at all; punishment akin to a parking ticket, punishment for a minor crime such as petty theft, and punishment for a major crime such as burglary.[73]

Kugler's survey suggests that lay opinion about when use is "authorized" differs considerably from trespass norms. In most of the scenarios, respondents viewed the computer use as unauthorized. Mean values of authorization ranged from a low of 1.43 (for an employee who used his employer's computer to sell employer trade secrets) to a high of 2.32 (for an employee who used his employer's computer to check the weather report for personal reasons).[74] But these evaluations had little connection to the respondents' evaluations of what should be criminal. For example, although checking the weather report from work was generally considered unauthorized, sixty percent thought it should not be punishable at all and another thirty-two percent concluded that it should only be punished like a parking ticket.[75] Where clear trespass norms exist, we would expect most to say that violating them should subject the trespasser to at least some criminal punishment. Kugler's results suggest that lay judgments of authorization probably do not accurately measure trespass norms, at least to the extent such norms now exist.

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. One plausible response from courts could be to refuse to go along. If the law rests on unknown norms, perhaps courts should strike down unauthorized access statutes as unconstitutionally void for vagueness—or at least construe them narrowly in light of the vagueness concerns they present.[76] I have argued that position before,[77] and it retains significant force. However, the alternative path is for courts to draw lines based on the normatively desirable rules and standards that should govern Internet use. In the interim period before norms emerge, courts can identify the best rules to apply as a matter

---

72. Email from Matthew B. Kugler to Orin Kerr, Fred C. Stevenson Research Professor, George Washington Univ. Law Sch. (Nov. 13, 2015) (on file with the *Columbia Law Review*).

73. Kugler, Measuring Norms, supra note 70 (manuscript at 6).

74. Id. (manuscript at 14).

75. Id. Seventy-seven percent thought that selling trade secrets should be a serious crime like burglary, but of course, it already is: The crime is theft of trade secrets, a separate offense from computer trespass. See 18 U.S.C. § 1832 (2012).

76. See Kerr, Vagueness Challenges, supra note 5, at 1561 (arguing "CFAA requires courts to adopt narrow interpretations of the statute in light of the void-for-vagueness doctrine").

77. See id. at 1562 ("The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional.").

of policy. Judicial decisions in the near term can influence norms in the long term.

C. *Trespass Law Provides the Appropriate Framework to Resolve Computer Misuse, and Courts Can Meet the Challenge*

It is worth asking whether trespass provides the right framework to apply and if judges are up to the task. I think the answer to both questions is yes. Trespass provides an appropriate framework because it implies an essential balance. On one hand, protecting online privacy requires recognizing some boundary that individuals cannot cross. On the other hand, preserving the public value of the Internet requires identifying uses that individuals can enjoy without fear of criminal prosecution. Some cases are easy. Everyone agrees that guessing another person's password to access his private email without his permission should be considered a criminal invasion of privacy. Similarly, everyone agrees that visiting a public website with no access controls or written restrictions should be legal. The trespass structure is sensible. The real challenge is applying it.

I am optimistic that courts can identify and apply computer trespass norms using existing statutes. The very first federal appellate case on the meaning of authorization in the CFAA, *United States v. Morris*,[78] shows why. *Morris* offers an early example of how courts can identify norms of computer trespass using the same three inquiries that govern trespass in the physical world: the nature of the space, the means of entry, and the context of entry.

In the fall of 1988, Robert Tappan Morris, a computer science graduate student, crafted and released a program often called "the Internet worm."[79] Morris designed the worm to reveal the weak computer security in place on the Internet.[80] First, the program exploited what the court called a "hole or bug (an error)" in three different software programs.[81] And second, the program guessed passwords, "whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password."[82] Morris sent the worm from a computer at MIT, and it quickly spread around the world.[83] Morris was then charged with and convicted of "intentionally access[ing] a Federal interest computer without authorization."[84]

---

78. 928 F.2d 504 (2d Cir. 1991).

79. Id. at 505.

80. Id. ("The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered.").

81. Id. at 506 (internal quotation marks omitted).

82. Id.

83. Id.

84. Id. (convicting defendant under 18 U.S.C. § 1030(a)(5)(A) (1986)).

On appeal, the Second Circuit affirmed the conviction. Writing for the court, Judge Jon Newman found three reasons why the access was without authorization. First, the evidence at trial demonstrated "that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program."[85] Second, the worm exploited security flaws in software commands. "Morris did not use either of those features in any way related to their intended function."[86] Instead, Morris "found holes in both programs that permitted him a special and unauthorized access route into other computers."[87] Finally, the worm also guessed passwords, rendering access to those accounts unauthorized.[88]

Judge Newman's brief explanation of why the Internet worm had accessed computers without authorization contains all of the ingredients for the proper way to think about computer trespass. First, *Morris* addressed the nature of the virtual space. Although the computers were connected to each other, access was limited to (and based on) private accounts. A user needed an officially sanctioned account to access that particular machine. Much like houses on a row in a suburban street, the computers were linked to each other but required a key or special permission to jump from the inside of one to the inside of another.

Second, *Morris* focused on the means of entry. None of the programs, used as intended, were ways of gaining access to a private account. But the Internet worm exploited security flaws by using "holes" and "bugs" in the programs that permitted "special access" in a way that was contrary to the "intended function" of the commands.[89] Instead of gaining access through the virtual front door, the worm gained access by exploiting security flaws: It broke in through an open window instead. It gained entrance through a bug, not a feature.

Third, the *Morris* opinion focused on the context of entry. When the Internet worm accessed a private account with a password, it did so only by guessing that password.[90] Here the analogy to physical entry seems intuitive. Guessing a password is like picking a physical lock. A successful guess provides access, just like a successful lock pick does. But the access is not authorized because it does not come directly or indirectly from the property owner. The trespass norm governing locks is that access is permitted only to those who have been granted the key in a delegation of permission beginning with the owner. Password guessing is outside the norm and therefore unauthorized.

---

85. Id. at 510.
86. Id.
87. Id.
88. Id.
89. Id.
90. Id.

Morris provides a helpful model for how courts can adopt sensible and clear computer trespass norms even when faced with new facts. A quarter century later, courts can follow the *Morris* example. The remaining Parts offer more specific guidance on how courts can do that for important cases that arise in the context of the Web, as well as blocked, canceled, and shared accounts.

III. NORMS OF THE WORLD WIDE WEB

Many tricky questions interpreting computer trespass statutes involve use of the World Wide Web. The Web did not exist when Congress enacted the CFAA.[91] But it has quickly become an important—if not the *most* important—way people use the Internet. Identifying the trespass norms of the Web is difficult because there are two competing narratives in play. On one hand, the World Wide Web is open: By default, anyone can go to any website. On the other hand, website owners frequently put up speed bumps, barriers, and caveats to access that range from hidden website addresses and terms of use to limiting cookies and banning IP addresses.[92] The hard question is this: When should use of the Web in the face of such efforts render the use unauthorized?

This Part argues that courts should adopt presumptively open norms for the Web. The nature of the space is inherently open. Courts should match the open technology of the Web by applying an open trespass norm. Limited efforts to regulate access such as terms of use, hidden addresses, cookies, and IP blocks should be construed as merely speed bumps rather than virtual barriers. None of these methods should overcome the basic open nature of the Web. Access that bypasses these regulations should still be authorized.

The authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement. An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web. This line achieves an appropriate balance for computer trespass law. It protects privacy when meaningful steps are taken to seal off access from the public while also creating public rights to use the Internet free from fear of prosecution.[93]

---

91. Tim Berners-Lee invented the World Wide Web in 1990, and the first browser was introduced in 1993. See Berners-Lee & Fischetti, supra note 56, at 69 (recounting history of first web browsers).

