William & Mary Law Review

Volume 62 (2020-2021)
Issue 2

Article 5

11-2020

Criminal Trespass and Computer Crime

Laurent Sacharoff

CRIMINAL TRESPASS AND COMPUTER CRIME

LAURENT SACHAROFF*

ABSTRACT

The Computer Fraud and Abuse Act (CFAA) criminalizes the simple act of trespass upon a computer—intentional access without authorization. The law sweeps too broadly, but the courts and scholars seeking to fix it look in the wrong place. They uniformly focus on the term "without authorization" when instead they should focus on the statute's mens rea. On a conceptual level, courts and scholars understand that the CFAA is a criminal law, of course, but fail to interpret it comprehensively as one.

This Article begins the first sustained treatment of the CFAA as a criminal law, with a full elaboration of the appropriate mens rea based upon congressional intent, cognate state criminal trespass statutes, and recent Supreme Court guidance on federal mens rea in general. A fully realized mens rea sweeps away many of the unjust potential applications of the CFAA on a far more principled basis than does a focus on, and re-writing of, "without authorization."

My interpretative approach limits unjust applications of the provision, but many will remain. In a coda, I briefly show why we should likely abolish the trespass provision of the CFAA. The flaws of the CFAA, such as criminalizing ordinary and innocent behavior and arbitrary enforcement, flow from the same pathologies already inherent in criminal trespass law.

---

* Professor of Law, University of Arkansas School of Law, Fayetteville; J.D., Columbia Law School; B.A., Princeton University. The author would like to thank Orin Kerr, Ric Simmons, Alan Trammell, Thomas E. Kadri, the participants of the CrimFest! Workshop, as well as Hannah Hungate for research assistance.

TABLE OF CONTENTS

INTRODUCTION

The Computer Fraud and Abuse Act (CFAA) criminalizes the simple act of computer trespass.[1] It targets anyone who "intentionally accesses a computer without authorization."[2] The defendant need not have a bad motive or an intent to gain, nor cause any harm or damage to the computer or its owner. This simple trespass provision, section 1030(a)(2)(C), remains the most frequently charged crime of the CFAA subsections.[3] It is also the most frequent count in analogous civil lawsuits.[4]

Scholars[5] and courts[6] have rightly sounded the alarm at the apparent breadth of this trespass provision and its potential to criminalize everyday behavior. They have pointed to the term "without authorization" as the culprit. They call it vague and unconstitutional; they say it fails to provide notice, especially when it rests upon obscure terms of service.[7] For example, Facebook's terms of service prohibit those under thirteen years old from creating an account.[8] If a twelve-year-old child creates a Facebook account, has she committed a federal crime because she "access[ed] a computer without authorization"?[9]

Many of these scholars have long advocated for a particular solution: courts should hold that terms of service can never establish

---

1. 18 U.S.C. § 1030.

2. *Id.* § 1030(a)(2). Subsection (a)(2)(C) lists two further elements, using the access to "obtain[ ] ... information from any protected computer," but these two additional elements are always met for any computer connected to the internet.

3. Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1493 (2016) (finding 47 percent of all CFAA criminal cases charge simple computer trespass).

4. *Id.* at 1487 (finding 67 percent of all CFAA civil filings claim simple computer trespass).

5. *E.g.*, Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1472-73 (2016); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1598-99 (2003); Mayer, *supra* note 3, at 1463 n.32 (collecting scholars' critiques of the CFAA as "overbroad or overly punitive").

6. *See, e.g.*, United States v. Nosal (*Nosal I*), 676 F.3d 854, 860 (9th Cir. 2012); United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009).

7. *See infra* Part II.A.

8. *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/6Z58-S4U7].

9. *Cf. Nosal I*, 676 F.3d at 861.

that access is without authorization.[10] Instead, many have argued for a code-based test. Access is without authorization only if the intruder circumvented some code-based barrier, such as hacking a password.[11]

Until very recently, courts had flirted with this code-based test, but declined to formally adopt it.[12] Then in September 2019 came a bombshell. The Ninth Circuit in *hiQ Labs v. LinkedIn* adopted, in part, this code-based test.[13] The court held that accessing a site to scrape millions of profiles against the express wishes of the platform likely does not violate the CFAA because the information is not protected by a password login or other authentication mechanism.[14]

Courts and scholars misdiagnose the problem as arising from the element "without authorization" and propose the wrong solution in the form of a code-based test.[15] At the same time, they often ignore the mens rea requirement of the statute[16] or fail to recognize its full potential.[17] Orin Kerr has highlighted this problem: "Courts have not explored the role of mental state in establishing liability for computer trespass."[18]

This Article, therefore, argues that we should focus on the mens rea of the CFAA. Doing so will exempt from prosecution the vast majority of examples given as potential unjust applications of the

---

10. *See infra* Part II.A.

11. *See, e.g.*, Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1161 (2016).

12. *See* Bellia, *supra* note 5, at 1468-69; Mayer, *supra* note 3, at 1503.

13. 938 F.3d 985, 1003 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

14. *See id.* at 1003-04. The Ninth Circuit reviewed a preliminary injunction and thus only ruled that the plaintiff was likely to prevail on the merits. *See id.* at 1005. Nonetheless, I treat the holding as though it were on the merits.

15. *See infra* Part II.

16. *See, e.g.*, *Nosal I*, 676 F.3d 854 (9th Cir. 2012) (making no mention of mens rea).

17. *E.g.*, United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (discussing mens rea but failing to give it appropriate effect); Bellia, *supra* note 5, at 1470 (defining the "scienter" requirement as "knows or has reason to know" rather than "knows"); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1479 (2016) (using "knew or should have known"). *But see* William A. Hall, Jr., *The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in* United States v. Nosal, 84 GEO. WASH. L. REV. 1523, 1529-30 (2016) (emphasizing a mens rea of *knowingly* in exceeding authorized access cases); Kerr, *supra* note 11, at 1180 (noting the "critical role" of mens rea in interpreting the CFAA).

18. Kerr, *supra* note 11, at 1180.

CFAA. When properly interpreted, the CFAA applies a mens rea of *knowingly* to the statute's element "without authorization." An individual must *know* that her intrusion is "without authorization." This stringent mens rea requirement will spare the unwitting twelve-year-old Facebook user who creates an account unaware of the prohibition.

Now the text of the CFAA uses the mens rea term "intentionally."[19] But, as I detail below, this term collapses into *knowingly* when applied to "without authorization."[20]

A proper appreciation of the CFAA's mens rea of *knowingly* leads to several conclusions. First, it undermines the common argument that "without authorization" in the CFAA is unconstitutionally vague because that argument rests primarily on lack of notice. A mens rea of *knowingly* means that an individual does have actual notice that her access is without authorization. Indeed, in the physical world, court after court has held that criminal trespass laws are not unconstitutionally vague.[21] "Without authorization" is perfectly comprehensible—it means "stay out."[22]

Second, a mens rea of *knowingly* imports a kind of mistake of law defense into the CFAA. Suppose an individual lacks authorization because of operation of some other law, regulation, or even simply a proper interpretation of a platform's terms of service. The mens rea of *knowingly* requires that the defendant be aware of these other sources, such as some other law, and subjectively understand that this other law, regulation, or term of service prohibits her access.

---

19. *See* 18 U.S.C. § 1030(a)(2).

20. Congress relied upon the Model Penal Code in drafting the CFAA, *see infra* notes 204-05 and accompanying text, and the Model Penal Code, in turn, justifies applying a mens rea of *knowingly* to "without authorization." MODEL PENAL CODE § 2.02(2)(a)(ii), (2)(b)(i), (4) (AM. L. INST. 1962).

21. *See, e.g.*, Adderley v. Florida, 385 U.S. 39, 42 (1966); Downer v. State, 375 So. 2d 840, 843 (Fla. 1979) ("We conclude that ['authorized' is] of such common understanding and usage that persons of ordinary intelligence are fully able to determine what conduct is proscribed by the challenged enactment."), *habeas corpus granted sub nom.* Cohen v. Katsaris, 530 F. Supp. 1092 (N.D. Fla. 1982); *see also infra* notes 306-08 and accompanying text.

22. Rayburn v. State, 300 S.E.2d 499, 500 (Ga. 1983) (holding that a trespass statute was not unconstitutionally vague and that a warning to "stay out" provided sufficient notice that presence was unauthorized); *see also, e.g.*, Martin v. City of Struthers, 319 U.S. 141, 147 (1943); Bowman v. United States, 212 A.2d 610, 611 (D.C. 1965); WAYNE LAFAVE, SUBSTANTIVE CRIMINAL LAW § 21.2(a) (3d ed. 2019).

She must grasp that the *effect* of this other law is to revoke her authorization.[23]

Third, this Article shows that federal courts often instruct juries incorrectly concerning mens rea. Judges leave juries unaware they must find that the defendant *knew* her access was without authorization or that she exceeded authorization.[24] The jury instructions instead suggest that the government must prove that the defendant's intent related to the conduct of accessing the computer only, and if that intentional access was also without authorization, the defendant is guilty—without the additional showing that the defendant *knew* she lacked authorization. Below I illustrate this critical failure with an Eleventh Circuit case pending before the Supreme Court in its October 2020 term, *Van Buren v. United States*.[25]

Finally, this mens rea of *knowingly* will render unnecessary a code-based regime. True, if a person hacks into a system, that fact might be strong evidence that she knew her access was without authorization, but the touchstone remains knowledge. A hack is neither necessary nor sufficient to establish knowledge and is therefore not an appropriate test.

To support my interpretation of the CFAA, this Article dives deeply into the statute's text, legislative history, and reliance on the Model Penal Code. This Article has the advantage of the Court's recent pronouncement on federal mens rea in *Rehaif v. United States* and applies its holding and analogous reasoning here. It also carefully considers state criminal trespass laws in the physical world to lend further support to the mens rea approach.[26]

My proposal will greatly simplify the case law muddied by a focus on "without authorization" and courts' baroque redefinition of that

---

23. Mistake of law is not always a defense, of course, but the Court in *Rehaif v. United States* made clear it is under these circumstances. 139 S. Ct. 2191, 2198 (2019).

24. *See infra* Part V.B.

25. 206 L. Ed. 2d 822 (U.S. Apr. 20, 2020) (No. 19-783).

26. Congress intended courts to analogize the CFAA to state criminal trespass laws. *See infra* Part IV.A; *see also* United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015) ("[T]he legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass.'"); Kerr, *supra* note 11, at 1153-54; Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 20 (2012); Goldfoot & Bamzai, *supra* note 17, at 1494.

term.[27] Different circuits have split on the meaning of the term "without authorization," along numerous fault lines,[28] and even the case law within the Ninth Circuit has become nearly incoherent.[29] The courts have taken a plain meaning term, "without authorization," and *made it* vague. An effective mens rea reduces the ambit of the statute far more simply and effectively than does a focus on the term "without authorization."

This Article ends with a coda, somewhat in tension with the rest of the Article but important nevertheless. The bulk of this Article accepts the CFAA as written and suggests the best interpretation based upon ordinary tools of statutory interpretation and construction. That interpretation also happens to ameliorate many of its potentially unjust applications as a happy byproduct.

But even my proposed interpretation leaves many unjust outcomes. The coda to this Article, therefore, makes a somewhat different argument: Congress should abolish the trespass provision of the CFAA. The provision will always remain unjust because at bottom, it criminalizes mere presence without any other harm, such as damaging the target computer or stealing valuable information. This coda sketches the history of unjust criminal trespass cases in the physical world to illustrate this problem.

In Part I, this Article surveys the breadth of the CFAA trespass provision using multiple examples. Part II surveys the diagnosis and solution by courts and other scholars: their undue focus on the term "without authorization" and the code-based regime as their proposed solution. Part III argues instead that we should focus on the CFAA's mens rea, why *knowingly* applies to "without authorization," and how powerful this mens rea can be. Part IV draws upon state trespass statutes and case law to reach similar conclusions. Part V applies these lessons to typical CFAA scenarios. Part VI

---

27. *E.g.*, Bellia, *supra* note 5, at 1445-60 (grouping CFAA cases into five categories based upon their different interpretations or theories of the statute).

28. *Compare Nosal I*, 676 F.3d 854, 862-63 (9th Cir. 2012) (rejecting terms of service as a basis for unauthorized access), *with* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 64 (1st Cir. 2003) (suggesting in dicta that terms of service suffice), *with* United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015) (finding the statute to be ambiguous and applying the rule of lenity), *with* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (applying state duty of loyalty law for employees and agency theory).

29. *See infra* Part II.C.

directly challenges the key justifications for a code-based approach, particularly in light of my own proposal. Part VII draws the final lesson from criminal trespass law in a coda: computer trespass suffers from many of the same injustices as its physical world analogue. Rather than trying to fix the CFAA to conform more comfortably with the criminal trespass analogy, we should abolish its trespass provision in order to avoid importing criminal trespass's pathologies.

I. AN OVERBROAD STATUTE

This Part shows how the CFAA has evolved into an extremely broad statute that criminalizes simple trespass to any computer merely to view any type of information. It shows how this breadth can lead to unjust applications with particular examples.

A. The CFAA

The CFAA criminalizes simple trespass in section 1030(a)(2)(C)—intentionally accessing a computer without authorization.[30] It also requires that a person obtain information, but since observing information suffices,[31] this element adds almost nothing. That is, the trespass provision of the CFAA almost completely parallels simple criminal trespass. Its formula—(i) intentionally (ii) access (iii) a computer, (iv) without authorization—precisely tracks a typical criminal trespass statute: (i) knowingly (ii) enter (iii) a building (iv) without authorization.[32] We simply replace "enter" with "access" and "building" with "computer."

---

30. 18 U.S.C. § 1030(a)(2)(C). The provision applies to "protected computers," but its definition effectively includes any computer connected to the internet and even perhaps some that are not. *Id.* § 1030(e)(2); *see also* Kerr, *supra* note 5, at 1663 n.284 ("The term 'protected computer' is defined extremely broadly to include essentially every computer connected to the Internet."); Jack Dahm, *No Internet Does Not Mean No Protection Under the CFAA: Why Voting Machines Should Be Covered Under 18 U.S.C. § 1030,* 94 NOTRE DAME L. REV. 1775, 1791 (2019) (arguing that even some computers not connected to the internet fall under the CFAA).

31. *E.g.*, H.R. REP. NO. 99-612, at 10 (1986) (explaining that the phrase "obtains information" includes merely "observing" or "accessing" it).

32. *E.g.*, FLA. STAT. ANN. § 810.08(1) (West 2020) ("Whoever, without being authorized, licensed, or invited, willfully enters or remains in any structure or conveyance.").

I call this crime "entry-level" both because it is a misdemeanor only[33] and because it forms a lesser included offense for most of the other provisions. For example, section 1030(a)(1) criminalizes computer trespass—access without authorization—in order to obtain classified information that could be used against the United States and delivering the information to someone not entitled to it.[34] Section 1030(a)(4) criminalizes trespass in order to commit fraud and obtain at least $5,000 in value.[35] Parts of section 1030(a)(5) criminalize trespass that causes damage to a computer, such as deleting data or altering it or making a computer unavailable to others and monetary loss to the company as a result.[36]

These other provisions are all trespass *plus* other elements. In its legislative history, Congress expressly referred to section 1030(a)(4) as "trespass plus theft," explaining it meant section 1030(a)(2) plus theft.[37] When we interpret the trespass provision of the CFAA, we must remember that the same formula appears in several of the other criminal provisions, and its meaning must likely remain the same across subsections.

This simple trespass provision was not always so broad, and its development helps us to understand just how broad it has become.[38] It originally criminalized, as it does today, access without authorization to obtain information, but it sharply limited the type of information (and therefore the types of computers) that counted.[39] It only applied to classified information that the intruder intended to be used against the United States, a bank's financial information about a customer, or a credit agency's information about a consumer.[40] It

33. 18 U.S.C. § 1030(c)(2)(A).

34. *Id.* § 1030(a)(1).

35. *Id.* § 1030(a)(4).

36. *Id.* § 1030(a)(5)(B)-(C).

37. H.R. REP. NO. 99-612, at 12 (1986) ("There must be a clear distinction between trespass plus theft, punishable as a felony, and mere computer trespass, punishable as a misdemeanor.").

38. *See generally*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010).