92. See infra section III.B (discussing authorized web access).

93. The CFAA sometimes distinguishes between violations of the CFAA based on "access without authorization" and violations based on acts that "exceed[] authorized access." Compare 18 U.S.C. § 1030(a)(2) (2012) (prohibiting actors from both kinds of violations when actors obtain information), with id. § 1030(a)(5)(B) (prohibiting only access without authorization when it results in damage). I agree with the conclusion of the Second and Ninth Circuits that the two forms of liability cover the same acts. See United States v. Valle, 807 F.3d 508, 524–28 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854,

A. *The Inherent Openness of the Web*

The first step in applying computer trespass law to the Web is to identify the nature of the space that the Web creates. The Web is a publishing protocol for the Internet. It allows anyone in the world to publish information that can be accessed by anyone else without requiring authentication. When a computer owner decides to host a web server, making files available over the Web, the default is to enable the general public to access those files. A user who surfs the Web enters an address into the prompt at the top of the browser, directing the browser to send a request for data.[94] If the address entered is correct, the web server will respond with data that the user's browser then reassembles into a webpage.[95]

This process is open to all. The computer doesn't care who drops by. By default, all visitors get service. In the language of the computer science literature, there is no authentication requirement.[96] A visitor might be any one of the billion or so Internet users around the world. For that matter, the visitor doesn't need to be a person. It could be a "bot," a computer program running automatically. It could even be a dog, as the famous *New Yorker* cartoon reminds us.[97] Because there is no authentication requirement, the web server welcomes all, and the norm is openness to the world. Access is inherently authorized.

The open nature of the Web is no accident; it is a fundamental part of the Web's technological design. From its inception in 1969, the creators of the Internet used "Requests for Comments" (RFCs) to describe the basic workings of different Internet protocols.[98] The Internet Engineering

---

858 (9th Cir. 2012) (en banc). That is, a person who violates a trespass norm to gain access to a computer commits an access without authorization if he has no authorization to access the computer, while he exceeds authorized access if he violates a trespass norm to gain a new level of access to a computer that he has some prior authorization to access. Both prohibitions implicate the trespass norms discussed in this Essay in the same way. The only difference is whether the defendant had some prior authorization to access the computer before violating the trespass norm. See Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1662–63 & n.283 (2003) [hereinafter Kerr, Cybercrime's Scope] (advocating such interpretation). For these reasons, my proposed approach applies equally to acts that constitute access without authorization and acts that exceed authorized access.

94. Preston Gralla, How the Internet Works 21–23, 31 (1998).

95. Id.

96. See generally William E. Burr, Donna F. Dodson & W. Timothy Polk, Nat'l Inst. of Standards & Tech., NIST Special Pub. 800-63, Version 1.0.2, Electronic Authentication Guideline (2006) (providing technical guidance to federal agencies on electronic authentication of users over open networks). Authentication requirements can be added, which changes the analysis. See infra section III.C (discussing implications of authentication requirements).

97. See Peter Steiner, Cartoon, On the Internet, Nobody Knows You're a Dog, New Yorker, July 5, 1993, at 61.

98. See Stephen D. Crocker, Opinion, How the Internet Got Its Rules, N.Y. Times (Apr. 6, 2009), http://www.nytimes.com/2009/04/07/opinion/07crocker.html (on file with the *Columbia Law Review*) (explaining history, function, and significance of RFCs).

Task Force later took over the task of crafting RFCs, and they stand as the definitive technical discussion of the intended function of different Internet applications. Think of them as computer-geek manuals for how the Internet works. The RFCs for the Web are RFC1945 and RFC2616.[99] They teach how the Web works, or more specifically, they teach how "Hypertext Transfer Protocol" (HTTP) works;[100] HTTP is one of the foundational protocols controlling data transfer between web servers and clients. And a quick review of the RFCs for the Web shows its inherently open nature.

RFC1945 and RFC2616 describe the protocol used for the Web as "a generic, stateless, object-oriented protocol"[101] for "distributed, collaborative, hypermedia information systems."[102] The means of operation are general and open. The Web works by allowing anyone to make a request for a webpage. As summarized in the RFCs, "[a] client establishes a connection with a server and sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers."[103] In English: Anyone can send a request without any authentication. And then, "the server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity metainformation, and possible body content."[104] Again, in English, the server responds to anyone who has made the request.

The protocols of the Web make websites akin to a public forum. To draw an analogy, websites are the cyber-equivalent of an open public square in the physical world. A person who connects a web server to the Internet agrees to let everyone access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale. 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.

B. *Authorized Access on the Web*

Although the Web is open by default, website operators often place limits and restrictions on access to information. The challenge for courts

99. T. Berners-Lee et al., Network Working Grp., Request for Comments: 1945, Internet Engineering Task Force (2006), http://tools.ietf.org/html/rfc1945 [http://perma.cc/PS74-4C3A] [hereinafter RFC1945]; T. Berners-Lee et al., Network Working Grp., Request for Comments: 2616, Internet Engineering Task Force (1999), http://www.ietf.org/rfc/rfc2616.txt [http://perma.cc/7MJN-PWFK] [hereinafter RFC2616].

100. RFC1945, supra note 99, at 1; RFC2616, supra note 99, at 1.

101. RFC1945, supra note 99, at 1.

102. RFC2616, supra note 99, at 7.

103. RFC1945, supra note 99, at 6.

104. Id. at 6–7.

is to distinguish provider-imposed restrictions and limits that are at most speed bumps (that cannot trigger trespass liability) from the real barriers to access (that can). In my view, an authentication requirement draws the proper line. When a limit or restriction does not require authentication, access is still open to all. The limit should be construed as insufficient to overcome the open nature of the Web. On the other hand, access that bypasses an authentication gate should, under proper circumstances, be deemed an unauthorized trespass. An authentication requirement provides a clear and easy-to-apply standard that both protects privacy and carves out public-access rights online.

A decade ago, I argued that unauthorized access should be limited to access that circumvents "code-based restrictions," which I defined as ways of tricking the computer into "giving the user greater privileges" when "computer code" has been used "to create a barrier designed to block the user from exceeding his privileges on the network."[105] With the benefit of hindsight, that formulation was vague. Trying to figure out when access circumvented a code-based restriction proved harder than I predicted. I now see that the more precise way to formulate the standard is that unauthorized access requires bypassing authentication. The key point is not that some code was circumvented but rather that the computer owner conditioned access on authentication of the user and the access was outside the authentication. This section covers examples of limits and restrictions on access that do not require authentication and should not trigger trespass liability.

Begin with a relatively simple case. Access to a website should be authorized even if the webpage address is not published or is not intended to be widely known. This issue arose in *United States v. Auernheimer*, in which the federal government charged the defendant with violating the CFAA by using a webscraper that queried website addresses that the computer owner, AT&T, had not expected people to find.[106] The website addresses queried were very difficult to guess because they ended in a long serial number. The defendant helped design a program to guess the numbers and collected information from over 100,000 website addresses.[107]

Had the Third Circuit reached the question,[108] it should have held that these website visits were authorized because the website had imposed no authentication requirement. The open norm of the Web still governed. Content published on the Web is open to all. Because the Web allows anyone to visit, a website owner necessarily assumes the risk that information published on the Web will be found. A hard-to-guess URL is

105. Kerr, Cybercrime's Scope, supra note 93, at 1644–46.

106. 748 F.3d 525, 530–31 (3d Cir. 2014) (presenting facts of case and criminal charges).