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

40. *Id.*

also prohibited altering or damaging computer information, but only on a government computer.[41]

In part because the text limited the CFAA, we can infer Congress intended to protect particularly sensitive computers and information, such as those of banks and the federal government.[42] These computers were not open to the public and were generally protected by passwords. Therefore, the textual limits to these computers and information reflected Congress's worry about outsiders hacking in, especially by breaking passwords.[43]

But in 1996[44] and later years,[45] Congress greatly expanded the scope by applying the trespass provision, access without authorization, to *any* computer that is in or affects interstate or foreign commerce, meaning—at minimum—any computer, anywhere in the world, connected to the internet.[46] Congress also made clear that "obtain information" now means any type of information, not just classified or government information.[47] Even worse, "obtain" already included simply to "observe" the information and does not require any kind of downloading or copying.[48] Finally, the term "accesses" has been read so broadly as to impose almost no limit at all, as long as the defendant's computer connects to the target computer.[49]

To foreshadow my argument in Part IV slightly, the above observations undermine the central pillar of the *hiQ Labs* case: that the CFAA protects private, not public, information and computers and draws that division by way of an authentication gate, such as a password login. The CFAA originally may well have done so by limiting the types of information and computers protected. But when Congress eliminated those limits and applied the CFAA to any information and any computer connected to the internet, it wiped

41. *Id.*

42. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1001 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

43. *Id.*

44. Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3491-92.

45. *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 814(d)(1), 115 Stat. 272, 384.

46. Kerr, *supra* note 38, at 1566-71.

47. *See* Economic Espionage Act, § 201(1)(B), 110 Stat. at 3492.

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

49. Kerr, *supra* note 38, at 1561.

away any such division between private and public information,[50] and similarly, rendered irrelevant a dividing line between those two based on a password login.

Putting together these amendments and definitions, the current entry level trespass provision of the CFAA becomes simple: it applies to anyone who intentionally accesses a computer connected to the internet without authorization. The prohibited conduct includes visiting the landing page of a newspaper, LinkedIn, or Google. It includes, of course, the further steps of creating an account. It also includes an employee who accesses a work computer. If the individual knows this conduct is without authorization, she may have violated the statute; if she is personally told to stay off, she almost certainly has.

"Entry level" suggests this crime is not serious. But first, all federal crime is serious. Second, prosecutors can easily, almost trivially, bump this misdemeanor to a felony.[51] Third, this trespass provision serves as a lesser included offense and predicate for the other more serious subsections, such as the fraud felony provision.[52]

Of the CFAA subsections, the simple trespass provision is the most widely brought criminal charge, as well as the most widely pleaded cause of action in civil suits.[53] Many of the cases construing the trespass provision are, in fact, civil cases,[54] and this may explain why courts have ignored or minimized the role of mens rea when interpreting the statute. They should not, though. Courts agree that even in a civil case, the statute must be interpreted as if it were a criminal case because the terms must be given the same meaning in both contexts.[55]

---

50. Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) ("For example, Congress might have written § 1030(a)(2) to protect only 'nonpublic' information.").

51. *See* 18 U.S.C. § 1030(c)(2)(B)(iii). Prosecutors need only show the information obtained has a value of at least $5,000. *Id.* They need not show the defendant gained $5,000, nor that the victim lost $5,000. *See* United States v. Batti, 631 F.3d 371, 375-76 (6th Cir. 2011). Merely *viewing* information that itself happens to be *worth* $5,000 makes the conduct a felony. *See id.*

52. *See supra* notes 33-36 and accompanying text.

53. *See* Mayer, *supra* note 3, at 1492-93.

54. *See id.* at 1487.

55. LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) ("[W]here a statute [such as the CFAA] 'has both criminal and noncriminal applications,' courts should interpret the statute consistently in both criminal and noncriminal contexts." (quoting Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004))).

One clarification: I have treated the CFAA as prohibiting initial unauthorized access only, but it also prohibits, in the alternative, *exceeding* authorized access, much as ordinary criminal trespass statutes do.[56] In particular, the text targets a person who "intentionally accesses a computer without authorization or exceeds authorized access."[57]

I treat the two alternatives, unauthorized access or exceeding authorized access, as amounting to the same test simply applied in different situations. The element "without authorization" applies to an outsider who lacks authorization to access at all. "Exceeds authorized access" applies to an insider, such as an employee who may legitimately access the computer but may not open certain files or folders.[58] The test for the first case is whether the access is with authorization; for the second, whether the person is entitled to obtain the additional information. An employee in the shipping department may be *authorized* to access the computer and the folders concerning shipping, but not *entitled* to obtain information from the human resources folders on the network.

"Authorized" and "entitled" are synonyms, and, as a result, the test for each situation will boil down to the same question: did the person enjoy authorization to access and obtain the information they accessed and obtained? The employee in shipping is authorized to access the computer, but he is not entitled to obtain information from human resources, such as the salary information of his coworkers.

Put another way, the two formulas, to "access without authorization" and "to exceed" authorized access and obtain information a person is not "so entitled to obtain," appear different but are the same because the conduct is the same. To access a computer *means* to obtain information. The individual sends information to the computer and receives information in response to establish any kind of access at all. To say the person's access is without authorization is the same as saying she is not entitled to obtain the information

56. *E.g.*, N.Y. PENAL LAW § 140.00(5) (McKinney 2020) ("A license or privilege to enter or remain in a building which is only partly open to the public is not a license or privilege to enter or remain in that part of the building which is not open to the public.").

57. 18 U.S.C. § 1030(a)(2).

58. *Nosal I*, 676 F.3d 854, 858 (9th Cir. 2012).

she obtains by accessing it. True, the emphasis is different, but the test remains nearly the same.[59]

This regime parallels the physical world of trespass. A person's initial entry into another's home is measured by whether that entry is licensed or authorized by the owner; the same test applies, once the person is in the home, to whether she can go upstairs to poke around the bedroom—is that additional step authorized?[60] Now we will look to a variety of factors and social customs to answer that question, but the test to which we apply those factors remains the same: authorization.[61]

B. Examples of Its Breadth

The problematic breadth of the CFAA can best be described through examples. This is not a taxonomy but rather a collection of difficult scenarios the courts have faced and hypothetical cases they or scholars have proposed.

First are terms of service cases.[62] These involve a person who accesses a web platform, such as Facebook or LinkedIn, in violation of a term of service that the person has not read or that is unclear. Facebook, for example, prohibits a person from creating an account with a fake name or joining if under thirteen years old.[63] Courts and scholars rightly point out it would be unfair to punish such a person for accessing a computer without authorization when she did not

---

59. We can identify one slight difference: the definition of exceeds authorized access includes the term "so," when describing the information that the individual is not "so" entitled to obtain. This "so" justifies distinguishing whether access is authorized based upon the *manner* of access, as opposed to the nature of the information obtained, or the purpose the individual has in obtaining it. The "so" might therefore mean that a business entity using automated software to scrape the website of a competitor may have authorization to access the competitor's website manually, but not by means of an automated software. The manner of access is arguably prohibited by the word "so" (assuming the terms of service or cease-and-desist letter have prohibited that manner of access).

60. *See, e.g.*, People v. Thomas, 872 N.E.2d 438, 443 (Ill. App. Ct. 2007) (finding that the defendant lacked "permission" to enter private area of public building); People v. Barnes, 41 N.E.3d 336, 339 (N.Y. 2015).

61. *E.g.*, Bowman v. United States, 212 A.2d 610, 610-11 (D.C. 1965) (describing how the defendant entered an area of the train station restricted to those with tickets).

62. United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009); *see also Nosal I*, 676 F.3d at 861-62 (describing such scenarios in dicta).

63. *Terms of Service*, *supra* note 8.

know she was violating the terms. Even if read, these terms of service often do not clearly say that violating them results in termination of authorization.[64] Courts have rarely, if ever, found liability for such facts,[65] but both courts and scholars regularly use this scenario as a central example of the potential problem with reading "without authorization" literally.[66]

Second are purpose or misuse cases that often involve employees on private systems rather than public web platforms. The *Van Buren* case pending before the Supreme Court involves a police officer who had permission to access a law enforcement database for police business but used it for personal reasons.[67] He had the right to look up a license plate for a valid investigation but not to help a friend, as he did.[68] This access violates the rules for the database, but only if we know the defendant's purpose or later misuse of the information.

The circuit courts are split on this issue. The Eleventh Circuit in *Van Buren* held that the officer had violated the CFAA.[69] By contrast, the Second Circuit held that such wrongful purpose alone does not trigger a violation of the CFAA. The case, the prominent cannibal cop case in New York, involved a police officer who used his access to a police database to look up a woman's address so he could follow her; again, he had valid access to the computer as an employee but violated city policy by using that access for his own purposes.[70]

Another common scenario under the purpose or misuse category involves an employee who has permission to log on to his employer's computer but does so for the purpose of taking confidential business

---

64. *Drew*, 259 F.R.D. at 466 (noting this ambiguity).

65. *See id.* at 451, 468 (refusing to find liability); Sandvig v. Barr, Civil Action No. 16-1368 (JDB), 2020 WL 1494065, at *4 (D.D.C. Mar. 27, 2020) (assuming no such cases), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020); Sandvig v. Sessions, 315 F. Supp. 3d 1, 18-20 (D.D.C. 2018) (explaining that no convictions have resulted from a violation of terms of service alone).

66. *See Nosal I*, 676 F.3d at 860-61; *Drew*, 259 F.R.D. at 466; Kerr, *supra* note 5, at 1659; Bellia, *supra* note 5, at 1473.

67. United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (mem.).

68. *Id.* at 1206.

69. *Id.* at 1207-08.

70. United States v. Valle, 807 F.3d 508, 511-13 (2d Cir. 2015).

information so he can quit and start his own business with a client list, for example.[71] Here, too, courts will ask whether an employer's terms of service[72] or even a state law duty of loyalty[73] should suffice to establish the access was without authorization.

These employee cases involving purpose or later use are often a subset of terms of service cases—and sometimes conflated with them[74]—because they do involve a violation of an employee manual or other written rule or even norm. But they differ from the first category of terms of service cases. A twelve-year-old who accesses Facebook has no permission *at all* based upon her status. By contrast, the officer or employee has permission to access for some purposes based upon his status as an officer but not for the purpose he actually has.

Third are scraping cases. These usually involve businesses that write automated software that visits thousands, millions, or even billions[75] of webpages on another's platform, or across the web, to obtain data from those pages.[76] A travel site might scrape data from a competitor to determine how to set its prices competitively.[77] In *hiQ Labs*, the plaintiff scraped public-facing profile information from LinkedIn.[78] For millions of profiles, it obtained names, employer information, education, and background to allow hiQ Labs to create its own database it could package and sell.[79]

Consider a more recent and large-scale scraping case. A company called Clearview AI has spent the last several years secretly

71. *See Nosal I*, 676 F.3d at 856.

72. United States v. Czubinski, 106 F.3d 1069, 1071-72, 1078 (1st Cir. 1997) (assuming subsection (a)(2) was met when IRS employee accessed files not for business but for curiosity).

73. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

74. *Nosal I*, 676 F.3d at 860 (conflating the problem that an employee might not be aware of a prohibition with the fact that the CFAA does not define prohibited purposes or uses at all).

75. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/65KJ-XBTU].

76. Jacquellena Carrero, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 COLUM. L. REV. 131, 132 (2020); Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 373-74 (2018).

77. Carrero, *supra* note 76, at 141.

78. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 991 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

79. *Id.*

scraping platforms such as Facebook, YouTube, Venmo, and Twitter to gather three billion photos and their associated names.[80] Clearview has developed sophisticated facial recognition algorithms and quickly deployed its services to hundreds of law enforcement agencies across the country.[81] These police departments simply upload the photo of a person caught on a surveillance camera, for example, and Clearview AI returns the person's name and other information, including links to their social media accounts.[82]

Courts are split on how to handle scraping cases.[83] But they often focus on "without authorization" as the key to answering the question and whether terms of service or an express cease-and-desist letter suffice to establish the access was unauthorized. The Ninth Circuit in *hiQ Labs*, for example, held that scraping the public portions of a public site never violates the CFAA trespass provision.[84] For public sites such as LinkedIn, the "without authorization" element does not apply.[85]

Fourth are password sharing cases. A person gains access to a site validly, in the sense that she enters a password that works and with the permission of the password/account holder, but in violation of the terms of service of the platform or even in the face of a cease-and-desist letter.[86] Does this conduct violate the CFAA?

Finally, I conclude my nonexhaustive collection with firmware pushing cases.[87] These are interesting because the computer owner is not a platform or business but rather an individual who owns a smartphone or computer. For example, Apple pushed firmware to its customers' devices, an iOS update, that caused the phone to operate more slowly to conserve battery time.[88] If the device owner consents to the download in general but not to the specific effects of the new firmware, has Apple accessed the individual's device without authorization?

---

80. Hill, *supra* note 75.

81. *Id.*

82. *Id.*

83. *See* Sellars, *supra* note 76, at 377.

84. *hiQ Labs, Inc.*, 938 F.3d at 1003-04.

85. *Id.*

86. *E.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1063 (9th Cir. 2016).

87. *In re* Apple Inc. Device Performance Litig., 347 F. Supp. 3d 434, 452 (N.D. Cal. 2018) (collecting cases), *on reconsideration in part*, 386 F. Supp. 3d 1155 (N.D. Cal. 2019).

88. *Id.*

II. AN UNDUE FOCUS ON "WITHOUT AUTHORIZATION"

Courts and scholars are right to treat criminalizing many of the above scenarios as unjust. I turn now to their diagnosis of the problem before turning to their proposed solutions. Both suffer from an undue focus on the term "without authorization."

A. A Misdiagnosis

Scholars[89] and many courts[90] point to the element "without authorization" as the problem. To read the term broadly as embracing a violation of terms of service, for example, would criminalize innocent conduct. The arguments almost all boil down to what they call notice and what I will later address via mens rea.[91] The individual does not know her access is without authorization, and it would be unfair or wrong to punish her. But scholars and courts have shaped this basic point into numerous different legal arguments.

First, they argue that the term "without authorization" is "unconstitutionally vague."[92] This follows, they argue, because the term fails to give fair notice as to when access is "without authorization."[93] This is again the terms of service argument—a person may not have read them. "Without authorization" has also been deemed vague because a platform can change its terms of service, and a user will be unaware of the change.[94] Others argue "without

89. *See, e.g.*, Kerr, *supra* note 38, at 1648-49; Bellia, *supra* note 5, at 1443; Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 486 (2019); Mayer, *supra* note 3, at 1463 n.32 (collecting the "voluminous" scholarly critiques of the overbreadth and broadness of the CFAA's "without authorization" provision).

90. *See, e.g.*, *Nosal I*, 676 F.3d 854, 862-63 (9th Cir. 2012); United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009).

91. *See infra* Part III.A.

92. *See* Kerr, *supra* note 38, at 1561-62.

93. *See Nosal I*, 676 F.3d 854; *Drew*, 259 F.R.D. 449; *cf.* United States v. Valle, 807 F.3d 508, 540 (2d Cir. 2015). *But see* WEC Carolina Energy Sols. L.L.C. v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1186 (N.D. Cal. 2013) (explaining that "a personally-addressed cease-and-desist letter" helps to inform "[a] person of ordinary intelligence" her "access was 'without authorization'").

94. *See Nosal I*, 676 F.3d at 862.

authorization" could be premised upon a contract model.[95] If a person clicks "I agree" to terms she has not read, contract law makes her bound by those rules.[96] These arguments all represent elaborations of the notice problem.

A variation on the terms of service problem arises under the Seventh Circuit view that "without authorization" can be established by state tort law, such as an employee's duty of loyalty. In *International Airport Centers, L.L.C. v. Citrin*, an employee quit and was supposed to return a work laptop.[97] The employee accessed the laptop one last time to delete files for his own benefit and to the company's detriment.[98] The court held that he accessed the laptop without authorization, not because he had quit, but because at the time he accessed the laptop, he was acting for his own benefit and not the company's.[99] Doing so breached his duty of loyalty, and, at that point, his agency with the company had terminated and with it his authorization to access the computer.[100]

Courts and scholars criticize this case because an employee would not be likely to know that his authorization had been terminated by operation of law—because he was unaware of this state law duty of loyalty or of its application to his conduct.[101] Even though this case involves state law, it is really just a notice case in the end and one that we can later address with mens rea.

Even cases decided on other grounds or raising other issues get dragged into the orbit of the supposed notice problem. For example, in *Nosal I*, the Ninth Circuit addressed whether the CFAA applies to one who has the right to access a computer but later *uses* the information obtained in violation of a term of service.[102] The court held that it does not.[103] But the Ninth Circuit then found itself

95. *See* Kerr, *supra* note 5, at 1598-99.
96. *Id.*
97. 440 F.3d 418, 419 (7th Cir. 2006).
98. *Id.* at 419.
99. *Id.* at 420-21.
100. *Id.* at 420.
101. *See* WEC Carolina Energy Sols. L.L.C. v. Miller, 687 F.3d 199, 203 (4th Cir. 2012); *Nosal I*, 676 F.3d 854, 860 (9th Cir. 2012) ("What exactly is a 'nonbusiness purpose'? If you use the computer to check the weather report for a business trip? For the company softball game?").
102. 676 F.3d at 863.
103. *Id.*

unnecessarily discussing at length the problem of terms of service and notice in general, even beyond later misuse cases.[104] Indeed, it appeared to assert that such terms of service can never be the premise for a finding that access was without authorization—a point unnecessary to the actual holding that the CFAA does not apply *at all* to the later misuse cases.[105]

Finally are two arguments *not* rooted in notice. Many argue that it would be unfair for a platform to unilaterally impose conditions for access because a violation of these conditions can lead to a criminal charge.[106] A private party appears to be enjoying the right to decide what is criminal, and the state should not delegate this power to a powerful business entity.[107]

As discussed below, the problem with this argument is that ordinary criminal trespass laws afford private property owners, including stores, malls, and parks, precisely this power to unilaterally impose conditions of entry, the violation of which will lead to criminal charges.[108] Therefore, this is an argument that we should abolish the trespass provision, as I argue in the final Part of this Article, and not a constitutional or even statutory interpretative argument that "without authorization" can never rest upon terms of conditions.

The term is also unconstitutionally vague, some argue, because its breadth can lead to arbitrary or discriminatory enforcement.[109] If terms of service are the predicate, for example, millions of ordinary Americans are acting without authorization in their routine computer use.[110] Law enforcement could then pick and choose among those millions which to prosecute, and there are no guidelines to decide which to choose.[111] To the extent this argument arises out of unclear terms, a robust mens rea will fix the problem. To the extent the argument rests merely upon the great number of

---

104. *See id.* at 861-62.

105. *Id.* at 862-63.

106. *See* Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 768-71 (2013).

107. *See id.*

108. *See infra* Part IV.E.

109. *See* Kerr, *supra* note 38, at 1562.

110. *See Nosal I*, 676 F.3d at 862-63; *see also* Note, *supra* note 106, at 755.

111. Note, *supra* note 106, at 768-70.

people violating a law, it seems curious. Millions violate federal marijuana laws in states where it is legal, and yet courts do not hold those laws unconstitutionally vague simply because of their breadth or even surprise.[112] The argument as to the sweep of these laws supports abolishing them, but their breadth alone does not render them *vague*.

In the final Part of this Article, I focus directly on the unilateral power of a property owner, real or virtual, to exclude for arbitrary or discriminatory reasons. That Part shows that the Supreme Court has never held such power renders trespass laws unconstitutional—and certainly not unconstitutionally "vague." That Part therefore argues instead that this power to discriminate or otherwise exclude arbitrarily is best seen as a reason to repeal the trespass provision of the CFAA.

The foregoing focuses on terms of service, largely attacked because a user might not be aware of them. But what about cease-and-desist letters personally communicated to an individual or business that then continues access? Some scholars argue even these cease-and-desist letters are insufficient. Orin Kerr, for example, has recently written that a site that opens itself to the public cannot selectively block certain users; therefore, any access by those users told to stay out is still authorized.[113] Indeed, *hiQ Labs* expressly held that a cease-and-desist letter could not establish that access was unauthorized for a public platform such as LinkedIn.[114] The court did not claim the letter failed to provide clear notice; rather, it held that the public portions of a platform are simply never protected by the CFAA.[115]

B. A Code-Based Solution?

Many scholars argue that the only way to fix the term "without authorization" is to focus on it even more diligently, as opposed to finding solutions elsewhere, such as in the statute's mens rea

112. *See* United States v. Bramer, 832 F.3d 908, 909 (8th Cir. 2016); State v. Parker, No. 45502-1-II, 2015 Wash. App. LEXIS 2691, ¶ 15 (Wash. Ct. App. Nov. 3, 2015).

113. Kerr, *supra* note 11, at 1147.

114. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003-04 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

115. *Id.*

provision. They urge us to define, or really redefine, "without authorization" as follows: only by circumventing a code-based barrier, such as a password gate, does an individual access the computer without authorization.[116] This rule, they argue, would ensure that the intruder knows that she is accessing without authorization, thus fixing the notice problem.[117] In addition, they argue, Congress intended the CFAA to criminalize hackers only, those who "break" into the computer somehow.[118]

One leading scholar has described the code-based regime as the dominant scholarly view.[119] Though rejecting the theory, Jonathan Mayer recently wrote that scholars have "coalesced around a theory that liability should turn on circumvention of technical protections."[120] The code-based theory comes in two main versions: an original, broad version and a recent, more refined version, such as that announced in *hiQ Labs*.[121]

1. The Original Code-Based Test

In its original, broad version, the code-based theory says that a person's access is "without authorization" only if it involved "circumvention of code-based restrictions"[122] In other words, absent such a code-based breach, the access was always authorized. Such a code-based breach also appears to suffice as a violation,[123] though

116. *See id.*; Kerr, *supra* note 5, at 1600; Kerr, *supra* note 11, at 1164 ; Bellia, *supra* note 5; David J. Rosen, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"*, 27 BERKELEY TECH. L.J. 737, 740 (2012).

117. Rosen, *supra* note 116, at 760-61.

118. *Id.* at 745-46.

119. Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying* United States v. Nosal, 84 GEO. WASH. L. REV. 1644, 1656 n.60 (2016) (collecting articles and notes).

120. *Id.* at 1656.

121. *See* 938 F.3d 985 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

122. Kerr, *supra* note 5, at 1600; *see* Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1036, 1039 (N.D. Cal. 2012) (interpreting the CFAA and California computer crime law), *aff'd in part, vacated in part, rev'd in part*, 844 F.3d 1058 (9th Cir. 2016); Bellia, *supra* note 5, at 1457; *see also* Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1054 (N.D. Cal. 2014) (interpreting California computer crime law); NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 965-66 (N.D. Cal. 2014) (citing cases under California computer crime law and relating history).

123. *Power Ventures*, 844 F. Supp. 2d at 1036.

some courts have recognized the code breach would suffice only if it also violated some kind of term of service or norm.

2. The Refined Code-Based Test

The recent, refined version of the code-based regime limits the type of code to password logins or some other technical method that the target computer uses to authenticate the user.[124] This authentication requirement appears to be a subset of code-based barriers because it still asks whether the computer owner has erected a "technical barrier."[125] But now the barrier must relate to authenticating the person seeking access or constitute some other method of breaking in.[126] The test seems to boil down to a username and password, or something analogous, that the intruder bypasses either by stealing credentials or exploiting security flaws.[127]

In Kerr's particular elaboration of this refined version of the code-based test, the technical barrier must also be high and hard to breach.[128] A person who clears her cookies from her browser to visit a site that limits visits does not count, nor does changing or disguising one's IP address.[129] These are technical barriers, true, but they are mere speed bumps that are easy to evade and, therefore, should not count as barriers.[130]

3. hiQ Labs

The Ninth Circuit in *hiQ Labs* announced yet a third version of the code-based regime. Following scholars, it held only information or computers protected by a password type authentication gate enjoy protection under the CFAA.[131] Information on the public-facing part of a public platform does not fall under the CFAA at all, and

124. *hiQ Labs*, 938 F.3d at 1003-04; Kerr, *supra* note 11, at 1164.

125. *See hiQ Labs*, 938 F.3d at 1003-04.

126. Kerr, *supra* note 11, at 1172 ("Exploits that circumvent authentication mechanisms or otherwise 'break in' to systems are similarly unauthorized.").

127. *Id.*

128. *Id.*

129. *Id.* at 1147.

130. *Id.*

131. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003-04 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

the term "without authorization" is, therefore, irrelevant to this information.[132]

But parting ways with scholars, the Ninth Circuit in *hiQ Labs* added a twist because it needed to harmonize its holding with existing precedent. Once information is protected by the CFAA through this code-based barrier, a person need not actually breach that barrier to violate the CFAA.[133] As to such private, protected information, defying a cease-and-desist letter *will* suffice.[134] There is thus a mismatch between the test for whether information is protected by the CFAA (a code-based test) and the test for whether a person accessed that information without authorization (a non-code-based test).

I will detail the facts, holding, and reasoning of *hiQ Labs* because they recapitulate many of the scholarly arguments in favor of a code-based regime. In addition, they capture one of the most challenging types of cases—scraping cases—whose rule will apply to the even more challenging Clearview AI scraping situation. Finally, *hiQ Labs* represents the most recent case to address the CFAA and its "without authorization" requirement.

In *hiQ Labs*, a startup company, hiQ Labs, used automated bots to scrape public-facing data from millions of LinkedIn profiles, "including name, job title, work history, and skills."[135] It packaged this data in a new product it sold to other businesses.[136] One of its products, Keeper, would take the name of an employee of a given company and, after scouring the public portions of LinkedIn, predict whether she was likely to be recruited away.[137] That information would allow her current employer, hiQ Labs' client, to make greater efforts to keep her.[138]

LinkedIn sent hiQ Labs a cease-and-desist letter requiring it to stop accessing LinkedIn's computers.[139] It also successfully blocked

132. *Id.*
133. *See id.* at 1002.
134. *See id.*
135. *Id.* at 991.
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.* at 992.

hiQ Labs technologically.[140] It was hiQ Labs, oddly, that sued LinkedIn claiming it had a legal right to scrape the site under California's anticompetition laws.[141] hiQ Labs argued LinkedIn should not be allowed to prevent hiQ Labs from securing data to create products to compete with LinkedIn, which also culled its own data to sell similar products.[142]

The Ninth Circuit ultimately found that hiQ Labs did have a right under anticompetition laws to scrape LinkedIn's site—albeit as a preliminary holding under a preliminary injunction standard.[143] But before the court reached this conclusion, it first had to determine whether hiQ Labs' scraping violated the CFAA's trespass provision.[144] The Court held that it did not.[145]

On the CFAA holding, the court expressly adopted part of Orin Kerr's test. It wrote that the CFAA protects private information only.[146] This information is "delineated as private" by a code-based barrier.[147] This barrier must be "an authentication requirement, such as a password gate."[148] The internet is presumed open, and this requirement "divides open spaces from closed spaces on the Web."[149]

In applying this test, the Ninth Circuit found that LinkedIn's public-facing information is open to the public and does not require a login to an account with a username and password to access.[150] True, hiQ Labs' access to LinkedIn's computers was unauthorized in the sense that LinkedIn objected and made hiQ Labs aware through a personally communicated letter as well as modest technological barriers.[151] But "without authorization," the court held, applies only to sites or areas that require a login access and

140. *Id.*
141. *Id.*
142. *Id.* at 995.
143. *Id.* at 996.
144. *Id.* at 999.
145. *Id.* at 1003-04.
146. *Id.* at 1001.
147. *Id.*
148. *Id.* (quoting Kerr, *supra* note 11, at 1161).
149. *Id.* (quoting Kerr, *supra* note 11, at 1161).
150. *Id.* at 1003-04.
151. *Id.* at 992.

never applies to the public portion of a public site.[152] For public sites such as LinkedIn, the "concept of 'without authorization' is inapt."[153]

But *hiQ Labs* has a second aspect of its holding: the mismatch noted above between the test for what gets protection and the test for what counts as a violation. I address this nuance more fully in the next Section, in which I also pull back to observe more generally just how complicated the case law is. I do so to show how my proposed shift in focus to mens rea greatly simplifies the analysis.

C. Complex Case Law

A focus solely on the element of "without authorization" has generated unnecessarily complex case law. First, there is a circuit split over whether terms of service can ever establish unauthorized access[154] and a split in authority for a cease-and-desist letter.[155] Kerr has grouped the case law into three categories as it defines "without authorization,"[156] and Bellia has grouped it into five.[157] Some courts are beginning to require some code-based hack,[158] whereas others at least suggest it will be sufficient.[159]

Even within the Ninth Circuit, the interplay of four key and widely cited cases—*Nosal I*,[160] *Nosal II*,[161] *Power Ventures*,[162] and *hiQ Labs*[163]—has created confusion and undue complexity. The rule

---

152. *Id.* at 1003-04.

153. *Id.* at 1002.

154. *Compare Nosal I*, 676 F.3d 854, 862-63 (9th Cir. 2012) (rejecting terms of service as a basis for unauthorized access), *with* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 64 (1st Cir. 2003) (suggesting in dicta that terms of service suffice), *with* United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015) (holding the statute is ambiguous and applying the rule of lenity), *with* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (applying state duty of loyalty law for employees and agency theory).

155. *Compare hiQ Labs*, 938 F.3d at 1003-04, *with* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969-70 (N.D. Cal. 2013).

156. Kerr, *supra* note 5, at 1628.

157. Bellia, *supra* note 5, at 1444-46.

158. *See hiQ Labs*, 938 F.3d at 1003-04; Sandvig v. Barr, Civil Action No. 16-1368 (JDB), 2020 WL 1494065, at *11 (D.D.C. Mar. 27, 2020), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

159. *See Nosal I*, 676 F.3d at 858.

160. 676 F.3d 854.

161. United States v. Nosal (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016).

162. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016).

163. 938 F.3d 985.

appears to be this: the public portion of a public site can never be the scene of unauthorized access (itself an astounding proposition) under *hiQ Labs*, no matter what steps the host site takes or how clearly and personally it communicates the ban.[164]

But what are the rules for information, areas, or accounts that do require some kind of access authentication, such as a username and password? *Nosal I* suggests in dicta that a violation of terms of service or even a cease-and-desist letter is never enough; some code-based hack must occur.[165] But *Power Ventures did* permit a cease-and-desist letter to establish the access was unauthorized without a code-based hack.[166] Indeed, Power Ventures had the express permission of the individual account holders to access their account using their passwords; their access was unauthorized because Facebook had expressly told them so.[167]

In *Nosal II*, the court held the defendant's access was completely without authorization under the CFAA's plain meaning because he had been told he could no longer access the computers.[168] He too did not use a code-based hack, but rather borrowed a password of a legitimate employee; nevertheless, his access was unauthorized because it was revoked after he left their employ.[169]

The Ninth Circuit placed particular and repeated emphasis on the plain meaning of "without authorization," arguing at length it was unambiguous and applied to anyone told to stay out.[170] This was precisely the situation in *hiQ Labs*—the company was expressly told to stay out—and yet that was not enough to establish that access was without authorization under the plain meaning.[171]

hiQ Labs thus appears to contradict *Nosal II* and *Power Ventures*. *hiQ Labs* attempted to harmonize them as already sketched above.[172] To reiterate, when an area or information *is* protected by

164. *Id.* at 1003-04.
165. 676 F.3d at 862-63.
166. 844 F.3d at 1069.
167. *Id.* at 1068.
168. 844 F.3d 1024, 1034-35 (9th Cir. 2016).
169. *See id.*
170. *Id.* at 1034 ("[W]e consider the plain and ordinary meaning of the words 'without authorization.'").
171. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).
172. *See supra* Part II.B.3.

a code-based barrier, such as a login, that barrier delineates the information as private and at least eligible for "without authorization" protection.[173] The code-based test does not mean that breaching the password is the only way in which a person might access information without authorization.[174] Rather, for such private information, a cease-and-desist letter *will* suffice to establish that any further access is unauthorized.[175]

The Ninth Circuit's mismatch makes its test different from Kerr's, from whom it borrowed. Kerr requires that the test and violation match.[176] The information must be protected by an authentication barrier *and* the intruder must bypass that barrier.[177] For Kerr, a cease-and-desist letter would not suffice even for such private information.[178]

The case law is confusing.

D. Dissenting Voices

Not all scholars support a code-based solution or even agree that terms of service or cease-and-desist letters are fundamentally insufficient.[179] Some argue the code-based regime introduces its own uncertainty and vagueness.[180] After all, the code-based regime parallels the same standard for the Digital Millenium Copyright Act (DMCA), which expressly adopts a code-based test in the statute.[181] The case law applying this test for the DMCA has struggled with whether certain barriers, such as blocking IP addresses, count.[182] These latter struggles apply equally to the code-based test under the CFAA.[183]

---

173. *hiQ Labs*, 938 F.3d at 1001.
174. *See id.* at 1002.
175. *See id.*
176. Kerr, *supra* note 11, at 1164.
177. *Id.*
178. *See id.*
179. *See, e.g.*, Mayer, *supra* note 119, at 1647 (arguing we should focus on use versus access instead as a way to "narrow" the reach of the CFAA).
180. *See, e.g.*, Annie Lee, *Algorithmic Auditing and Competition Under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization*, 33 BERKELEY TECH. L.J. 1307, 1317-18 (2018).
181. *Id.* at 1317.
182. *Id.* at 1317-18.
183. *Id.*

James Grimmelmann argues we need not limit the term "without authorization" to code-based hacks for a different reason.[184] In his view, it is permissible to find someone liable even for terms they only should have been aware of.[185] "Without authorization" can be viewed as a legally constructed term.[186] Something can be "without authorization" as a matter of law if a court believes it should be, or more likely should not be, based on policy.[187]

A few scholars *have* pointed to the statute's mens rea, arguing that it can eliminate those problematic terms of service cases. But many of these scholars argue for the far lower negligence standard of "should have known"[188] rather than *knowingly*. Their negligence standard robs the mens rea of its power to exclude the unjust cases.