107. Id. at 531.

108. The Third Circuit did not reach the authorization question, as the court reversed the conviction on venue grounds. See id. at 532.

still a URL, and the information posted at that address is still posted and accessible to the world. Accessing the URL does not violate a trespass norm because all users are implicitly invited to access a publicly accessible address.

This conclusion is bolstered by the social value and ubiquitous nature of websurfing together with the severity and chilling effect of criminal punishment. We think, and therefore we Google. Courts should not lightly conclude that visiting an unwelcome URL should subject a person to arrest by federal agents and the potential for jail time. That is a particularly sensible approach because what looks like a hard-to-guess URL to a person may not seem hard to guess for a computer. To a computer, an address is an address. Even complicated addresses are easy for computers to find. Consequently, there is no workable line between an "easy" URL that can be accessed and one so hard to guess that access is implicitly forbidden.

The open understanding of the Web should also control access that violates terms of use.[109] Many websites come with terms of use that may on their face say when users are permitted to access the website.[110] The conditions can be arbitrary. One site might say that users must be eighteen years old to visit; another might say that users must agree to be polite.[111] Such terms should not be understood as controlling authorization. Access regulated only by written terms is not authenticated access. Everyone is let in, just subject to contractual restrictions. Such written terms should be understood as contractual waivers of liability rather than barriers to access.

This understanding is backed by the understandings of most website owners and users. Lawyers draft terms of use to minimize liability.[112] Broad terms allow computer owners to take action against abusive users and show good faith efforts to stop harmful practices occurring on the site.[113] True, terms of use may be drafted by lawyers to read like limitations on access. But companies do not actually expect the many visitors to otherwise-public websites to comply with the terms by keeping themselves

---

109. This was the issue first raised in United States v. Drew, 259 F.R.D. 449, 451 (C.D. Cal. 2009) ("This case raises the issue of whether . . . violations of an Internet website's terms of service constitute a crime under the [CFAA]." (footnote omitted)). Full disclosure: I represented Drew.

110. See United States v. Nosal, 676 F.3d 854, 861–62 (9th Cir. 2012) (providing examples).

111. See id. (listing specific details of various terms of use).

112. Consider this legal advice for franchisors who create websites:

> If a franchisor does decide to operate a site where it allows others to post content, it must address a number of issues. For example, it must take steps to avoid liability for copyright infringement, defamation, violation of privacy rights, and misappropriation of "hot news" and even criminal charges associated with such postings. It should, therefore, develop and publish comprehensive terms of use that prohibit inappropriate postings . . . .

Powell & Ralls, supra note 67, at 235 (footnotes omitted).

113. Id.

out.[114] And because terms can be arbitrary, violating them implies no culpable conduct.[115] If a public website has terms prohibiting access by people who are left-handed and enjoy opera, a left-handed opera lover who visits the site anyway does not deserve arrest and jail time.

This understanding is also backed by the experience of most computer users. Studies suggest that very few Internet users read terms of use.[116] (For the record, I don't.) Few users could understand them if they tried. Terms of use are often lengthy and filled with legalese.[117] The terms can be hard to find and difficult to interpret. Such terms don't restrict access to a computer any more than a standard waiver of rights on the back of a baseball game ticket could control rights to enter the ballpark. Violating the terms on the ticket might change your legal rights to sue the ballpark if something goes wrong, but it doesn't make your entry to the ballpark a trespass. Similarly, violating terms of use while accessing a website should not render the access a computer trespass.

The same rule should apply to the use of cookies to record prior visits and prompt paywalls. Cookies are pieces of code that websites can place on a browser to customize the user's experience.[118] Websites can use cookies to prompt repeat visitors to subscribe rather than visit for

---

114. In the *Drew* prosecution, for example, the government charged Drew with having participated in the creation of a MySpace profile that was not truthful in violation of MySpace's Terms of Use. *Drew*, 259 F.R.D. at 452 (listing charges on indictment, including setting up profile of "16 year old male juvenile named 'Josh Evans'"). Although the government presented the use of MySpace in violation of the terms as a trespass, it turned out that the co-founder of MySpace, Tom Anderson, whose MySpace profile greeted every new user, lied about his age in his own profile in violation of MySpace's Terms of Use. See Jessica Bennett, MySpace: How Old Is Tom?, Newsweek (Oct. 27, 2007, 11:22 AM), http://www.newsweek.com/myspace-how-old-tom-103043 [http://perma.cc/8FZS-28ZD] (reporting on Anderson's false age on his profile).

115. See Kerr, Cybercrime's Scope, supra note 93, at 1657–58 ("[A] qualitative difference exists between the culpability and threat to privacy and security raised by breach of a computer use contract on one hand, and circumvention of a code-based restriction on the other.").

116. According to one study, only 1.4% of users fully read end user license agreements (EULAs) for software programs, even though they require explicit agreement and generally require the user to claim she read the agreement. See Jens Grossklags & Nathan Good, Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers, http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-USEC.pdf [http://perma.cc/VP8S-RGVF] (last visited Jan. 26, 2016). The readership of terms of use on a website is likely much lower, as readers ordinarily are not prompted to do so and are less likely to see visiting a website as a significant occasion.

117. See Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 565 (2008) (concluding it would take hundreds of hours for typical consumer to actually read privacy policies encountered in one year of typical Internet use).

118. See In re Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 439–40 (D. Del. 2013) ("Cookies are used in internet advertising to store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services and web mail as individuals surf the internet.").

free. Consider the popular *New York Times* website, nytimes.com. When you visit the *Times* website, it places a cookie on your browser that records the visit.[119] The cookie allows the *Times* to meter access: If a browser is used to visit more than ten stories on the site in a month, the website brings up a screen blocking the reading of additional articles.[120] The point of the block is to pressure frequent readers to buy a subscription. But what if a reader regularly clears out his browser, which erases the cookie and enables unlimited access?[121] Is accessing the site after clearing out the browser unauthorized?

The answer should be that access enabled by erasing cookies is still authorized. Browsers are designed to give users control over what cookies are stored on their browsers.[122] Such cookies do not authenticate users: They merely allow users to customize their browsing experience. Users can accept cookies, reject cookies, or clear out the cookies kept in their browsers as often as they like.[123] They can use different browsers or different computers. As a result, user control of cookies is an expected and common way to use the Internet. They do not really limit access to computers; they only complicate access to the text of particular stories. Access limitations based on cookies are at most speed bumps rather than barriers. Instead of keeping people out, cookies-based barriers only impose enough of a hassle to encourage some users to buy a subscription.[124] Only the most unsophisticated users will see cookies as a barrier, and it will only be because they don't yet understand how cookies work.[125]

A more difficult case is raised by IP address blocking, which was the issue in *Craigslist v. 3Taps*.[126] Every device connected to the Internet has

---

119. Amit Agarwal, How to Bypass the *New York Times* Paywall (July 15, 2013), http://www.labnol.org/internet/nyt-paywall/18992 [http://perma.cc/R6XH-2GKD].

120. Id.

121. See id. (describing how to bypass *New York Times* paywall by deleting cookies).

122. This is the case with traditional browser cookies, at least. Different kinds of cookies may present different issues. See, e.g., Paul Lanois, Privacy in the Age of the Cloud, 15 J. Internet L. 3, 5 (2011) (discussing flash cookies).