We appear to be left with a somewhat small group of scholars who have recognized the full potential of a mens rea of *knowingly*. William Hall, Jr. has provided the most in-depth argument for why prosecutors must prove the defendant knew about the restriction in exceeding authorized access cases.[189] But even he largely limits himself to the argument over whether an individual's purpose in accessing the computer should matter rather than the larger question addressed here concerning mens rea in all contexts.[190]

Kerr does point to the CFAA mens rea as "critical" and recognizes how a mens rea of intent can carve out some of the unjust applications of the CFAA.[191] Nevertheless, he underestimates the potential of the CFAA's mens rea. For example, he argues that the CFAA's

---

184. James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1501 (2016).

185. *See id.* at 1511-12.

186. *See id.* at 1501, 1514.

187. *See id.* at 1501.

188. *See, e.g.*, Goldfoot & Bamzai, *supra* note 17, at 1478-79 (defining mens rea in the CFAA as "knew or should have known"); Bellia, *supra* note 5, at 1470 ("knows or has reason to know"); Michael S. Dorsi & Keenan W. Ng, *Computer Criminal Intent*, 51 U.S.F. L. REV. 469, 501 (2017) ("know ... or should have reason to know"). David Thaw appears to argue that the CFAA's text, at least as interpreted by the courts, requires no mens rea for the term "without authorization" at all. David Thaw, *Criminalize Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 945 (2013). He suggests rewriting the statute to expressly include a mens rea that the defendant "reasonably should have known" her access was without authorization, though he later appears to argue for a mens rea of "intent" or "actual notice." *Id.* at 910-11, 945-46.

189. *See* Hall, *supra* note 17, at 1531.

190. *See id.* at 1524-25.

191. *See* Kerr, *supra* note 11, at 1180-82.

mens rea likely does not afford a mistake of law defense that would allow a defendant to argue she did not understand that the operation or interpretation of some other law would render her access without authorization.[192] But *Rehaif*, which the Supreme Court decided in 2019 and since Kerr's argument, held that a mens rea of *knowingly* will afford a defendant precisely this defense.[193]

* * *

In sum, courts and scholars have focused too much on the term "without authorization." In their effort to limit the unjust applications of the CFAA, they have contorted this term, ignored its plain meaning, and substituted a code-based test that does not rest on the text, the legislative history, or the analogy to trespass that controls.

III. THE CFAA AS A *CRIMINAL* LAW

I argue that we should treat the CFAA more thoroughly as a *criminal* law and that we shift our focus from "without authorization" to the statute's mens rea. This Part first demonstrates how this proposal will map onto specific facts, creating a more natural division that follows the elements of the statute.

Next, the Part shows why a mens rea of *knowingly* must apply to the "without authorization" element. This simple point has eluded many courts and scholars but is amply supported by the text, case law, and legislative history. That same legislative history supports an enhanced mens rea of *knowingly*.

This Part then shows why *knowingly* affords a type of mistake of law defense for defendants who do not understand that some other law or policy renders their access "without authorization"—a potentially very powerful defense. A proper application of a robust mens rea will sideline many of the unjust applications of the CFAA. But since some large categories will remain, this Article will later argue for repealing the provision.

---

192. *See id.* at 1181 ("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.").

193. *See* Rehaif v. United States, 139 S. Ct. 2191 (2019).

A. A More Natural Division

A shift of focus to mens rea will simplify the analysis of these cases by dividing the inquiry among elements of the statute more naturally and efficiently. Under my view, "without authorization" means, at a minimum, that the computer owner subjectively does not want the visitor to access her computer. Its meaning could theoretically also require that the computer owner have *communicated* this desire.[194] Indeed, courts and scholars currently load up all the communicative aspect of the statute onto the term "without authorization," greatly confusing the case law.[195]

A mens rea of *knowingly* will subsume whatever communicative aspect "without authorization" itself contains. Courts can, therefore, safely define "without authorization" subjectively and in a very targeted manner. In other words, in applying the statute to a given case, courts will determine whether the computer owner *subjectively* desired to keep the defendant out—that is, whether the access was without authorization. When assessing the defendant's mens rea, courts will assess whether he *knew* of this desire. How well the subjective desire of the computer owner was actually communicated to the defendant will rest entirely in the mens rea department.

This new division of mapping the facts of a given case to the elements of the crime will greatly simplify the analysis and help identify the difficult questions concerning the CFAA that remain. For example, even if a computer owner desires to keep a person out and that person knows it, the CFAA may not prohibit the person's conduct, because the conduct does not meet some other element, such as "access" (versus use).[196]

---

194. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016) (holding that Power Ventures acted "without authorization" and violated the CFAA "only after it received Facebook's cease and desist letter and nonetheless continued to access Facebook's computers without permission").

195. *See supra* Part II.A.

196. *See, e.g.*, *Nosal I*, 676 F.3d 854 (9th Cir. 2012) (holding the CFAA applies to unauthorized access, not unauthorized later use of information obtained). The Ninth Circuit in *Nosal I* became so distracted by its reflections on the possible injustices of the CFAA by focusing on the meaning of "without authorization" that it obscured its far simpler holding that the CFAA does not prohibit later misuse whether by terms of service or otherwise. *See id.* at 863-64.

B. A Mens Rea of Knowingly

The CFAA requires a mens rea of *knowingly* with respect to whether an individual's access to the computer was "without authorization." The intruder must not only know that she is accessing the computer, but also know that she does not have authorization. This follows from the text, court precedent concerning the CFAA, Supreme Court precedent concerning statutory interpretation, and the legislative history of the act.

The argument proceeds in three main steps. First, the text contains a mens rea term, "intentionally," which applies to every element of the statute, including the term "without authorization."[197] Second, when one applies the mens rea "intentionally" to "without authorization," it collapses into the mens rea of *knowingly*. This follows because "without authorization" is an attendant circumstance. Third, a mens rea of *knowingly* must apply to "without authorization" because recent Supreme Court precedent requires that standard to apply to any element that divides innocent conduct from unlawful conduct.

1. Step One

The term "intentionally" applies to each element of the statute, including the term "without authorization." First, ordinary rules of English syntax tell us that "intentionally" modifies both "access" and "without authorization" because no break comes between the terms.[198]

The Supreme Court has often relied upon this simple understanding of English syntax in holding that a mens rea term applies not only to the conduct element that immediately follows, but also to those other elements that round out the statute. Indeed, the Court held recently that "[a]s a matter of ordinary English grammar, we normally read the statutory term 'knowingly' as applying to all the

197. *See* 18 U.S.C. § 1030(a)(2).

198. *Cf.* Flores-Figueroa v. United States, 556 U.S. 646, 650 (2009) ("In ordinary English, where a transitive verb has an object, listeners in most contexts assume that an adverb (such as knowingly) that modifies the transitive verb tells the listener how the subject performed the entire action.").

subsequently listed elements of the crime."[199] By contrast, when a legislature wants to cut off the force of a mens rea term, it might compose the language like this: "intentionally access a computer and that access is without authorization."

Second, the interpretative tools of the Model Penal Code tell us that "intentionally" should apply to every element, including "without authorization." The Model Penal Code simply says that if the statute contains a mens rea term, it applies to every element unless grammatically differentiated or a contrary purpose plainly appears.[200] No such differentiation or contrary purpose appears here. Again, in *Rehaif*, the Court took the same approach, quoting expressly this Model Penal Code principle.[201]

Now federal criminal law does not always rely upon the Model Penal Code for its drafting or interpretation, but the CFAA did. The House Report accompanying the original 1984 legislation fashioned its definition of "knowingly" upon the Model Penal Code and expressly said it was doing so with respect to a part of that definition.[202] It also expressly relied upon the Model Penal Code for the specific intent element of the fraud provision.[203]

The House Report accompanying the 1986 amendments similarly follows the Model Penal Code,[204] and the Senate Report does so implicitly.[205] Those amendments included the substitution of the mens rea term "intentionally" for "knowingly" in the trespass provision.[206] The House Report defines "intentionally" the same as the Model Penal Code, noting that the "term 'purposely' in the Model Penal

199. Rehaif v. United States, 139 S. Ct. 2191, 2196 (2019) (internal quotations omitted).

200. *See* MODEL PENAL CODE § 2.02(4) (AM. L. INST. 1962) (when a statute "prescribes the kind of culpability that is sufficient for the commission of an offense, without distinguishing among the material elements thereof, such provision shall apply to all the material elements of the offense, unless a contrary purpose plainly appears").

201. *See* 139 S. Ct. at 2195.

202. *See* H.R. REP. NO. 98-894, at 16-17 (1984) ("This follows the practice of the proposed Model Penal Code (section 2.02(7)).").

203. *Id.* at 17, 20 ("The Committee intends that the term 'with the intent' have the same culpable state of mind as the term 'purpose' as used in the proposed Model Penal Code (§ 2.02).").

204. H.R. REP. NO. 99-612, at 9-10 (1986).

205. *See* S. REP. NO. 99-432, at 5-6 (1986) (quoting H.R. REP. NO. 96-1396, at 33 (1980)) (discussing MPC definition of "knowingly" contained in House report).

206. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(a)(1), 100 Stat. 1213, 1213.

Code is the equivalent of 'intentional' in the proposed code."[207] It also justifies substituting this new mens rea based upon the Model Penal Code's more prosecution-friendly definition of "knowingly."[208]

Finally, in the 1970s and early 1980s, Congress began to consider adopting the Model Penal Code culpability standards as part of a much broader criminal law reform effort.[209] It held numerous hearings[210] and in 1980, the House Judiciary Committee produced a report summarizing a proposal to move almost entirely to the Model Penal Code approach for mens rea.[211] That larger effort never became law.[212] But the CFAA in 1984 was part of a much larger omnibus criminal law reform bill that did in part arise out of that larger reform effort. Both the House[213] and Senate[214] Committee Reports for the 1986 amendments liberally quote from a 1980 House Judiciary Committee Report that contained the full proposal for a Model Penal Code approach.[215]

The Supreme Court has apparently followed these breadcrumbs. By 1980, the Court noted this general change from the common law mens rea approach to the Model Penal Code approach.[216] *Rehaif* expressly relied upon the Model Penal Code in noting that a mens rea term should apply to all elements unless a contrary purpose appears.[217] *Rehaif*, in turn, interpreted a 1986 federal criminal law that itself arose during this larger federal criminal law reform effort.[218]

---

207. H.R. REP. NO. 99-612, at 9-10.

208. *See id.* at 5.

209. *See* Ronald L. Gainer, *Federal Criminal Code Reform: Past and Future*, 2 BUFF. CRIM. L. REV. 45, 97-98, 101 (1998); William S. Lofquist, *Legislating Organizational Probation: State Capacity, Business Power, and Corporate Crime Control*, 27 LAW & SOC'Y REV. 741, 749 (1993).

210. Lofquist, *supra* note 209, at 749.

211. H.R. REP. NO. 96-1396 (1980).

212. *See* Sanford H. Kadish, *Fifty Years of Criminal Law: An Opinionated Review*, 87 CAL. L. REV. 943, 949 (1999).

213. H.R. REP. NO. 99-612, at 9-10.

214. S. REP. NO. 99-432, at 6 (1986).

215. H.R. REP. NO. 96-1396.

216. United States v. Bailey, 444 U.S. 394, 403-04 (1980); United States v. U.S. Gypsum Co., 438 U.S. 422, 444 (1978).

217. Rehaif v. United States, 139 S. Ct. 2191, 2195 (2019).

218. *See id.* at 2194.

2. Step Two

When the mens rea term "intentionally" is applied to the element "without authorization," it collapses into *knowingly*. This follows directly from ordinary Model Penal Code interpretative rules.[219] The element "without authorization" is an attendant circumstance, primarily because it is neither the conduct of the statute ("access") nor any proscribed result.

Plus, "intentionally" in the sense of "purposely" makes no sense for an attendant circumstance such as "without authorization," and, therefore, it must collapse into *knowingly*. That is, we do not require that the person *wanted* her access to be unauthorized, simply that she knew it was. True, one could imagine hackers who do consciously want their access to be unauthorized—those who hack into a Pentagon website might do so for the challenge *because* they are excluded. But common sense tells us the CFAA is not limited to hackers who hack only for the challenge and not, for example, money.

3. Step Three

Supreme Court precedent also shows that the mens rea for "without authorization" in the CFAA should be *knowingly* for a separate, but critical, reason. The Court has repeatedly held that when a federal criminal statute contains a mens rea of "knowingly," it applies to every element that divides criminal from innocent conduct.[220] For example, child pornography laws prohibit the knowing possession of an image that depicts the sexual conduct of a minor.[221] The Court requires "knowingly" to apply not only to the possession of an image, but also knowledge that the person depicted

219. *See* H.R. REP. NO. 99-612, at 10 (1986) ("The term 'purposeful' in the Model Penal Code is the equivalent of 'intentional' in the proposed code."); MODEL PENAL CODE § 2.02(2) (AM. L. INST. 1962) (providing that "purposely" defaults to "knowingly" for attendant circumstances).

220. *Rehaif*, 139 S. Ct. at 2195; United States v. X-Citement Video, Inc., 513 U.S. 64, 72 (1994) ("[T]he presumption in favor of a scienter requirement should apply to each of the statutory elements that criminalize otherwise innocent conduct."); *see* Staples v. United States, 511 U.S. 600, 618-19 (1994).

221. *See, e.g.*, 18 U.S.C. § 2252(a).

is a minor and that they are engaged in sexual activity.[222] This follows, the Court reasoned, because without the element of a "minor," for example, the person knowingly possesses adult pornography and such possession is not a crime.[223]

The Supreme Court has not directly addressed the mens rea under the CFAA, but the above test applies in a straightforward manner. Under the CFAA, the element of "without authorization" is necessary to transform innocent conduct (merely accessing a computer) into criminal conduct (doing so without authorization). Therefore, the existing mens rea term of "intentionally" must apply to "without authorization"—though again, it collapses into *knowingly*.

Finally, a clarifying note: the CFAA also criminalizes "exceed[ing] authorized access" as an alternative to access "without authorization."[224] I have already argued that the test for this alternative is the same as for access "without authorization."[225] As for mens rea, the same principles from above apply. The force of the term "intentionally" continues to apply to all later elements unless a contrary purpose plainly appears, and none does here. In addition, the exceeding authorized access element—which prohibits one from obtaining files that he is not entitled to obtain—would be the only element separating innocent from criminal behavior. Under the line of Supreme Court cases referenced above, this "exceeding" element also requires that the mens rea of *knowingly* apply.[226] Finally, in the House Report from 1984, Congress said that the mens rea for the element that ultimately became "exceeding authorized access" was "knowingly."[227]

Unfortunately, lower courts construing the CFAA in particular pay little heed to the mens rea in this context. Some have applied the negligence standard of "has reason to know."[228] Others, such as

222. *X-Citement Video*, 513 U.S. at 78.
223. *See id.* at 72-73.
224. 18 U.S.C. § 1030(a)(2).
225. *See supra* notes 56-61 and accompanying text.
226. *See supra* notes 220-23 and accompanying text.
227. *See* H.R. REP. NO. 98-894, at 2-3, 20 (1984).
228. *See, e.g.*, United States v. John, 597 F.3d 263, 273 (5th Cir. 2010).

Nosal I, have treated the statute as having no apparent mens rea based merely upon its voluminous illustrations.[229]

C. An Enhanced Knowingly

In 1986, Congress made clear that it sought a mens rea that was a heightened version of "knowingly" as applied to "without authorization."[230] In the original 1984 statute, Congress used the mens rea term "knowingly."[231] In doing so, it expressly intended the somewhat watered-down version of "knowingly" contained in the Model Penal Code and elsewhere in criminal law. This watered-down "knowingly" included the mens rea of "practically certain," Congress said in its legislative report.[232] This "knowingly" also included "willful blindness."[233] This latter term means a person might merely be aware of the probability, or high probability, that a fact is true and yet be deemed to meet the mens rea of "knowingly" if she ignored facts that would lead to knowledge.[234]

In 1986, Congress amended the statute and substituted "intentionally" for "knowingly" as the mens rea.[235] As noted above, under ordinary circumstances, this change should not really create a change with respect to "without authorization" because "intentionally" collapses into *knowingly* when applied to a circumstance rather than to conduct.[236] What did Congress hope to accomplish, then, by substituting "intentionally"?