123. For example, in the popular Chrome browser, users can go into "incognito" mode, which will not store cookies. Alternatively, they can delete all of the cookies stored on their browsers. See Laura, Google, Manage Your Cookies and Site Data, Chrome Help, http://support.google.com/chrome/answer/95647?hl=en [http://perma.cc/W262-45MU] (last visited Jan. 26, 2016) (describing how to delete cookies). Each step takes only seconds and is a common and expected part of surfing the Web.

124. See Danny Sullivan, The Leaky *New York Times* Paywall & How "Google Limits" Led to "Search Engine Limits," Search Engine Land (Mar. 22, 2011, 4:45 AM), http://searchengineland.com/leaky-new-york-times-paywall-google-limits-69302 [http://perma.cc/DW9Y-8KVZ] (describing shortcoming of *New York Times* paywall system).

125. The same principle also applies to browser restrictions based on "user agents," an issue that arose but was not resolved in the *Auernheimer* case. See Appellant's Amended Reply Brief at 13–14, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 13-1816), 2013 WL 6825411 ("Changing the user agent does not make a person guilty of trespass, whether that trespass is a physical trespass or the cyber trespass of the CFAA.").

126. 964 F. Supp. 2d 1178 (N.D. Cal. 2013).

an IP address, which is a number that represents the Internet address of that device.[127] Web servers communicate with users on the Internet by receiving requests and sending data to them at their IP addresses. In *3Taps*, the defendant business scraped ads from Craigslist and republished them on its own website.[128] Craigslist responded by sending 3Taps a cease-and-desist letter and by blocking the IP addresses associated with 3Taps's computers.[129] 3Taps changed its IP addresses to circumvent the IP block. Judge Charles Breyer ruled that 3Taps's access was an unauthorized access under the CFAA because "[a] person of ordinary intelligence would understand Craigslist's actions to be a revocation of authorization to access the website."[130] Judge Breyer explained:

> IP blocking may be an imperfect barrier to screening out a human being who can change his IP address, but it is a real barrier, and a clear signal from the computer owner to the person using the IP address that he is no longer authorized to access the website.[131]

Judge Breyer is wrong. Understood in the context of the open Web, an IP block is not a real barrier. A user's IP address is not fixed. For many users, the IP addresses of their devices will change periodically during normal use.[132] Using multiple computers often means using multiple IP addresses. A person might surf the Web from his phone (using his cell phone's IP address), from his laptop at home (using his home connection's IP address), and from work (using the company's IP address). Users also can easily change their IP addresses if they wish. For some users, turning on and off their modems at home will lead their IP addresses to change.[133] For more sophisticated users, accessing the Web using Tor or a virtual private network allows them to change their IP addresses with the click of a button.[134] There is nothing untoward or blameworthy about using different IP addresses. It is a routine part of using the Internet.

Because of these technical realities, bypassing an IP block is no more culpable than bending your neck to see around someone who has temporarily blocked your view. To be sure, an IP block indicates that the com-

---

127. E.g., id. at 1181 n.2.

128. Id. at 1180.

129. Id. at 1180–81.

130. Id. at 1186.

131. Id. at 1186 n.7.

132. Why Does Your IP Address Change Now and Then?, What Is My IP Address, http://whatismyipaddress.com/keeps-changing [http://perma.cc/QE8N-KDLB] (last visited Jan. 26, 2016).

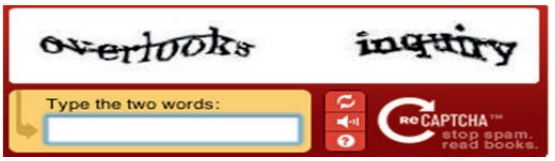
133. See How to Change Your IP Address, What Is My IP Address, http://whatismyipaddress.com/change-ip [http://perma.cc/9GLE-73RK] (last visited Jan. 26, 2016) (noting turning modem off and then back on will sometimes change IP address).

134. See Quentin Hardy, VPNs Dissolve National Boundaries Online, for Work and Movie-Watching, N.Y. Times: Bits Blog (Feb. 8, 2015, 5:30 AM), http://bits.blogs.nytimes.com/2015/02/08/in-ways-legal-and-illegal-vpn-technology-is-erasing-international-borders/ (on file with the *Columbia Law Review*) ("Millions of people around the world now pay for virtual private computer networks . . . to hook into a server in the United States.").

puter owner does not want at least someone at that IP address to visit the website. But that subjective desire is not enough to establish a criminal trespass in light of the open nature of the Web. A computer owner cannot both publish data to the world and yet keep specific users out just by expressing that intent. It is something like publishing a newspaper but then forbidding someone to read it. Publishing on the Web means publishing to all, and IP blocking cannot keep anyone out. Merely circumventing an IP block does not violate trespass norms.

A particularly tricky case is access that circumvents a CAPTCHA, an issue that arose in *United States v. Lowson*.[135] CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."[136] You have probably seen CAPTCHAs when buying tickets online or posting online comments. The website presents you with an image like this requiring you to type in the words before you can proceed:[137]

FIGURE 1: CAPTCHA EXAMPLE



The purpose of the CAPTCHA, as the full name suggests, is to allow humans in but to block computer "bots" that can make thousands of automated requests at once.[138]

The interesting question is whether use of an automated program to bypass the CAPTCHA by guessing or reading the words is an unauthorized access. The question is difficult because the technology shares some characteristics of a traditional authentication gate but not others. Like a password gate, it requires a code to be entered; but unlike a password gate, it presents the code to the user. Although it's a close case, I think the better answer is that automated bypassing of a CAPTCHA is not itself an unauthorized access. Although the CAPTCHA *looks* like a password gate, it does not operate like one. The site tells everyone the password. It invites all to enter.

---

135. No. 10-114 (KSH), 2010 WL 9552416 (D.N.J. Oct. 12, 2010).

136. E.g., Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1048 (N.D. Cal. 2010).

137. See CAPTCHA: Telling Humans and Computers Apart Automatically, CAPTCHA, http://www.captcha.net/ [http://perma.cc/9FHM-C62D] (last visited Jan. 26, 2016) (using this image as sample).

138. See id. (explaining usefulness of CAPTCHAs).

It is tempting to think that a CAPTCHA authenticates users as people instead of bots. But a "bot" request is still ultimately a request from a person. It is merely an automated request, with the person who used the software still responsible. That person could gain access and bypass the CAPTCHA manually by visiting the page and typing in the string of numbers that appear. As a result, a CAPTCHA is best understood as a way to slows a user's access rather than as a way to deny authorization to access. The CAPTCHA is a speed bump instead of a real barrier to access. Courts should hold that automated access is not a trespass merely because it bypasses a CAPTCHA.

Finally, it is worth considering the business implications of my proposed trespass rules. The examples in this section mostly involve businesses that might try to control customer use of their computers for business reasons. A ticket seller might use a CAPTCHA to limit scalpers, for example, just like the *New York Times* might use cookies to encourage readers to purchase subscriptions. That raises a fair question: If courts hold that these methods do not constitute a trespass, would that prevent businesses from using these methods—and if so, is that a policy reason to adopt different trespass norms?

The answer is that criminal trespass liability is unlikely to impact business strategies. Companies can already use civil contract law, based on terms of use, to set legal limits on how visitors use their websites.[139] Companies may not want to enforce those limits for a range of reasons.[140] But at least as a matter of law, often they can.[141] The scope of computer trespass laws implicates a different question: not just what user conduct is legal but what user acts are *criminal*. As a practical matter, it's hard to imagine a company using a business model that depends substantially on the prospect of the police arresting and prosecuting customers who circumvent speed bumps designed to regulate website use. Jailing customers for using a website isn't likely to be a good business strategy. It is telling that when the government has pursued aggressive criminal charges under the CFAA for use of websites, it has often been without the support of the companies claimed as victims.[142]

---

139. See, e.g., Ward v. TheLadders.com, Inc., 3 F. Supp. 3d 151, 162 (S.D.N.Y. 2014) (denying motion to dismiss in contract claim brought under website terms of use); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937–38 (E.D. Va. 2010) (evaluating contract claim based on website terms of use).