The legislative report for the 1986 amendment is not entirely clear, but it appears Congress wanted to want to rule out any watered-down versions of *knowingly*. It refers to the new standard as "a slightly higher state of mind standard ... than 'knowingly.'"[237]

---

229. *Nosal I*, 676 F.3d 854 (9th Cir. 2012). *But see id.* at 864, 866 (Silverman, C.J., dissenting) (arguing for a mens rea of "knowingly").

230. H.R. REP. NO. 99-612, at 2 (1986).

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

232. H.R. REP. NO. 98-894, at 17, 20 (1984).

233. *Id.* at 16-17, 20.

234. *Id.*

235. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(a)(1), 100 Stat. 1213, 1213.

236. *See supra* Part III.B.2.

237. H.R. REP. NO. 99-612, at 6-7 (1986).

For example, the report notes that "knowingly" includes not only to "know" but also to be "practically certain."[238] The report says Congress wanted to rule out the alternative of "practically certain."[239] In other words, it wanted to define "knowledge" as "certain."

The report also says that it substituted "intentionally" to limit prosecutions to those who have "clear intent to" access, "without [proper] authorization," the files or data of another.[240] Finally, the new mens rea in the 1986 amendment to the CFAA appears to rule out the lower version of "knowingly" that can be met by "willful blindness."[241] The House Report for the original law states that "willful blindness" would have sufficed to meet the "knowingly" standard.[242] The new mens rea of "intentionally" appears to be intended to eliminate this "willful blindness" version of "knowingly" just as much as it eliminates "practically certain."

D. Mistake of Law

The federal mens rea of *knowingly* in the CFAA will also afford defendants a species of mistake of law defense that will rule out an entire class of potentially unjust cases. The leading example of this type of unjust case is *Citrin*.[243] There, the Seventh Circuit held that an employee who uses his work computer for personal reasons adverse to his employer's interests, rather than for work reasons, breached his state law duty of loyalty.[244] This breach of a separate state law revoked his authorization to access his employer's

238. *Id.* The Report includes an explanation that muddies the waters. It appears motivated to protect insiders who enjoy authorized access but then "stumble into" unauthorized files by "mistake[]." *See id.* at 10. One could argue Congress intended the new, enhanced mens rea to apply to "exceeding authorized access" cases only. But regardless of its original motivation, the new mens rea textually applies to both alternatives, "without authorization" and "exceeds authorized access." It would be difficult to interpret the "intentionally" differently for each.

239. *See id.* at 9-10.

240. *Id.* at 70; *see also* Thaw, *supra* note 188, at 914 (noting the heightened mens rea and that courts have unfortunately "whittled away" this protection).

241. 18 U.S.C. § 1030(a)(2).

242. H.R. REP. NO. 98-894, at 16-17, 20 (1984) (cross-referencing the mens rea for the counterfeit device provisions of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984).

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

244. *Id.* at 420.

computer.[245] The defendant was held liable even though he did not know about this separate state law or its effect on his access rights.[246]

The Ninth Circuit in *Nosal I* correctly parodied this holding. It asked, sarcastically, whether an employee who uses his work computer to check the weather for "the company softball game" violates this duty of loyalty and thus exposes himself to prosecution under the CFAA.[247] This cannot be the law, the *Nosal I* court declared.[248] Therefore, the court concluded that terms and conditions, or even other state laws, can never be the premise for a CFAA violation.[249]

We can agree with the complaint in *Nosal I* without accepting its overbroad solution because a mens rea of *knowingly* solves the problem. It solves the problem by including the type of mistake of law defense that means such an employee cannot violate the CFAA. This hypothetical employee surely does not know that breaching the duty of loyalty by looking up the weather would lead, by operation of law, to a revocation of his access rights.

Criminal law traditionally denies defendants a mistake of law defense if his mistake or ignorance is about the very law under which he is prosecuted.[250] That is, a defendant cannot claim he was unaware of or mistaken about the CFAA itself. But the mens rea of *knowingly* does supply a mistake of law defense about a *separate* law that determines whether an element of the criminal law is met. In this case, the mens rea of *knowingly* means that the prosecution must show that a defendant knows about any separate law that determines whether access is "without authorization" and must understand its application to his conduct.

The Supreme Court in *Rehaif v. United States* held that the mens rea of "knowingly" in the federal statute at issue includes exactly

245. *Id.*
246. *See id.*
247. *Nosal I*, 676 F.3d 854, 858 (9th Cir. 2012).
248. *See id.* at 862-64.
249. *See id.*
250. *See, e.g.*, Cheek v. United States, 498 U.S. 192, 199 (1991) (discussing voluminous case law on the issue while recognizing a term of "willfully" can sometimes afford a mistake of law defense).

this type of mistake of law defense.[251] I consider *Rehaif* here in some detail because the Supreme Court interpreted a law that closely resembles the CFAA and the facts of the case make this resemblance clear.

In *Rehaif*, the defendant "entered the United States on a nonimmigrant student visa."[252] He did poorly in school and received notification that he would lose his visa because of his poor grades if he did not transfer to another school.[253] At some point after receiving this notification, he went to a firing range to fire guns.[254]

Rehaif was arrested, prosecuted, and convicted of federal gun possession as an "alien" in the United States "illegally or unlawfully."[255] At trial, he argued the prosecution must prove not only that he was here unlawfully, but also that he *knew* he was here unlawfully.[256] The trial judge disagreed and the jury convicted.[257]

On appeal, the Supreme Court reversed.[258] In doing so, it made several holdings directly relevant to the CFAA. First, as noted above, it held that the mens rea term "knowingly" applies to the element "illegally or unlawfully in the United States."[259]

Once it applied "knowingly" to the element of being in the United States "unlawfully or illegally," the Court explained that this mens rea term affords a type of mistake of law defense.[260] It does not afford a mistake of law defense as to the federal criminal gun law, but it does afford one as to the immigration law that would tell a defendant whether he was in the United States "illegally or unlawfully."[261] Under that law, the prosecution must prove that a defendant understood that a separate immigration law made his presence unlawful.[262]

---

251. 139 S. Ct. 2191, 2194, 2198 (2019).
252. *Id.* at 2194.
253. *Id.*
254. *Id.*
255. *Id.*
256. *Id.*
257. *Id.*
258. *Id.* at 2195.
259. *Id.* at 2198.
260. *Id.*
261. *Id.*
262. *Id.* at 2200.

The *Rehaif* facts and law closely parallel the CFAA. The gun law bans conduct if undertaken by a person present in the United States "unlawfully."[263] The CFAA bans conduct—access to a computer—undertaken without authorization.[264] The gun law requires that an individual understand how a separate law—the immigration law—determines whether he is in the country lawfully.[265] Therefore, the CFAA should require, in a case such as *Citrin*, that prosecutors prove the defendant knew that a separate law, such as the state tort duty of loyalty, renders his access without authorization.[266]

IV. LESSONS FROM STATE CRIMINAL TRESPASS

This Part draws lessons from ordinary state criminal trespass statutes and case law to shed light on the CFAA. It first shows why Congress intended courts to look to these sources. It then shows how criminal trespass supports a mens rea of *knowingly* and, indeed, an enhanced mens rea that requires "personally communicated" notice for public places.

On the one hand, as I then show, the criminal trespass cases make clear that "without authorization" means what it says—"keep off."[267] Criminal trespass cases afford property owners, even of public places, great power to unilaterally and selectively exclude whomever they wish, even as courts sometimes acknowledge the potential injustice of such a property-preferring regime. Courts in these ordinary criminal trespass cases have uniformly rejected the argument that the term "without authorization" or its synonyms are unconstitutionally vague.

On the other hand, this plain meaning view of the CFAA produces normatively undesirable results. It is the best interpretation of the statute, I argue, but also a reason to abolish it. I return to the trespass cases in the final Part of this Article to glean more lessons from historical trespass cases. These cases involve overt racial discrimination and illustrate the underlying injustices of the crime

263. *Id.*
264. 18 U.S.C. § 1030(a)(2).
265. *Rehaif*, 139 S. Ct. at 2198.
266. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).
267. *See* Martin v. City of Struthers, 319 U.S. 141, 147 (1943).

of trespass and why we should not expand its ambit to criminalize virtual trespass, as the CFAA currently does.

A. Why Criminal Trespass?

The congressional committee reports repeatedly state that they are enacting a computer trespass statute that should be viewed as akin to ordinary trespass. The House Report for the original 1984 law noted the problem of hackers who "access (trespass into)" computers.[268] The legislation would address a "flurry of electronic trespass[es]."[269] Similarly, the 1986 House Report accompanying the amended legislation repeatedly referred to the misdemeanor offense conduct as "trespass" or "computer trespass."[270] The Senate Report repeatedly denotes the trespass provision not only as "trespass" but also as "simple trespass," which is a misdemeanor.[271]

Courts[272] and scholars[273] agree Congress intended to analogize to "trespass" law. The Second Circuit summarized the consensus: "Consequently, the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in

---

268. H.R. REP. NO. 98-894, at 10 (1984).

269. *Id.*

270. *See* H.R. REP. NO. 99-612, at 10-11 (1986).

271. *See* S. REP. NO. 99-432, at 7 (1986).

272. *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000 (9th Cir. 2019) (pointing to the 1984 House Report that equates a hacker's access to a "trespass into"), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020); *Nosal I*, 676 F.3d 854, 858 (9th Cir. 2012) ("Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, '[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system.'" (alteration in original) (quoting S. REP. NO. 99-432, at 9)); Sandvig v. Sessions, 315 F. Supp. 3d 1, 24 (D.D.C. 2018) ("Congress thus viewed exceeding authorized access as the digital equivalent of being allowed into a house but entering a room within it that the owner has declared to be off-limits.").

273. *See, e.g.*, Kerr, *supra* note 5, at 1617 ("[T]he available evidence suggests that legislators mostly saw [computer crime] statutes as doing for computers what trespass and burglary laws did for real property."); Goldfoot & Bamzai, *supra* note 17, at 1494 ("By incorporating the rules of physical trespass in the CFAA, Congress also incorporated the relevant norms of trespass."); Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 GEO. WASH. L. REV. 1703, 1711 (2016) ("In its original 1984 computer crime legislation, Congress ... only focused on the crimes of 'computer damage' and 'computer trespass.'").

terms of the portion of the computer's data to which one's access rights extend."[274]

Neither courts nor the legislative history expressly use the term "*criminal* trespass." They just use "trespass." But it must be contemporary criminal trespass statutes we analogize to for several reasons.[275]

First, the CFAA is a criminal statute.[276] Its trespass provision imposes misdemeanor criminal liability just as most criminal trespass statutes do.[277]

Second, the text of the CFAA precisely tracks the text of criminal trespass statutes. For example, many states define criminal trespass as knowingly entering "without authority," "without authorization" or when "not authorized."[278] The Model Penal Code[279] and many other states, such as New York,[280] use the synonym not "licensed or privileged" to enter.[281] Other states use other synonyms for this element including "without permission," and "without effective consent."[282]

State criminal trespass statutes thus all share practically the same structure: (i) knowing entry, (ii) without authorization, (iii) to a building or other structure. We can see how closely the CFAA tracks this structure and meaning: (i) intentional access (ii) without authorization (iii) to a computer.[283]

Remember, here and elsewhere, that it is the text of the CFAA, of course, that governs. When the structure and actual language

274. United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015).

275. 18 U.S.C. § 1030(c).

276. *Id.* § 1030.

277. *Id.* § 1030(c)(2)(A).

278. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-1501(2) (2020) ("not ... authorized"); FLA. STAT. ANN. § 810.08(1) (West 2017) ("without being authorized"); GA. CODE ANN. § 16-7-21(b) (2019) ("without authority"); 720 ILL. COMP. STAT. ANN. 5/19-4(a)(1) (West 2020) (residential, "without authority"); KAN. STAT. ANN. § 21-5808(a)(1) (West 2012) ("not authorized"); LA. STAT. ANN. § 14:63(A) (2020) ("without express, legal, or implied authorization"); MISS. CODE. ANN. § 97-17-97(1) (2013) ("without authority"); N.C. GEN. STAT. § 14-159.12(a) (2020) ("without authorization"); VT. STAT. ANN. tit. 13, § 3705(a)(1) (2020) ("without legal authority"); VA. CODE ANN. § 18.2-119 (2019) ("without authority of law").

279. MODEL PENAL CODE § 221.2(1) (AM. L. INST. 1962).

280. N.Y. PENAL LAW § 140.00(5) (McKinney 2020).

281. *See* LAFAVE, *supra* note 22, § 21.2(a) (collecting statutes).

282. *See id.* (noting that terms like authorization, license, and privilege are basically the same for purposes of criminal trespass).

283. *See supra* note 278 and accompanying text.

of the text so precisely track criminal trespass statutes, that similarity should garner far more attention than the legislative history, even if that history did not support the text in showing that criminal trespass must be the analogy.

Third, it must be *contemporary* criminal trespass for the simple reason that criminal trespass was not a crime at common law, unlike larceny or burglary. The leading treatises of common law crime do not mention "criminal trespass."[284] All made clear that burglary was the primary crime that protected homes, and burglary has many elements that differ substantially from trespass, including breaking and entering and the specific intent to commit a felony therein.[285] Blackstone also recognized "forcible entry" to lands as a crime, but it required "force, with violence, and unusual weapons" and did not appear limited to or even chiefly concerned with dwellings or other buildings.[286] Not until the twentieth century did state legislatures pass criminal trespass statutes similar to those today.[287]

The legislative history also makes clear Congress's intent to analogize the CFAA to contemporary criminal law by repeatedly referencing the Model Penal Code, as detailed above.[288] In turn, the Model Penal Code itself represents contemporary criminal law and

---

284. *See* 4 WILLIAM BLACKSTONE, COMMENTARIES; 1 MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN (1736); 1 WILLIAM HAWKINS, A TREATISE OF THE PLEAS OF THE CROWN (1716).

285. *See* 4 BLACKSTONE, *supra* note 284, at *270-71; 1 HALE, *supra* note 284, at 547-48; 1 HAWKINS, *supra* note 284, at 101.

286. 4 BLACKSTONE, *supra* note 284, at *171-72. It is true that the common law did allow for indictable trespasses under certain circumstances as misdemeanors. *See, e.g.*, Miller v. Harless, 149 S.E. 619, 624 (Va. 1929); Henderson v. Commonwealth, 49 Va. (8 Gratt.) 708, 710 (1852). Courts would essentially elevate a tort trespass into a misdemeanor if that trespass also threatened to breach the public peace. *See, e.g.*, *Miller*, 149 S.E. at 624*; Henderson*, 49 Va. (8 Gratt.) at 710. For trespass to houses and other buildings, courts in England and the early republic, as well as treatises, announced the same basic principle: a mere trespass would remain a civil cause of action unless there was a breach of the peace as might be wrought by force against the inhabitant or a potential for such a faceoff. *See, e.g.*, *Henderson*, 49 Va. (8 Gratt.) at 710; R v. Storr (1765) 97 Eng. Rep. 1053, 1053 (KB); 1 HAWKINS, *supra* note 284, at 141. Time and again courts insist upon the line between criminal and civil, relegating a homeowner to civil remedies for trespass. *See, e.g.*, *Henderson*, 49 Va. (8 Gratt.) at 710; *Storr*, 97 Eng. Rep. at 1053; 1 HAWKINS, *supra* note 284, at 141.

287. *See* Martin v. City of Struthers, 319 U.S. 141, 147 (1943) (citing statutes); MODEL PENAL CODE § 221.2 cmt. at 85-86 (AM. L. INST. 1980).

288. *See supra* Part III.C.

a focus on clear statutory crimes that give notice.[289] Its overall philosophy focused on elemental analysis: breaking a statute down into its elements and determining what mens rea applied to each element.[290]

B. Criminal Trespass—Mens Rea

A majority of states require that the person making entry *knows* her entry is without authorization.[291] New York's statute makes a person guilty of trespass who "knowingly enters or remains unlawfully [without license]."[292] Courts in New York,[293] as elsewhere,[294] apply this "knowingly" element to the term "unlawfully," as well as to the term "enters." That is, the prosecutor must show the defendant *knew* her entry was without license.[295] A standard lower than knowledge is "exceedingly rare."[296]

Many states also permit a type of mistake of law defense to the extent that license or authorization depends upon interpretation of some other law other than the trespass law itself, such as property or contract law.[297] These sources closely parallel the sources relied upon in *Rehaif v. United States*, detailed above, in recognizing a mistake of law defense.[298] For example, a landlord who enters a tenant's residence may not know that state law does not afford him authorization to do so under those circumstances; the entry is without authorization, but not criminal trespass if the landlord does not actually know this separate law.[299]

This defense makes sense. After all, license or authorization are, in a sense, facts—a person says, "Get out." License also requires

---

289. *See* MODEL PENAL CODE § 1.02(1)(d), (2)(d).

290. Herbert Wechsler, *Codification of Criminal Law in the United States: The Model Penal Code*, 68 COLUM. L. REV. 1425, 1436-37 (1968).

291. LAFAVE, *supra* note 22, § 21.2(c).

292. N.Y. PENAL LAW § 140.10 (McKinney 2020).

293. *See, e.g.*, People v. Luke, 955 N.Y.S.2d 465, 469 (App. Div. 2012).

294. *See, e.g.*, State v. Pugh, 357 S.W.3d 310, 314 (Mo. Ct. App. 2012).

295. *Luke*, 955 N.Y.S.2d at 469; LAFAVE, *supra* note 22, § 21.2(c).

296. LAFAVE, *supra* note 22, § 21.2(c).

297. *Id.* § 21.2; *see also* State v. Fanger, 665 A.2d 36, 38 (Vt. 1995).

298. *See supra* Part III.D.

299. *Cf. Fanger*, 665 A.2d at 37-38 (finding property manager did know his entry was unlawful based upon his wrongful purpose).

some application of law in determining, for example, whether the person who said "get out" was authorized by law to do so.

These observations about the mens rea for trespass cases provide additional support for the proposition that the CFAA mens rea for "without authorization" should be *knowingly* and that this standard should afford a mistake of law defense. Congress borrowed terms from criminal trespass laws for the CFAA, and it analogized the CFAA to criminal trespass statutes in the legislative history. We can therefore infer Congress intended an interpretation of the CFAA's mens rea to parallel that of criminal trespass statutes.

C. Enhanced Mens Rea

In addition, state criminal trespass statutes usually require an additional element of notice, such as a fence or a sign that makes clear that entry is unlawful.[300] After all, community custom usually provides implicit permission for a person to enter even private places, such as a walkway up to a suburban home or the lobby of a city apartment building.[301] A fence or sign that says "no trespassing" makes clear that the owner has overridden this implicit license.[302] The sign also provides unambiguous clarity to support the finding of mens rea. Defendants should be on particular notice, a high level of evidentiary mens rea, before we will criminalize the simple act of entering a place, particularly a quasi-public place, such as an apartment lobby or public housing.[303]

Note, of course, that the requirement of a sign or a fence is in addition to the requirement of the mens rea of "knowingly." Criminal trespass laws do not substitute the sign or fence for "knowingly," imposing any kind of "should have known" standard. If the person fails to read the sign, or understand it, or does not understand that the fence means keep out, the prosecution has not

---

300. *See, e.g.*, N.Y. PENAL LAW § 140.10(a) (McKinney 2020); 18 PA. STAT. AND CONS. STAT. ANN. § 3503(b) (West 2020) ("defiant trespasser"); MODEL PENAL CODE § 221.2(2) (AM. L. INST. 1962) (same).

301. Florida v. Jardines, 569 U.S. 1, 8 (2013) ("A license may be implied from the habits of the country." (quoting McKee v. Gratz, 260 U.S. 127, 136 (1922))).

302. State v. Merhege, 394 P.3d 955, 957, 959 (N.M. 2017).

303. People v. James, 902 N.Y.S.2d 293, 298 (Crim. Ct. 2010) (summarizing legislative history and purpose of sign requirement and collecting cases).

proved "knowingly."[304] Of course, the presence of a sign might lead a jury to conclude that a particular defendant did, subjectively, know her entry was unlawful.

For places open to the public, many criminal trespass laws require an even higher version of "knowingly": "personally communicated" notice.[305] In places that are open to the public, such as malls or stores, or places that are actually public places, such as Amtrak stations or government buildings, trespass statutes often require express, face-to-face notice to a person that that person is banned from entering in particular.[306] These face-to-face notices are also often required in cases in which the initial entry is lawful but the person is demanded to leave. Before a person can be convicted of trespass based on remaining only, the person must have been told to leave face-to-face.[307] Hawaii's second degree trespass law requires *written* notice to stay away from a business.[308]

New York's criminal trespass statute became a model for other jurisdictions and illustrates many of these general principles.[309] The statute makes it a mere violation—not a criminal offense—to knowingly enter or remain unlawfully upon a building or real property.[310] The statute requires more to make it a crime. To simplify, it requires either (i) a fence or other enclosure "designed to exclude intruders," (ii) a conspicuously posted sign setting forth the rules for entry, or (iii) a personally communicated request to leave.[311]

---

304. *E.g.*, People v. Luke, 955 N.Y.S.2d 465, 469 (App. Div. 2012) (sign prominently posted but court held defendant did not know his entry was in violation of the sign's prohibition).

305. *See, e.g.*, ARK. CODE ANN. § 5-39-101(3)(B)(i) (2020); N.Y. PENAL LAW § 140.00(5); LAFAVE, *supra* note 22, § 21.2(a) (collecting statutes).

306. *See, e.g.*, CAL. PENAL CODE § 602(10) (West 2020).

307. N.Y. PENAL LAW § 140.00(5).

308. HAW. REV. STAT. ANN. § 708-814(1)(b) (LexisNexis 2019) (A "'reasonable warning or request' means a warning or request communicated in writing.").

309. N.Y. PENAL LAW § 140.10; *see also* State v. Lucio-Camargo, 18 P.3d 467, 470 (Or. Ct. App. 2001) (noting influence of New York statute), *vacated on other grounds*, 52 P.3d 1056 (Or. 2002); MODEL PENAL CODE § 221.2 cmt. at 89 ("A large number of states have followed the New York provision, which applies to one who 'knowingly enters or remains unlawfully.'") (AM. L. INST. 1980).

310. N.Y. PENAL LAW § 140.10.

311. *Id.* §§ 140.00, .05, .10.

In addition, New York law presumes entry to any place open to the public is licensed.[312] It can only become trespass if the person "defies a lawful order" from the owner "not to enter or remain," and this order must be "personally communicated" to the person.[313]

D. Personally Communicated Notice and the CFAA

We arrive at a fundamental question: should courts import or read into the CFAA an additional requirement not actually in its text? Specifically, for public platforms, should a defendant be shown to have defied a personally communicated order to stay off the platform before we deem his access to be knowingly without authorization? I argue we should, though as with any judicial gloss, the case is far from certain.

I provide three reasons to support the addition of a personally communicated requirement for public platforms. First, it follows Congress's desire to establish an enhanced mens rea as shown in its legislative history: a *knowingly* that is "clear" and rules out any watered-down version. Second, as a policy matter, it addresses a future that Congress did not foresee—public platforms analogous to malls, parks, and stores. Third, some courts have already required personally communicated notice in the form of cease-and-desist letters, at least in dicta, but without linking the requirement to any principle. My proposal would link this existing requirement, a cease-and-desist letter, to the analogous existing requirement in state trespass statutes. I elaborate on these three reasons below.

First, as detailed above, Congress in 1986 substituted "intentionally" for "knowingly" in order to create an enhanced version of *knowingly* as applied to the term "without authorization."[314] Congress said it wanted it to be "clear" a defendant knew she was accessing without authorization.[315] We can, of course, leave it to juries to determine based on the facts whether a prosecutor has proved clear knowledge beyond a reasonable doubt.

---

312. *Id.* § 140.00.
313. *Id.*
314. *See supra* Part III.C.
315. *See, e.g.*, H.R. REP. 99-612, at 9-10 (1986).

But state legislatures have concluded that the mens rea of "knowingly" does not sufficiently protect individuals when it comes to public places.[316] These states concluded that it would be vastly unfair to allow a person to be convicted of a crime for entering a public place without personalized notice *in addition* to the mens rea requirement that she knew her entry was unlawful.[317] The notice requirement serves as an objective, irreducible indicator that the defendant truly knew.

Thus, it makes sense to add this same requirement to the CFAA, as applied to public platforms. Like parks, malls, and stores, a person accessing a public platform, even without logging in or creating an account, may not *truly* believe her access is without authorization, even if she is aware of some term of service that prohibits her access. She may think, "Oh, they don't really mean that." A cease-and-desist letter, addressed to her, prohibiting further access, ensures she knows any such further access would be without authorization. She now knows they do "really mean it," since they went to the trouble to create individualized notice. It avoids unfairness and possible surprise that exists in malls, parks, and web platforms alike.

One might ask, then, why did Congress not add a requirement of a cease-and-desist letter in the text of the CFAA? The answer leads to my second argument: Congress likely did not have in mind public web platforms, such as LinkedIn or Facebook, in 1984 or 1986. Tim Berners-Lee invented the web in 1989 and wrote its protocols in 1990;[318] the web did not gain widespread use until later in the 1990s.[319]

Rather, Congress originally envisioned and enacted a CFAA that applied to private computers and information, such as classified information or financial data and government or bank computers, only.[320] It envisioned a paradigm in which an authorized user must

316. *See supra* notes 305-13 and accompanying text.

317. *See supra* notes 305-13 and accompanying text.

318. *A Short History of the Web*, CERN, https://home.cern/science/computing/birth-web/short-history-web [https://perma.cc/UYF3-W3PV].

319. *Id.*

320. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190-92.

log into such a system using a password to gain legitimate access.[321] Paradigmatically, at least, the CFAA protected such private information and places only.

But in later years, Congress expanded the type of information and computers far beyond these categories of private information and places to include any information and any computer connected to the internet.[322] In doing so, it expanded, perhaps inadvertently, the ambit of the CFAA to include public platforms, even though these computers go beyond the original paradigm of a government or bank computer containing only certain, private information.

My proposal—personally communicated notice—inserts what Congress would have included had it foreseen public platforms because it relied so directly on ordinary physical trespass cases. My proposal also has a textual home: it arises naturally as an objective protector of the existing mens rea element that *is* in the statute.

Finally, some courts have already required, perhaps in dicta, such personally communicated notice. The Ninth Circuit in *Power Ventures* held that a cease-and-desist letter was not merely sufficient but also necessary to make the defendant's intrusion without authorization.[323] Unfortunately, the court did not root this requirement in any principle, such as borrowing from trespass law or as a required element to safeguard the mens rea.[324] We can backfill that justification, however, and root it in the requirement under many state criminal trespass laws requiring personally communicated notice for public places.

Nosal II similarly relied upon an *express* revocation of the defendant's authorization.[325] *Nosal II* is analogous to a trespass case premised on "remaining" rather than the original "entry," since the defendant previously had authorization.[326] It makes sense to impose a requirement of personally communicated notice as one might in an ordinary criminal trespass case that involves "remaining" rather than "entering."

---

321. H.R. REP. NO. 98-894, at 10 (1984).
322. *See supra* notes 44-48 and accompanying text.
323. 844 F.3d 1058, 1067-68 (9th Cir. 2016).
324. *Id.*
325. 844 F.3d 1024, 1028 (9th Cir. 2016).
326. *Id.* at 1029.

The justifications for requiring personally communicated notice help to sketch its particulars. To do its job, a personally communicated notice must be more than an automated pop-up from the website; this method would fail to alert an individual that the prohibition was personal and serious. Rather, the notice should occur along a channel separate from the web session, such as a postal letter.

In addition, the notice must not be conditional on purpose; rather, it must be an unconditional termination of authorization.[327] It cannot simply repeat ambiguous terms of service that might say, "You are forbidden by this notice if you continue to visit our site to scrape data." After all, it is unclear whether the CFAA even applies to wrongful purpose cases. Instead, the notice must simply say, "You may no longer access our site." This unconditional ban parallels the type of ban typical in real-world cases.[328]

E. Without Authorization

State criminal trespass law similarly affords us insights into the plain meaning of the term "without authorization" and shows the term is not unconstitutionally vague in the CFAA or in state criminal trespass cases. It simply means that the property owner does not want the individual there. For example, the commentaries to the Model Penal Code section on criminal trespass noted a common thread among the then-existing state laws: "unwanted intrusion, usually coupled with some sort of notice."[329] Or, as Wayne

327. *See* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) (finding cease-and-desist letter valid under CFAA in part because it unconditionally prohibited the defendant's access "for any purpose").

328. State v. Zimbelman, No. 111759, 2015 WL 4577693, at *1 (Kan. Ct. App. July 24, 2015) (quoting the form Walmart uses for personally communicated notice: "This document constitutes formal notice and warning that you are no longer allowed on Walmart property" and the defendant's written acknowledgment that he was "prohibited from entering Walmart property").

329. MODEL PENAL CODE § 221.2 cmt. at 87 (AM. L. INST. 1980).

LaFave puts it, the owner or agent has "forbid[den] ... entry."[330] An early Supreme Court case said it means "keep off."[331]

Many trespass statutes use the exact term, "without authorization," or synonyms such as without consent, license, or privilege.[332] Trespass cases have also expressly held that "without authorization" and its synonyms are not unconstitutionally vague.[333] The Supreme Court, speaking of a state trespass law, noted that "[t]here is no lack of notice in this law, nothing to entrap or fool the unwary."[334] The Florida Supreme Court similarly concluded that the term "authorized" in the trespass statute was not vague.[335] The court "conclude[d] that the challenged terms are of such common understanding and usage that persons of ordinary intelligence are fully able to determine what conduct is proscribed by the challenged enactment."[336] The Georgia Supreme Court similarly held that its state criminal trespass statute was not unconstitutionally vague and that an officer's warning to "stay out" constituted sufficient notice.[337]

These state trespass cases also help us understand the layers of presumptions with respect to licenses. The default for any visitor is no license. To own property means to have the right to exclude, and exclusion is assumed. But custom can override this presumption to

---

330. LAFAVE, *supra* note 22, § 21.2(a). ("[T]he [typical] rule as to private premises is that the mere demand of the owner constitutes a lawful order for the purposes of the criminal trespass statute, so that the reason for requesting removal is irrelevant." (internal quotations omitted)).

331. *See, e.g.*, Martin v. City of Struthers, 319 U.S. 141, 147 (1943) ("Traditionally the American law punishes persons who enter onto the property of another having been warned by the owner to keep off.").

332. *See supra* notes 278-82 and accompanying text.

333. *See, e.g.*, Adderley v. Florida, 385 U.S. 39, 42 (1966); Ahmed v. Rockefeller, 308 F. Supp. 935, 937 (S.D.N.Y. 1970); State v. Steinmann, 569 A.2d 557, 560 (Conn. App. Ct. 1990); Downer v. State, 375 So. 2d 840, 843 (Fla. 1979), *habeas corpus granted sub nom.* Cohen v. Katsaris, 530 F. Supp. 1092 (N.D. Fla. 1982). The federal district court in *Cohen* agreed with the Florida Supreme Court that the term "authorized" was not unconstitutionally vague. 530 F. Supp. at 1094-95. It did rule, however, that the application of the term "structure" in the statute to the defendant was unconstitutionally vague. *Id.* at 1096-97.

334. *Adderley*, 385 U.S. at 42.

335. *Downer*, 375 So. 2d at 843.

336. *Id.* On the other hand, some courts have held that trespass laws may implicate vagueness concerns for government buildings apparently because these are not private property and, therefore, directly involve First Amendment rights. *E.g.*, City of Seattle v. Rice, 612 P.2d 792, 793 (Wash. 1980).

337. Rayburn v. State, 300 S.E.2d 499, 500 (Ga. 1983).

create a new one.[338] A person who opens her store to the public creates for all an implied license to enter.[339]

This implied license, in turn, can be revoked by the business owner at any time and for any reason.[340] She can keep her store open to all the public except one person, and in most jurisdictions, she can exclude that person for nearly any reason whatsoever including race, at least under traditional trespass law, though civil rights statutes supersede such discriminatory use of trespass law in many but not all contexts.[341] These straightforward trespass principles often lead to unjust results;[342] courts nevertheless stand behind this plain meaning understanding of "without authorization."[343]

A relatively recent trespass case illustrates the foregoing. In *Alexis v. McDonald's*, after a Black customer and a white manager argued over an order, the manager ordered the customer and her family to leave.[344] The family refused and took their food to a table where they ate in apparent peace.[345] The manager nevertheless summoned an officer who told them they would be arrested if they did not leave and, when they did not, arrested the mother.[346] The officer made a racist remark as he did so.[347]

A jury acquitted Alexis of trespass, and she then sued both the manager and the officer for a violation of her civil rights.[348] The court held that the officer was potentially liable, but that the arrest itself was based upon probable cause.[349] The McDonald's manager

338. Florida v. Jardines, 569 U.S. 1, 8 (2013).

339. *E.g.*, State v. Paye, 865 N.W.2d 1, 5 (Iowa 2015).