140. Suing customers is costly and can trigger negative press attention, making such suits rare even if website misuse is common.

141. See, e.g., *Ward*, 3 F. Supp. 3d at 162 (denying motion to dismiss claim based on violation of website's terms of use).

142. For example, in the Lori Drew case, which involved a CFAA prosecution for violating MySpace's Terms of Use, MySpace remained curiously silent throughout the case. See, e.g., Scott Glover & P.J. Huffstutter, 'Cyber Bully' Fraud Charges Filed in L.A., L.A. Times (May 16, 2008), http://articles.latimes.com/2008/may/16/local/me-myspace16 [http://perma.cc/6QY3-M9DX] (reporting on Drew's indictment and noting MySpace had not responded to request for comment). In the *Auernheimer* case, the victim, AT&T, was

C. *Unauthorized Access on the Web and the Authentication Requirement*

In contrast to the examples above, bypassing an authentication requirement should trigger liability for computer trespass. Even open spaces often have closed subspaces. Like a store open to the public in the front but for employees only in the back, the Web can have real barriers through which access violates trespass norms and is unauthorized. This moves the norms question from the first inquiry of the nature of the space to the second inquiry of the types of permitted entry. What counts as a real barrier on the Web, and what ways of overcoming those barriers are authorized? When a user bypasses an authentication requirement, either by using stolen credentials or bypassing security flaws to circumvent authentication, access should be considered an unauthorized trespass. This standard harnesses criminal law to protect privacy when network owners use technical means to enable access only to specific authenticated users.

The basic principle of authentication is probably intuitive to most Internet users. Every Internet user is familiar with the notion of an account that limits access. The requirement of credentials to identify the user is an authentication requirement.[143] When access to a computer requires an account, the user must register and obtain login credentials such as a username and password. Before allowing the user to access specific information, the user must establish that he is someone with special rights to access the account. A user who cannot satisfy the authentication requirement is blocked from access. The account structure imposes an access control that separates the insiders with accounts from outsiders without them. Because only the account holder should be able to satisfy the authentication requirement, the world—minus one user—is blocked. An authentication requirement creates a technical barrier to access by others. It carves out a virtual private space within the website or service that requires proper authentication to gain access.

Authentication requirements should be understood as the basic requirement of a trespass-triggering barrier on the Web. By limiting access to a specific person or group, the authentication requirement imposes a barrier that overrides the Web default of open access. The norm shifts from open to closed. At that stage, the emphasis shifts to means of access.

---

also quiet: At sentencing, when the probation office asked AT&T to detail its losses at sentencing, AT&T declined to respond. Brief of Defendant-Appellant at 52, United States v. Auernheimer, 748 F.3d 525 (3rd Cir. 2014) (No. 13-1816), 2013 WL 3488591. In the Aaron Swartz case, the victim, JSTOR, actively opposed the prosecution. See, e.g., Zach Carter et al., Aaron Swartz, Internet Pioneer, Found Dead Amid Prosecutor 'Bullying' in Unconventional Case, Huffington Post (Jan. 13, 2013), http://www.huffingtonpost.com/2013/01/12/aaron-swartz_n_2463726.html [http://perma.cc/VXS8-W4LM] ("JSTOR opposed prosecuting Swartz . . . .").

143. See generally William E. Burr, Donna F. Dodson & W. Timothy Polk, Nat'l Inst. of Standards & Tech., Electronic Authentication Guideline 12–13 (2006), http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf [http://perma.cc/VXS8-W4LM] (noting credentials are required part of e-authentication process).

Much like with a physical key to a door, access is authorized to the person who was given the password. On the other hand, as the *Morris* court noted, gaining access by guessing a password is just like picking a lock; both lack authorization.[144]

Exploits that circumvent authentication mechanisms or otherwise "break in" to systems are similarly unauthorized. *Morris* is again instructive. Access enabled by an exploit that uses a command in a way contrary to its intended function is unauthorized, much like entering through a window or a chimney in the physical world. For example, hacking techniques such as SQL injection attacks are unauthorized and illegal.[145] A Structural Query Language (SQL) injection attack is executed by attaching special extra language to the end of a web request.[146] Some web servers are misconfigured so that this extra language will execute a command on the web server rather than return a webpage.[147] The special command can provide access to the private database on the web server rather than just the pages to be published, providing the attacker with means to retrieve, alter, or delete the data.[148] Although a hacker using an SQL injection attack executes the injection by entering a command into a web browser—just like one would enter a username or password—the act exploits a security bug or hole just like the SENDMAIL flaw used in *Morris*. Access using an SQL injection is unauthorized for the same reason. An SQL injection attack is contrary to the intended function of the web browser: It violates the trespass norms surrounding the proper means of access to information on the server.

Importantly, the application of trespass norms can be technologically arbitrary even if they are socially meaningful. Consider the role of session cookies and persistent login cookies, which are browser cookies generated on a user's web browser during a typical login process to a website.[149] The website generates a long number associated with that login and passes the information back to the user's browser, with instructions for the browser to store it as a cookie.[150] When the user subsequently visits the website, the browser passes along the unique session-cookie value back to the website. Websites then use this information to automatically log in the user. You have likely benefited from these cookies when using web-based email, Amazon, or Facebook. After not visiting the page

144. United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991).

145. Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 858 (N.D. Cal. 2011).

146. E.g., Josh Shaul, Why Do SQL Injection Attacks Continue to Succeed?, SC Mag. (May 24, 2011), http://www.scmagazine.com/why-do-sqlinjectionattacks-continue-to-succeed/article/203679/ [http://perma.cc/PM4C-TECV].

147. Id.

148. Id.

149. Michael R. Siebecker, Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?, 76 S. Cal. L. Rev. 893, 897 (2003).

150. See id. at 897–90 (outlining process by which cookies are placed on computers, how they work once deposited, and purposes they serve).

for a few minutes or even a few days, you can go back to the website and it will automatically log you in. The website does this by reading your stored login or session cookie and matching it to an ongoing known login session.[151]

Now consider how computer trespass principles might apply to access made by hijacking such information. Imagine a third party intercepts a login cookie sent over the Web, loads it into his own browser, and visits the website. Use of the cookie will automatically log the third party into the user's email or Facebook account without the user's permission or knowledge. Is the third-party access authorized because it was obtained merely by sending on a specific cookie value as part of the browser's web request? Or is it unauthorized because it does so in a way that bypasses an authentication gate?

Unauthorized use of a persistent login cookie should be considered a violation of trespass norms. The cookie acts as a temporary password, tied to the user's permanent password, that identifies the account and provides access to it. It circumvents the password gate in exactly the same way that entering the permanent username and password would. The fact that the cookie is sent by the browser, which is normally an environment controlled by the user for the user's benefit, should not lead to a different result. This kind of cookie is an exception to the usual rule because it is a password; the embedding of the password in the browser does not change its function as a password.