340. *E.g.*, State v. Zimbelman, No. 111759, 2015 WL 4577693, at *3 (Kan. Ct. App. July 24, 2015).

341. Alexis v. McDonald's Rests. of Mass., Inc., 67 F.3d 341, 350-51 (1st Cir. 1995). True, some jurisdictions require the reason to be a condition that applies to all—much like a platform's terms of service. *Id.*

342. City of Greenville v. Peterson, 122 S.E.2d 826, 828 (S.C. 1961) (holding selective right of private individual to exclude includes right to exclude based on race), *rev'd on other grounds*, 373 U.S. 244 (1963) (sidestepping private trespass law, finding state action, and deciding the case under the Equal Protection Clause); *see also infra* Part VII.

343. *Peterson*, 122 S.E.2d at 828.

344. 67 F.3d at 345.

345. *Id.*

346. *Id.* at 345-46.

347. *Id.* at 346.

348. *Id.*

349. *Id.* at 348, 351.

had an unfettered right to decide to exclude anyone she wanted as long as it was not based on race, and in this case, the court held the evidence was insufficient to show that the exclusion was based on race.[350]

The court wrote, almost regretfully, that "Massachusetts recognizes [no] exception to the seemingly absolute right of a private business owner to withdraw, without cause, its implied license to enter a business establishment."[351] I say "regretfully" because the court said it scoured the precedents for some limit to the arbitrary power to exclude.[352]

Consider the very trespass case cited by the Ninth Circuit in *hiQ Labs*. In *Blankenhorn v. City of Orange*, a person entered a shopping mall, an area open to the public.[353] Normally he could enter like anyone else, but the defendant had been banned with a written order months before.[354] The police arrested him for criminal trespass, and the Ninth Circuit held that the arrest was valid as against the claim the police lacked probable cause.[355] The presumption that a person enjoys a license to enter a public place had, for Blankenhorn, been superseded by the ban to stay out.[356] In the words of the court, the ban transformed a place "open to the public," to one "not open to the public."[357]

On the other hand, the Model Penal Code and some states do provide some limits. These states allow an affirmative defense for criminal trespass to a public place if the person had abided by all the lawful conditions for entry imposed by the business.[358]

As an affirmative defense, this limit does not change the plain meaning of "unauthorized." Rather, it finds that even though the entry is unauthorized, it cannot be criminalized because the revocation of authorization is arbitrary. These statutes provide in express language for such a policy outcome. Moreover, the law does

350. *Id.* at 351.
351. *Id.* at 350.
352. *Id.*
353. 485 F.3d 463, 468 (9th Cir. 2007).
354. *Id.* at 467-68.
355. *Id.* at 472-73.
356. *Id.* at 474.
357. *Id.* (citing Picray v. Sealock, 138 F.3d 767, 772 (9th Cir. 1998)).
358. LAFAVE, *supra* note 22, § 21.2(a).

not limit the types of conditions a property owner may impose (other than that they be lawful). The conditions themselves can be unilateral and arbitrary. These states' trespass laws merely require that the person ejected be banned because she violated those conditions.

Trespass law thus affords property owners unilateral power to decree who may enter and who may not, certainly by general terms applicable to all and often on an individual, selective basis. Courts agree that this arbitrary power, enlisting law enforcement to secure a person's removal, does not make the term "without authorization" unconstitutionally vague—as long as a particular defendant knows she cannot enter or must leave.

V. APPLIED TO CFAA CASES

One may gather the foregoing threads to summarize their lessons for the CFAA. A mens rea of *knowingly* as applied to "without authorization" eliminates a great many of the unjust cases. Consider how much work *knowingly* does for terms of service, for example. It requires a prosecutor to show that the defendant read the terms of service, that she understood them, that she understood that those terms applied to her conduct and prohibited her conduct, and finally, that violating the term of service *terminated* her authorization.

As a result, it is not enough that a person should have read the terms of service, was aware of them, or was given specific notice where to find them. It is not enough that she scrolled through them and clicked "I agree" at the end. All of these facts might be enough to bind one to a contract term, but they do not establish the defendant *knew* of the terms of service. And even knowledge of the terms is not enough.

Next, she must understand those terms and that they apply to her conduct. An employer's manual may restrict the use of a computer to business tasks. To return to the example from *Nosal I*, is "check[ing] the weather report ... [f]or the company softball game" related to business?[359] We need not answer this metaphysical

359. *Nosal I*, 676 F.3d 854, 860 (9th Cir. 2012).

question because a prosecution cannot show that the defendant *knew* it violated the terms of use in part because that condition is ambiguous as applied to this conduct.

In addition, the mistake of law defense from *Rehaif*[360] and the trespass cases[361] should also afford defendants a powerful defense in cases such as *Citrin*, which are premised upon an employee's duty of loyalty.[362] In the vast majority of cases, prosecutors will struggle to establish guilt because they must show several related steps. Prosecutors must prove the defendant: (i) knew of some other law such as a state duty of loyalty law; (ii) knew this separate law applies to their conduct; (iii) knew their particular type of access violates that separate law (perhaps because of some complex interaction between that law and their employer's policy manual); and finally, (iv) knew that violating that separate law actually does revoke their authorization to access.

A. Van Buren v. United States

As a threshold matter, the question presented to the Supreme Court in *Van Buren v. United States* does not involve mens rea.[363] Rather, it involves a separate question that is harder to answer: Does a person who has authority, including a valid password, to access a work database violate the CFAA if he accesses that same information for an unsanctioned purpose?[364] Indeed, many of the prominent CFAA cases involve this question—prosecutions of police officers,[365] government employees,[366] or corporate employees[367] who use a valid login to view information out of curiosity or for some

360. 139 S. Ct. 2191, 2198 (2019).

361. *See supra* Part IV.B.

362. 440 F.3d 418, 420 (7th Cir. 2006).

363. *See* Question Presented, Van Buren v. United States, No. 19-783 (U.S. Apr. 20, 2020) ("Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.").

364. *See id.*

365. *E.g.*, United States v. Valle, 807 F.3d 508, 512 (2d Cir. 2015).

366. *E.g.*, United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010) (involving a Social Security Administration employee); United States v. Czubinski, 106 F.3d 1069, 1071 (1st Cir. 1997) (involving an IRS employee).

367. *Nosal I*, 676 F.3d 854, 856 (9th Cir. 2012); United States v. John, 597 F.3d 263, 269 (5th Cir. 2010).

more nefarious purpose. That purpose question lies outside the scope of this Article.

Nevertheless, the *Van Buren* case also happens to show just how powerful a robust mens rea can be as a defense against aggressive applications of the CFAA. It shows how an appropriate use of mens rea will help to sideline many of these difficult purpose cases by affording a strong defense along a separate dimension.

Take *Van Buren*'s facts as an example. My framework would have required the prosecution to show that *knowingly* applies to whether Van Buren exceeded his authorization in trying to access the license plate information.[368] It would have required a jury instruction that the mens rea of *knowingly* applies to authorization. Perhaps most importantly, the trial court should have instructed the jury that it must find Van Buren consciously and subjectively understood that accessing the license plate database was not only "wrong" in some sense but also contrary to a specific prohibition that would have the effect of terminating his authorization to access the database.

But at trial, the judge provided the jury instructions that failed to meet this basic standard.[369] The judge told the jury only that it must find Van Buren intentionally accessed the computer and then exceeded his access.[370] Indeed, the actual instruction tended to imply that *no* mens rea applied to exceeding authorized access by separating that element off from the conduct.[371] In particular, the judge instructed that the jury must find "the defendant intentionally accessed a computer in a way or to an extent beyond the permission given."[372]

The jury instruction certainly never said, as it should have, that "intentionally," or any other mens rea, applied to the "exceeding" element.[373] The jury could well have concluded that Van Buren intentionally *accessed*, and then merely have found that the license plate information exceeded his rights. The jury may not have found that Van Buren truly *knew* that accessing the license plate

368. *See* United States v. Van Buren, 940 F.3d 1192, 1198 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (mem.).

369. Appellant's Appendix Volume III at 116, *Van Buren*, 940 F.3d 1192 (No. 18-12024).

370. *Id.*

371. *Id.*

372. *Id.*

373. *Id.*

information both exceeded his rights and rendered his access without authorization; or, more precisely, the jury may not have found Van Buren knew he was not "entitled" to obtain that information.

Similarly, the prosecution's opening and closing arguments focused primarily on whether the defendant exceeded his access rights in such a way as to leave aside any consideration of whether Van Buren knew this.[374] The defense similarly did not argue mens rea at trial, but rather it argued the purpose argument: that a wrongful purpose can never vitiate initial authorization.[375]

Putting aside this failure to provide the jury the proper standard, we can still survey the trial evidence supporting mens rea—without examining the trial record comprehensively. The evidence emphasized in closing and on appeal showed that Van Buren conceded his attempt to access the license plate information "was 'wrong.'"[376] The prosecution showed officers in general are told they cannot use the database for personal reasons,[377] and it may have shown such use is a crime under state law.[378] But it did not show, apparently, that Van Buren attended these trainings or knew gaining access for personal reasons terminated authorization as opposed to something short of that. Van Buren may have believed it was morally wrong to obtain the information but not have realized he was legally not entitled to obtain that information. The parties at trial did not focus on mens rea. Perhaps the evidence would have shown Van Buren's access exceeded authorization, but in the end, he was entitled to a jury instruction that required such a finding.

My insistence on such a literal application of true, subjective, and conscious knowledge may seem overly technical, but it is what Congress intended when it amended the CFAA to enhance its mens rea, as discussed thoroughly above.[379] Congress eliminated a version of knowledge that would have included "practically certain" and

374. *Id.* at 75; Appellant's Appendix Volume I at 65, *Van Buren*, 940 F.3d 1192 (11th Cir. 2019) (No. 18-12024).

375. Appellant's Appendix Volume I, *supra* note 374, at 73.

376. *Van Buren*, 940 F.3d at 1198.

377. *Id.* at 1208.

378. Brief United States in Opposition at 3, Van Buren v. United States, No. 19-783, (U.S. Mar. 10, 2020).

379. *See supra* Part III.C.

apparently ruled out "willful blindness" as well.[380] It would not be enough, therefore, even if Van Buren suspected but avoided consciously concluding that he lacked authorization for that purpose.

To use a trespass analogy from the physical world, imagine a host who invites a guest to a dinner party. The guest enters the home with permission. At dinner, the guest insults the host, uses profanity, humiliates him in front of his other friends, and hurts his feelings. This conduct is wrong and even contrary to the purposes and assumptions of the invitation. But the insults do not make the guest a trespasser; the insults do not *automatically* vitiate the permission to be there, and we certainly cannot conclude the guest *knows* he must leave. Indeed, the host might want him to leave and make a face that most reasonable people would understand says, "Leave." Even still, we likely cannot conclude that the guest knows he must leave. If the host says "Please leave," we can probably conclude the guest now knows he must leave. But the guest could still argue that he thinks the host is joking when he says, "Please leave," even if that understanding is unreasonable. Until the guest consciously understands that he must leave, the guest is not a trespasser because there is no mens rea of "knowingly."

Finally, consider the facts in *Rehaif* that closely parallel those in *Van Buren* and other CFAA cases. In *Rehaif*, the defendant was convicted of possessing a gun while being in the United States "unlawfully."[381] In fact, he was in the United States lawfully at first, so the question was really whether he overstayed his welcome—similar to exceeding authorized access to a computer.[382] As in *Van Buren*, the trial court in *Rehaif* did not tell the jury it must find Rehaif knew he was here unlawfully. Worse, the trial judge expressly told the jury it need not make this finding.[383] The Supreme Court held, as noted above, that the jury instruction was

380. *See supra* Part III.C.

381. Rehaif v. United States, 139 S. Ct. 2191, 2194 (2019).

382. True, the facts of the cases differ in one way. Rehaif exceeded his permission to be in the United States lawfully along the dimension of time; he stayed here too long. *Id.* at 2194-95. Van Buren exceeded his authorized use because of his purpose and not because he stayed on the computer too long. United States v. Van Buren, 940 F.3d 1192, 1208 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (mem.). But this difference does not matter for mens rea purposes because either way the question is whether the defendant *knew* his presence, or type of access, exceeded authorization.

383. *Rehaif*, 139 S. Ct. at 2194.

wrong and that the prosecution must prove Rehaif *knew* he was here unlawfully.[384] The Court remanded for the trial court to determine whether the error was harmless.

On remand, the trial court found the error was not harmless because it was not clear that Rehaif knew his right to be in the United States had terminated.[385] Again, note how parallel the facts are to *Van Buren*. Rehaif knew he flunked out and even told the FBI during his interrogation that he knew "he was 'out of status.'"[386] The school sent him an email that he would lose his immigration status if he failed to transfer to another school.[387] The prosecution also showed that the school provides initial training to foreign students at the beginning of the year on immigration status.[388]

Nevertheless, the trial court found a reasonable juror could have concluded that Rehaif did *not* know he was in the United States unlawfully because of other facts.[389] Rehaif had not attended that school training session for foreign students.[390] The school could not show he had read the email.[391] He otherwise acted openly in being in the United States, even applying for a hunting license.[392] Applied to the CFAA, *Rehaif* on remand shows just how powerful this mens rea defense can be and how hard for a prosecutor to show that a defendant truly knew her access was without authorization.

B. Jury Instructions

CFAA jury instructions nationwide appear similarly deficient in requiring that juries find, beyond a reasonable doubt, that a defendant truly knew her access was without authorization, or that it exceeded authorization—at least when we survey federal pattern jury instructions that apply either nationwide,[393] or in particular,

---

384. *Id.* at 2200.

385. United States v. Rehaif, No. 6:16-CR-3-ORL-28GJK, 2020 WL 1904068, at *5 (M.D. Fla. Apr. 17, 2020).

386. *Id.* at *2.

387. *Id.* at *1.

388. *See id.* at *1, *4.

389. *See id.* at *5.

390. *See id.* at *1.

391. *See id.*

392. *Id.* at *1, *5.

393. 2A KEVIN F. O'MALLEY, JAY E. GRENIG & WILLIAM C. LEE, FEDERAL JURY AND

federal circuit courts of appeal.[394] Several circuits have not created pattern jury instructions for the CFAA, but those that have generally suffer the same problem as the instructions in *Van Buren*.

These pattern jury instructions fail at several critical junctures. They fail to inform juries that the mens rea term in the statute, "intentionally," collapses into *knowingly*[395]—without doing so, a jury might reasonably conclude that it applies to the conduct of access only. They fail to instruct juries that *knowingly* applies to the attendant circumstance of "without authorization" or "exceeds authorization."[396] They fail to define *knowingly* as subjective, conscious understanding (ruling out "practically certain" or "willful blindness").[397] Finally, they fail to instruct juries on the quasi-mistake of law defense: that the defendant must have read and understood any terms of service, or any other law, and consciously concluded that those sources make his access unauthorized.[398]

A typical pattern instruction with nationwide application simply restates the statute, stating, for example, that the jury must find the "[d]efendant intentionally accessed a computer without authorization"[399]—an instruction followed by some individual circuits.[400] This instruction will confuse the jury. It may well apply "intentionally" to access only and apply no mens rea to the "without authorization" element. If it does apply some mens rea to "without authorization," which mens rea will it likely apply? Knowingly? Should have known?

The pattern jury instructions for the Eleventh Circuit are worse, especially for the element "exceeds authorized access." For this element, the Eleventh Circuit pattern jury instructions require a jury to find that "the defendant intentionally accessed a computer ... in a way or to an extent beyond the permission given."[401] It goes

---

PRACTICE INSTRUCTIONS § 42:06 (6th ed. 2020).

394. *E.g.*, PATTERN JURY INSTRUCTIONS (CRIM. CASES), O42.2, (ELEVENTH CIR. JUD. COMM. ON PATTERN JURY INSTRUCTIONS 2020) [hereinafter ELEVENTH CIR. JURY INSTRUCTIONS].

395. *See, e.g.*, *id.*

396. *See, e.g.*, *id.*

397. *See, e.g.*, *id.*

398. *See, e.g.*, *id.*

399. 2A O'MALLEY ET AL., *supra* note 393, § 42:06.

400. *E.g.*, PATTERN CRIM. JURY INSTRUCTIONS OF THE SEVENTH CIR., 369 (COMM. ON FED. CRIM. JURY INSTRUCTIONS OF THE SEVENTH CIR. 2012).

401. ELEVENTH CIR. JURY INSTRUCTIONS, *supra* note 394.

on to define this formula as applying to a person who uses "authorized access to get or change information that the person is not permitted to get or change."[402] These instructions suggest that the mens rea of "intentionally" applies to access only and that the jury need find no mens rea with respect to whether the defendant had permission to obtain that particular information. They certainly fail to make clear that a mens rea of *knowingly* applies and what that means.