The lines here are subtle, to be clear. Recall the *Auernheimer* case, where the information posted on a website was available only at a hard-to-guess website address.[152] The difference between a hard-to-guess website address, which should not act as an authentication gate, and a hard-to-guess session cookie, which should, is a matter of social understanding rather than technology. We can draw plausible lines about what acts as a password, but at some level the differences will boil down to shared understandings that some information is part of a public address while other information is a unique identifier. In close cases the technological arbitrariness is inevitable, as trespass norms are ultimately shared views about what invades another's private space and what doesn't. Technology alone cannot provide the answer.[153]

---

151. After a period of inactivity, the session may expire and the session cookie no longer works. At that point, the user must enter in the username and password to log in.

152. See supra notes 50–53 (discussing *Auernheimer* facts and issues).

153. Good security practices can help avoid the murkiest cases, however. For example, imagine a website required users to enter a secret password to enter the site but announced that the password was either "red" or "green." Such an example blurs the line between speed bump and authentication gate. But it is easy for website owners to avoid the blurry lines simply by having better authentication practices.

IV. CANCELED, BLOCKED, AND SHARED ACCOUNTS

The next set of questions asks how computer trespass statutes should apply to canceled, blocked, and shared accounts. These questions implicate the third way that norms control trespass, the identification of norms governing the context of permitted access. At this stage, authentication clearly implicates trespass liability. If a stranger guesses a victim's username and password and enters those credentials to access her account without permission, that access is plainly unauthorized.[154] On the other hand, if the user enters her own credentials to access her own private account, that access is authorized. The hard cases lie between these two poles.

The gray area involves three basic problems. First, a computer owner might revoke the user's right to access an account but not close the account. If the credentials still work, and the user continues to access the account using them, is that access authorized or unauthorized? Second, a computer owner might cancel access to a user's account, and the user might then respond by creating a new account on the same system unbeknownst to the owner. Is use of the new account authorized or unauthorized? Third, an account holder might share her username and password with a third party who accesses the account. Is the third-party access authorized because it was by permission of the account holder, or is it unauthorized because it was not actually accessed by the account holder? In these cases, the law must grapple with how authorization norms apply when account rights are terminated, modified, or shared with others.

This Part attempts to answer all three questions using the principle of authentication. As explained in Part III, authentication of a user authorizes the user to access the account but makes access by others unauthorized. The trespass norm should aim to preserve that delegation of authority. Again, the goal is to achieve an optimal balance. Overly restricting delegations would prevent beneficial uses of networks by authenticated users. On the other hand, permitting authenticated users to further delegate authority, or to ignore withdrawals of delegation, would nullify the owner's power to designate who can access the network. Applying this approach suggests three rules. First, suspending an account withdraws authorization to access the account. Second, a suspension may or may not signal that access to additional accounts is prohibited. Finally, use of shared passwords should be permitted only when the third party access is within the scope of agency of the authenticated user.

This Part concludes by discussing the role of mental states, or mens rea, on computer trespass liability. When authorization hinges on the context of access, the user often will not know the facts that determine whether access was authorized. In that context, the statutory requirement

---

154. See United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (discussing "unauthorized access" requirement).

that unauthorized access must be intentional or knowing plays an important role in narrowing criminal liability.

A. *Canceled Accounts*

The first issue is how trespass laws should apply when the authority to use an account has been revoked but the user accesses the account anyway. The answer should come from an understanding of what authentication means. By permitting an account that requires authentication, the computer owner should be understood to have delegated access rights to the authenticated user. The authenticated user has permission to access the account so long as the computer owner grants the account. The trespass norm should be to preserve that delegation. Preserving the delegation achieves the same dual goals as the authentication requirement provided in Part III. It enables use of computers (here, accounts held by authorized users) while affording them appropriate space to use their delegated accounts without fear of criminal prosecution for trespass.

Under this standard, the owner's revocation of the right to use an authenticated account revokes authorization. When the computer owner communicates the revocation to the user, the delegated authority ends. Subsequent account access violates trespass norms; it should be understood as entering a space where the user is no longer welcome. Because authority to use an authenticated account should exist only inside the zone of delegated power, ending the right to access the account should end the delegated right and end the authorization.

Courts have so far adopted this approach, as the Fourth Circuit's decision in *United States v. Steele*[155] demonstrates. Robert Steele worked as a backup system administrator at a business named SRA, and for work purposes he created a backdoor account that gave him access to SRA's network files.[156] After he resigned, Steele continued to use the account to access SRA's network. The Fourth Circuit ruled that "the fact that Steele no longer worked for SRA when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed."[157] Having left the company, Steele's rights to access the account were revoked: "Just because SRA neglected to change a password on Steele's backdoor account does not mean SRA intended for Steele to have continued access to its information."[158]

---

155. 595 F. App'x 208 (4th Cir. 2014).

156. Id. at 209–10.

157. Id. at 211.

158. Id. For a similar case reaching the same result, see United States v. Shahulhameed, No. 14-5718, 2015 WL 6219237, at *2 (6th Cir. Oct. 22, 2015) (holding employee's authorization to access his work account ended when he was informed by telephone and email that he was fired). The point was assumed by the parties and apparently accepted by the court in LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009) (noting

This approach implies a distinction between the rules that should apply to a user who violates terms of use and a user whose account is suspended for violating terms of use. Recall that a user who violates terms of use is not committing an unauthorized access.[159] On the other hand, I argue here that a user whose account is revoked for violating terms of use but uses the banned account anyway is guilty of trespass. The distinction is justified because violating terms of use merely provides legal justification for revocation if the website owner chooses to do so. When a website owner authorizes an account for a user, the user has access rights unless the account is actually revoked. The authority is delegated by the issuing of the account and withdrawn by its revocation, so the act of revocation is needed to undo the act of granting the account.

B. *New Accounts Following the Banning of an Old Account*

Next imagine that the computer owner cancels or blocks the account but the user can readily sign up for a new one. Imagine Gmail suspended your email account for violating Gmail's terms of use and you want to open another Gmail account the next day or the next year. Does the company's blocking the first account deny authorization to set up a second account? Or is the user free to start again after having been blocked once—or twice, or three times, or even hundreds of times?

This problem arose in the controversial case of *United States v. Swartz*.[160] The Internet activist Aaron Swartz created a guest account on MIT's network and used it to download a massive number of academic articles to his laptop.[161] Network administrators canceled the guest account in response; Swartz created a new guest account.[162] When system administrators blocked access through the new guest account, Swartz then figured out a way to circumvent guest-account registration: He found a closet in the basement of one of MIT's buildings that stored the server, entered it, and hard-wired his computer to the network.[163] He then assigned himself two new IP addresses from which he could con-

---

"[t]here is no dispute" that if employee accessed company computer after leaving company then employee "would have accessed a protected computer 'without authorization' for purposes of the CFAA").

159. See *Morris*, 928 F.2d at 511 (discussing meaning of "unauthorized access").

160. Indictment, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011). Swartz committed suicide before his case went to trial. John Schwartz, Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide, N.Y. Times (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html (on file with the *Columbia Law Review*). I will assume the facts in the indictment are true.

161. Indictment at 4–5, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011).

162. See id. at 4 (noting computer was registered under "fictitious guest name 'Gary Host'").

163. See id. at 8–9 (describing observation of Swartz "entering the restricted basement network wiring closet" and "attempt[ing] to evade identification").

tinue his access.[164] The question was, did having been blocked with an account once mean that subsequent efforts to obtain access were unauthorized?

As before, the legal line should track the delegation of authority implied by authentication. The application of that principle is trickier, however, because the revocation of delegated authority is less obvious. When anyone can open an account, there is an implicit delegation to anyone who registers for a new account. In some contexts, a single act of blocking does not imply a total and permanent revocation. In other contexts, it does. For example, a user who has an account suspended for misconduct may be perfectly welcome to start again with a new account on the understanding that no further misconduct continues. On the other hand, users who are repeatedly banned eventually must get the message that they are not welcome.

The key question should be the objective signal sent by the banning or suspension, which will in some contexts allow the user to create a new account but in other contexts won't. When the ban would be reasonably interpreted as "don't do *that*," creating a new account and using it properly is authorized. When the ban would be reasonably interpreted as "go away and never come back," creating another account is unauthorized. In the *Swartz* case, for example, access would have been unauthorized by the time Swartz entered the closet to circumvent IP registration. Having had his accounts blocked multiple times by MIT's system administrators for violating the rules on MIT's network, Swartz had received clear signals that he was no longer welcome to create another account to continue the same conduct.

This approach once again ends up drawing a subtle distinction. Recall my earlier conclusion that an IP block is insufficient to trigger trespass liability.[165] Circumventing an IP address ban is permitted and authorized. At the same time, I am arguing here that if the computer owner requires an account to access a computer and then bans the account, circumventing that ban might not be authorized if the context can be interpreted as a complete ban. Is there really a difference? I think there is. Everyone can visit a public website, while not everyone can have the privilege of an account. By creating the access control of an account regime, the computer owner takes control of who can access it by making individualized decisions about specific accounts. A suspended account is not just a speed bump. It's a block to using that account and a potential signal about opening another one. The rules governing the two cases should be different.

---

164. Id. at 7–8.

165. See supra notes 126–134 and accompanying text (discussing trespass liability for circumventing IP blocks).

C. *Password Sharing*

The last and most difficult issue is identifying trespass norms that should govern shared passwords. Consider the facts of *United States v. Rich*.[166] A financial-services company, LendingTree, sold valuable access to financial information on its website to customers who paid a fee and received a username and password to access the site.[167] The defendant, Brian Rich, made a side deal with an employee at one of LendingTree's customers; he agreed to pay the employee to get the company username and password.[168] Rich then used the credentials to access the LendingTree website without paying LendingTree.[169] The question is: Does using a shared password constitute an unauthorized access in violation of trespass norms?

The starting point should again be that the computer owner's granting of an authenticated account delegated access rights to the account holder. The account holder is authorized but others are not. To preserve this principle, the trespass norm should be that access by the account holder or his agent is authorized while other access to the account is not.[170] When the account holder gives login credentials to a third party, access by the third party is authorized only when the third party acts as the agent of the account holder.

This approach mirrors the analogous rule in the physical world. When access is limited by a physical lock and key, whether entry is a physical trespass law depends on whether it falls within the zone of permission granted by the owner.[171] For example, in *Douglas v. Humble Oil & Refining Co.*, a business owner gave an employee the key to his home so the employee could feed his pets when he was away.[172] The employee later used the key to enter the home for a different reason. According to the court, this entry for reasons outside the scope of permission was a trespass.[173]

This approach allows computer account holders to share usernames and passwords with an agent. If the agent accesses the account on the account holder's behalf, the agent is acting in the place of the account holder and is authorized. The agent then has the same authorization

---

166. 610 F. App'x 334 (4th Cir. 2015).

167. Brief of Appellant at 3, *Rich*, 610 F. App'x 334 (No. 14-4774), 2015 WL 860788, at *9.

168. Id. at 4.

169. Id.

170. See generally Restatement (Third) of Agency § 1.01 (Am. Law Inst. 2006) (defining agent).

171. See, e.g., Rich v. Tite-Knot Pine Mill, 421 P.2d 370, 374 (Or. 1966) (noting "one who originally enters the premises as a licensee may forfeit his license and become a trespasser if he exceeds its scope").

172. 445 P.2d 590, 591 (Or. 1968) (en banc).

173. See id. ("The undisputed evidence was that the only purpose for which Douglas had authorized his employee to use the house key was to attend to the feeding of the Douglas's household pets.").

rights as the account holder. For example, I recently set up a Gmail account for my students to email class assignments. I gave my assistant the account password and asked her go into the email inbox and collect them for me. When she did so, she was acting as my agent. Legally speaking, she was me.[174] She was fully authorized to access the account in her capacity as my agent. Her conduct was authorized and legal, much like employee access to an employer's account for work purposes.

On the other hand, a third party who uses a password in pursuit of her own ends stands in the same place as a third party who has guessed or stolen the password. Consider the facts of *Rich*.[175] When Rich accessed the LendingTree website using a password, he was not acting as an agent of a legitimate customer. Rich paid for access to the password, but he did not pay LendingTree. Instead, he paid an employee of a legitimate customer. Rich accessed the account to help himself get richer, not to help the employee. From the perspective of LendingTree, Rich's access was no different from access using a guessed or stolen password. Rich was not a legitimate customer or an agent of a legitimate customer. Whether he obtained the password by stealing it from the employee or by paying for it makes no difference to LendingTree. For that reason, Rich's access was unauthorized.

Two wrinkles need to be ironed out. First, what is the impact of terms of use to the delegated authority of the computer owner? Recall my use of a Gmail account for class. What if Gmail's Terms of Use forbid password sharing and my secretary's access violates those Terms?[176] In my view, terms of use barring shared access should be irrelevant for the same reason they are irrelevant to access more generally. As explained earlier, terms of use create rights for the computer owner rather than the account holder.[177] When terms are violated, the computer owner can suspend or restrict the account. But violating the terms does not render access an unauthorized trespass either in the context of public access websites or of specific accounts. By granting a user an account, the computer owner necessarily grants the user authorization to access the account for any reason.

Second, note that my treatment of the delegation from the computer owner to an account holder is different from my treatment of the delegation from the account holder to a third party. When authorized by the computer owner, the account holder has full access rights. When au-

---

174. See State ex rel. Coffelt v. Hartford Accident & Indem. Co., 314 S.W.2d 161, 163 (Tenn. Ct. App. 1958) ("The basis for holding the principal for the acts of his agent is that the agent acts as the principal's *alter ego* or other self.").

175. United States v. Rich, 610 F. App'x 334, 335–36 (4th Cir. 2015).

176. They don't, at least right now. See Google Terms of Service, Google (Apr. 14, 2014), http://www.google.com/intl/en/policies/terms/ [http://perma.cc/7T2J-PEQL] (including warning to "keep your password confidential" but refraining from enacting formal requirement).

177. See supra section III.B (discussing legal implications of terms of use).

thorized by the account holder, on the other hand, the third party has narrower rights only to act as the account holder's agent. This distinction is justified by the underlying role of an authentication requirement. Setting up the authentication gate and granting a user account confers rights on the account holder and her agents. An account holder should have only a narrower power to confer access rights because otherwise that delegation would interfere with the original authentication. If computer owner A can confer access rights to account holder B, an unlimited power of B to confer access rights to C, D, and E would nullify A's judgment to confer access rights to only account holder B. The rule should be that third-party access outside the agency relationship is unauthorized access.

D. *The Critical Role of Mens Rea*

The problem of canceled, blocked, and shared accounts is not complete without understanding the associated mental state, or mens rea, that accompanies computer trespass statutes.[178] The problem here is with the fact-sensitive context of permitted entry. The facts relevant to authorization may not be known to the user. In this context, the mental state of authorization plays a critical role. Computer trespass statutes generally require that the user commit an intentional or knowing unauthorized access.[179] The government's burden to prove that an unauthorized access was intentional or knowing plays a crucial role in establishing a limit on liability when authorization is lacking due to the context of entry.

Courts have not explored the role of mental state in establishing liability for computer trespass, so it is important to understand what a mental state or knowledge or intent might mean in this context. Consider the broadest section of the CFAA, which prohibits "intentionally access[ing] a computer without authorization" or intentionally "exceeding authorized access."[180] The intent requirement plainly applies to the element that authorization is lacking. But does the requirement of intent with respect to lack of authorization require intent as to the legal conclusion that access is unauthorized, or does it merely mean intent as to the facts that make access legally unauthorized?

---

178. For an introduction to mens rea, see generally Joshua Dressler, Understanding Criminal Law 117–36 (6th ed. 2012).

179. See, e.g., 18 U.S.C. § 1030(a)(2) (2012) (prohibiting intentional access without authorization or exceeding authorized access); Cal. Penal Code § 502(c)(7) (West 2010) (prohibiting "access[] to "any computer, computer system, or computer network" that is "[k]nowing[] and without permission"); Colo. Rev. Stat. Ann. § 18-5.5-102 (West 2013) (prohibiting knowing access without authorization or exceeding authorized access).

180. 18 U.S.C. § 1030(a)(2).

Courts have not addressed the question, and it is surprisingly complex.[181] The usual rule, however, is that a knowledge or intent requirement for a criminal element requires knowledge or intent about the facts that are legally relevant to the element rather than to a legal status the element implies.[182] It is not entirely free from doubt that this rule applies to computer trespass statutes,[183] although it is often enough the default rule in federal criminal law that it seems likely to apply at least to the CFAA.[184] Applying the usual rule to computer trespass statutes, proving intentional unauthorized access likely requires the government to show that the defendant knew of or hoped for the facts legally relevant to authorization and intentionally accessed the computer anyway. The prosecution need not prove that the defendant knew or intended his conduct

---

181. See generally Kenneth W. Simons, Ignorance and Mistake of Criminal Law, Noncriminal Law, and Fact, 9 Ohio St. J. Crim. L. 487 (2012) (exploring difficulty raised by mental states with respect to criminal elements having aspects of both law and fact).

182. See, e.g., McFadden v. United States, 135 S. Ct. 2298, 2304 (2015) (holding, in prosecutions for knowingly distributing a controlled substance, government must prove either that defendant knew substance he distributed was on list of controlled substances or that defendant "knew the identity of the substance he possessed" and it was on the controlled-substances list); Elonis v. United States, 135 S. Ct. 2001, 2009 (2015) ("[A] defendant generally must know the facts that make his conduct fit the definition of the offense even if he does not know that those facts give rise to a crime." (citations omitted) (internal quotation marks omitted) (quoting Staples v. United States, 511 U.S. 600, 607 n.3 (1994))); Morissette v. United States, 342 U.S. 246, 271 (1952) ("He must have had knowledge of the facts, though not necessarily the law, that made the taking a conversion."); United States v. Brown, 669 F.3d 10, 19–20 (1st Cir. 2012) (ruling, in prosecution for intentionally thwarting officers in course of their official duties, it was irrelevant that defendant believed officers were enforcing unconstitutional law and that therefore officers were not acting in course of their official duties).

183. For example, in *Liparota v. United States*, the Court construed a statute that punished knowingly using or possessing food stamps in a way unauthorized by law as requiring knowledge that the use or possession was legally unauthorized. 471 U.S. 419, 433 (1985). Applying *Liparota*, it could be argued that intentional unauthorized access also requires intent—here, awareness or hope—about the act being legally unauthorized. This might be bolstered by the text of physical trespass statutes, which often plainly requires knowledge that presence is legally unauthorized. See, e.g., Model Penal Code § 221.2(2) (Am. Law Inst. 2015) ("A person commits an offense if, knowing that he is not licensed or privileged to do so, he enters or remains in any place as to which notice against trespass is given . . . ."). *Liparota* is potentially distinguishable, however, because the lack of authorization in the computer trespass statute concerns lack of authorization with respect to the relevant norms, not the relevant law. Further, not all physical-trespass statutes have required knowledge as to the absence of legal privilege. See, e.g., N.J. Stat. Ann. § 2A:170-31 (repealed 1979).

184. See supra notes 160–164 (discussing defendant's knowledge of facts in *United States v. Swartz*). This is bolstered by the common use of "willfulness" in federal criminal statutes to indicate knowing violation of a legal duty, see, e.g., Cheek v. United States, 498 U.S. 192, 193 (1991) (applying willfulness standard to failure to file federal income tax return), a use that does not appear in the CFAA. A 1986 Senate report has a brief discussion of the purpose of changing the mental state for unauthorized access from knowing to intentional. S. Rep. No. 99-432, at 5–6 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2483–84. The discussion is unclear and can be read as supporting either position.

to be legally unauthorized. Instead, the key question is the defendant's state of mind about the facts that, once the law is understood, made the access unauthorized.

So construed, the mental state requirement of computer trespass has a significant narrowing effect on liability for using canceled, blocked, and shared accounts. The individual must not only take steps that are contrary to the delegated authority; he must know or hope that his steps are contrary to that delegated authority. Recall the *Steele* case, in which the ex-employee used the backdoor account after he had resigned.[185] Steele obviously knew that the authority to access the account had been revoked: As the Fourth Circuit explained, the company had taken his work laptop, denied him physical access to the building, and made him sign a letter that he would not try to access the employer's network in the future.[186] In other cases, however, the revocation might not be so clear. The ex-employee might not know that her access rights to the account had been revoked. In such a case, she would not be guilty of criminal computer trespass.

The mental state requirement is particularly important in cases that involve shared passwords. If B shares a password with C, C's access is without authorization when C is acting outside the agency of B. At the same time, C's access is intentionally without authorization only if C knows or hopes of facts that would bring C*'s* access outside the agency of B. In many cases, C may not know how B uses the account, how often, or for what. C's state of mind about whether C is outside the agency relationship element may sharply limit C*'s* liability.

For example, imagine Ann gives Bob her Netflix username and password and tells Bob to feel free to use her account. Bob then uses Ann's account as if it were his own. Whether Bob's use of Ann's account is outside the agency relationship is itself a murky question: General permission to use the account whenever Bob likes implies a broad or even perhaps limitless authorization. But that murkiness aside, Bob can't be criminally liable for accessing Ann's account unless he knows or hopes that his acts are outside Ann's authorization. In the usual case, Bob would lack intent to access the account without authorization.[187]

CONCLUSION

Applying law to the Internet often rests on analogies. In litigation, each side will offer analogies that push the decisionmaker in a particular direction. Courts faced with competing analogies must know how to de-

185. United States v. Steele, 595 F. App'x 208 (4th Cir. 2014).

186. Id. at 211.

187. If courts construe the intent requirement as going to the legal conclusion that authorization is lacking, then the mental state requirement has an even more dramatic effect. It would prohibit liability unless the government can prove beyond a reasonable doubt that the defendant knew or hoped that his conduct was unlawful.

cide between them: How do you know whether Internet facts are more like one set of facts from the physical world or another?

This Essay can be understood as a conceptual guide to choosing analogies in the interpretation of computer trespass statutes. By appreciating the role of norms in the interpretation of physical trespass laws, courts can adopt sensible rules based on technological realities and their social construction. Because computer-network norms remain largely unsettled, the task is normative rather than descriptive. Judicial identification of the best norms to apply can help bring public acceptance of those norms, or at least provide a temporary set of answers until real norms emerge.

This approach helps avoid analogies that mislead rather than inform by missing the underlying norms that make analogies fit. Applying physical-world trespass cases to the Internet without first considering the difference between the physical and network worlds risks applying precedents from an environment with one norm to an environment that merits a very different one.