These pattern jury instructions typically draw from binding appellate case law in that circuit, but those cases are typically spelling out the legally required elements and not proposing jury instructions that will be clear to ordinary jurors. That is, in stating the elements of the CFAA, an appellate court will typically assume the reader is a lawyer who understands that the term "intentionally" will apply to all later elements and that it will collapse into *knowingly* as applied to attendant circumstances. We cannot make these assumptions about juries, of course, and we must be careful to instruct that they must find that the defendant *knew* her access was without authorization.

C. Public Platforms

The foregoing discussion leverages a robust mens rea to rule out prosecuting many cases of ordinary individuals unaware of access restrictions or prohibitions, but sophisticated business entities or institutions may have studied terms of service and separate laws to conclude that certain access methods might well violate such terms. The recent *Sandvig v. Barr* case involved just such sophisticated individuals and institutions—academic researchers who sought to create fake accounts on large web platforms in violation of those platforms' terms of service.[403] For them, even a robust mens rea of *knowingly* might often be met.

---

402. *Id.*

403. Civil Action No. 16-1368 (JDB), 2020 WL 1494065, at *1 (D.D.C. Mar. 27, 2020), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020); Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. (forthcoming 2021), https://papers.ssrn.com/so13/papers.cfm?abstract_id=3665040 [https://perma.cc/SF74-VW59] (critiquing the power of platforms to exclude researchers).

But my proposal for *public platforms* would require more: personally communicated notice. Thus, even if a person knows that terms of service prohibit her access, she may still access until she receives a personal notice, such as a cease-and-desist letter from the platform banning her access. This requirement of personally communicated notice, if adopted by courts, would likely protect many researchers and institutions. These platforms might fear bad publicity by expressly banning researchers on racial or gender discrimination or other kinds of bias.

But when a platform *does* send a cease-and-desist letter, my proposal would enlarge culpability compared to the rule adopted by *hiQ Labs*. Under my proposed interpretation, *hiQ Labs* comes out the other way. When LinkedIn expressly told hiQ Labs to stay out,[404] any future access was without authorization. In response to the argument that LinkedIn cannot open its site to the public generally but can kick out some visitors, that simply contradicts how criminal trespass law works in the physical world.

Recent trespass cases such as *Blankenhorn*—cited by *hiQ Labs*—and *Alexis* show us that trespass law bestows great power upon property owners: the power to selectively exclude for any reason or no reason at all.[405] To take a common real-world example, Walmart stores regularly ban persons by serving them personalized written notice. This notice states that Walmart reserves the right to ban those who shoplift, destroy property, or "otherwise behave in a manner that is unacceptable to Walmart."[406]

The CFAA applied these (unfortunate) trespass principles to computers by using precisely the same language in the text as criminal trespass statutes do and by indicating it intended the CFAA to be analogized to criminal trespass laws. We can just barely justify personally communicated notice as arising, by analogy, from the trespass cases; we cannot justify, however, interpreting a trespass provision such that it *never* applies to public platforms.

---

404. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

405. *See* Blankenhorn v. City of Orange, 485 F.3d 463, 474 (9th Cir. 2007); Alexis v. McDonald's Rests. of Mass., 67 F.3d 341, 350 (1st Cir. 1995).

406. State v. Zimbelman, No. 111759, 2015 WL 4577693, at *1 (Kan. Ct. App. July 24, 2015).

This interpretation, the best interpretation of the statute, does confer too much power on platforms, making them "digital gatekeepers."[407] The answer, however, is not to ignore the plain meaning of the statute; the answer, rather, is to repeal it, as I discuss in the last Part of this Article.

VI. THE PROBLEM WITH A CODE-BASED REGIME

In this Part, I further show how treating the CFAA as a criminal statute undermines many of the reasons supporting a code-based regime. I have already shown how mens rea eliminates cases in which the defendant might not have notice of the terms of service. This mens rea makes the notice function of a code-based regime completely unnecessary. This Part furthers the argument by showing that the code-based test is actually *more* vague than the plain meaning of "without authorization."

This Part next takes another, more detailed look at the legislative history of the CFAA. It does so within the context of ordinary criminal law principles to show why those advocating the code-based regime, including the Ninth Circuit in *hiQ Labs*, have misread, or at least over-read, that legislative history.

A. A Code-Based Regime Is Vague

The code-based regime itself is vague and hard to apply and will, therefore, give less notice in many situations. This follows because the code-based test lacks any underlying principle with which to determine its scope in new situations.

Take, for example, the test in *hiQ Labs* and most recently elaborated by Kerr—bypassing a technological barrier that authenticates users.[408] The test sounds straightforward, but what about an example Kerr himself raises: a site, such as the *Washington Post* or the *New York Times*, that limits the number of free visits by use of

407. Kadri, *supra* note 403.

408. *See hiQ Labs, Inc.*, 485 F.3d at 1001-03; Kerr, *supra* note 11, at 1161.

cookies or blocking IP addresses.[409] Such sites want readers to sign up for subscriptions after the free limit.[410]

In response, a user might clear her cache of cookies, browse in "incognito mode," or use a VPN to disguise her IP address; all are simple expedients that may bypass those limits. But in doing so, she has breached a code-based barrier and, therefore, under the code-based test, should be guilty of unauthorized access under the CFAA.

But Kerr says this use of cookies or IP-blocking to limit access would *not* count as a technological barrier based on authentication under his test.[411] This is an odd conclusion and shows how vague his test is. After all, cookies and IP addresses *are* used in this scenario to authenticate a user via her browser and computer, and they are technological barriers used to prevent an unauthorized person from accessing the site after the limit has been reached. The site determines the person has met her limit by authenticating, through the use of cookies, that it *is* the same web browser and computer. Kerr finesses this problem by saying that this use of cookies or IP blocking erects a "speed bump" only and is not really a "barrier."[412] But according to what principle? Because it is easy to circumvent? Why should that matter?

By contrast, under my view, this cookie and IP blocking regime shows that the computer owner does not want the individual to continue to access the site; the access is without authorization. Indeed, the *New York Times* terms of service state that a person is prohibited from evading the technological limit on free visits.[413] Perhaps a person who clears her cache or browses incognito may not know her access is without authorization; if not, she cannot be guilty. But if she does know, the plain terms of the statute criminalize her conduct. Of course, I have argued above that public platforms should also be required to mail a personally communicated cease-and-desist letter. If a court accepted that protective gloss on the statute, she would likely not be guilty. In the vast majority of cases, websites such as the *New York Times* are unlikely to identify

409. Kerr, *supra* note 11, at 1167.

410. *Id.*

411. *Id.*

412. *Id.*

413. *Terms of Service*, N.Y. TIMES, https://help.nytimes.com/hc/en-us/articles/115014893428-Terms-of-service#4 [https://perma.cc/H8YR-E2ZB].

a person who has cleared her cache to access beyond the limit and send them a personal cease-and-desist letter.

Unlike Kerr's attempt to distinguish this type of situation as not really a code-based evasion, my proposal requiring personal communication does rest upon a principle. Personally communicated notice is precisely the manner in which many states handle the difficult question of criminal trespass to a public place,[414] and the CFAA was intended to follow such state law.[415] A personally communicated notice also furthers the goals of the elements actually in the text: it helps to establish mens rea, and it shows that the host website genuinely does not want the visitor to continue visiting—especially if we decide that this use of cookies to limit visits is ambiguous to the average visitor.[416]

Password sharing and stealing cases are also unclear under the code-based regime. Suppose a person steals a password in the physical world by reading it off a post-it note. She then uses the password to access the other person's computer account. The intruder has not circumvented a code-based barrier in the sense of hacking the password or otherwise circumventing *code* on the system. Instead, she has used the password precisely as intended. Her circumvention occurred in the physical world and was, therefore, not a *code-based* circumvention.

And yet, we certainly want to consider stealing and using a password as access without authorization. How do we know? The intrusion is without authorization not because the person breached a code-based barrier, but rather because she knew she was accessing without authorization. We can establish she knew because she stole a password.

Again, an analogy to the real world helps. If a person steals a key to a home and enters it, she has not broken in, but she *has* trespassed because her entry was without authorization. And she knows it was without authorization because she stole the key.

Even at its core, the *hiQ Labs* code-based test falls apart. It delineates between public and private areas and information based

414. *See supra* notes 305-13 and accompanying text.

415. *See supra* Part IV.A.

416. This last point *does* fall under "without authorization" but is rooted in the plain meaning of that term rather than the code-based effort.

upon a login,[417] but that dividing line—logging in—does not accord with ordinary intuitions about what is public on such platforms. After all, Facebook, LinkedIn, and many other sites require a login to access most information. But once a person has logged in, she has access to much of the public-facing information of hundreds of millions of other accounts that she did not have access to before she logged in. Yet even this next level of information surely counts as public. Any adult can get an account on Facebook, sign in, and see nearly a billion profiles. Rather, the line between private and public is more nuanced and likely comes, at least on Facebook, at the next level of intimacy, "friends of friends."

LinkedIn limits the number of profiles a person who is not logged in can visit to ten; a person logged in can visit all 690 million profiles.[418] As with Facebook, this next level of information is public by any ordinary meaning of that term. Indeed, it is precisely the information that the individual account holder will have denominated as "public."

And yet the holding in *hiQ Labs* would deem this information private merely because it is behind a login, even though anyone can get an account and log in.[419] The difference seems to turn on a technicality of the way large platforms work and not on any difference in culpability, privacy, or some sense that one method is more of a "hack" than the other. Indeed, in response to the rule in *hiQ Labs*, a platform can simply move information behind the login and transform its terms of service from ineffective suggestions to operative exclusions.

The wall of such a login is so easily surmounted that it is really more of a curb one must step up onto in order to enter a mall. This ease of access makes this test based on a password not only the wrong line for what counts as private but also, again, a vague test for where the line lies.

Finally, and perhaps most absurdly, almost everyone accesses the internet itself through an Internet Service Provider (ISP) that

417. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1001-03 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

418. *About LinkedIn*, *Statistics*, LINKEDIN: NEWSROOM, https://news.linkedin.com/about-us#1 [https://perma.cc/EQ3M-VDT8].

419. 938 F.3d at 1001-03.

requires a login and password. When I log into my ISP, as I must to get access, does this now mean the entire internet counts as the type of private information suddenly protected by the CFAA? If so, *hiQ Labs* gets us nowhere.

Now one might argue that the login and password to get into the internet does not count because that authentication is erected by the ISP and not the web platform that potentially complains about access. But nothing in *hiQ Labs* supports that distinction because *hiQ Labs* rests upon the nature of information—dividing public from private. Moreover, as noted above, *hiQ Labs* expressly acknowledges a mismatch between how we establish that information is private—a password regime—and how we might find that a person accesses without authorization.[420]

Finally, and perhaps most fatally, at least Kerr's elaboration of the new, refined test still retains a vague catch-all provision. That is, in addition to breaches of authentication gates, Kerr's test reserves a category of other methods of breaching technological barriers that will count as being without authorization.[421] This category involves exploits that "otherwise 'break in.'"[422]

What it means to "otherwise break in" is itself hopelessly vague. He concedes it must be determined on a very fact-intensive inquiry, comparing the technology breached with the norms of the internet. For example, he argues an SQL-injection attack counts as a breach, but the hack in *United States v. Auernheimer*—which also involved entering code into a web browser—does not.[423] He concedes that "[t]he lines here are subtle, to be clear."[424] The two cases strike me

420. *Id.*

421. Kerr, *supra* note 11, at 1172.

422. *Id.*

423. In an SQL-injection attack, a hacker enters valid information into a search form on a website but adds particular characters at the end of her query. *See SQL Injection*, PORTSWIGGER, https://portswigger.net/web-security/sql-injection [https://perma.cc/FA7K-YR3Q]. The web platform server interprets these extra characters as separate code rather than part of the query. *See id.* It executes the code, giving the hacker additional access. In *United States v. Auernheimer*, the defendants entered a URL into their browser, but added a number at the end that acted as an identifier for another's account, allowing the defendants to access a portion of that account. 748 F.3d 525, 530-31 (3d Cir. 2014). The defendants wrote a computer program to repeat this process 114,000 times, gaining the email addresses of 114,000 account holders. *Id.* at 531. Kerr argues these two cases differ. *See* Kerr, *supra* note 11, at 1172-73. The first would violate the CFAA; the second would not, in his view. *See id.*

424. Kerr, *supra* note 11, at 1173.

as indistinguishable by any principle that would give fair notice, however, illustrating a test too vague for criminal law purposes.

What we can see here is that the code-based test and its elaborations do not work because they attempt to erect proxies for what the statute actually forbids: intentionally accessing without authorization.[425] Breaching a code-based barrier may *sometimes* establish that a person knew her access was without authorization and sometimes not. But it fails as a substitute for the actual test. Prosecutors, courts, and juries need to look at all the circumstances to determine whether the person knew her access was without authorization.

B. The Hacker Paradigm Amended Away

Many courts,[426] including the *hiQ Labs* court,[427] also argue that the CFAA primarily targets hackers. Congress sought to address a particular paradigm described expressly in the legislative history: a youth at home with his or her PC dialing into a government or bank computer and hacking in by guessing the password through a brute force attack.[428] As a result, the CFAA applies, they argue, only to areas or information protected by a password, and we should, therefore, use a code-based regime to interpret "without authorization."[429]

This hacker-paradigm argument has superficial appeal. After all, the CFAA originally applied only to government, bank, and credit agency computers that would likely have been protected by login credentials and contained particularly private information, such as

---

425. *See* Thaw, *supra* note 188, at 943.

426. *See Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012) (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005)).

427. 938 F.3d 985, 1000 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

428. *E.g.*, H.R. REP. NO. 98-894, at 10 (1984) ("Compounding this is the advent of the activities of so-called 'hackers,' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results.").

429. *E.g.*, *hiQ Labs*, 938 F.3d at 1001.

classified or financial information.[430] The legislative history points to this paradigm. The congressional reports,[431] as well as floor speeches,[432] frame the problem as one of hackers "breaking into" computers by breaching passwords. This paradigm also supplied the cultural background and accessible touchstone for many government officials, including President Reagan.[433]

But we must temper this argument with two observations. First, this paradigm may have motivated the CFAA, but the text Congress chose does not limit its ambit to this application. The term "without authorization" is not ambiguous such that we would even look at the legislative history to limit it to a particular type of access.

Second, and more importantly, Congress later broadened the statute beyond this initial paradigm. The original law applied to government, bank, and credit agency computers and information only.[434] But as detailed above,[435] a series of later amendments, taken together, expanded both the type of computers and type of information. Under those amendments, the CFAA applies to *any* computer, at least if it is connected to the internet, and to any information whatsoever. The original paradigm of a hacker cracking a password rested upon those original computers protected—government and bank computers—that generally *did* have password protection. It also rested on particularly sensitive types of information that would also have been protected by password access. It is from that original law that the court in *hiQ Labs* was able to say that a password is what delineates public from private.[436] But when Congress expanded the CFAA to include any computer and any information, it expanded

---

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

431. *E.g.*, H.R. REP. NO. 98-894, at 10, 20.

432. *E.g.*, 130 CONG. REC. 20,642 (1984) (statement of Rep. Hughes); *id.* at 20,644 (statement of Rep. Nelson).

433. STEPHANIE RICKER SCHULTE, CACHED: DECODING THE INTERNET IN GLOBAL POPULAR CULTURE 26, 47 (2013) (describing how a partial motivation for the CFAA came after President Reagan watched the movie *War Games* about a young hacker who accidentally breaks into a military computer, causing chaos and nearly starting World War III).

434. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, § 2102(a), 98 Stat. at 2190-91.

435. *See supra* notes 44-48 and accompanying text.

436. 938 F.3d 985, 1001 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

the scope of the statute to computers and information that are often not protected by passwords or other code-based protections.

One might argue that even with the expansion to any computer and any information, we should read a limit into the CFAA that covers only those computers and information that are protected by passwords because the original computers and information would have been so protected. But why? We do not import any other aspect of those previous limits. The statutory text notwithstanding, we do not say that the CFAA protects only information analogous to classified government or sensitive bank information. Instead, we really mean *any* information.

An analogy to criminal trespass helps here. Burglary originally applied to dwellings only, but in the twentieth century, states expanded the locus to any building or structure.[437] Similarly, modern trespass law applies to any building or structure and even to any place, such as a mall or park.[438] We would never say a trespass statute that expanded beyond homes to include stores does not really include stores because originally the statute only applied to homes.

Finally, Kerr has argued that the CFAA protects only private information or areas delimited by a code-based barrier because of the norms of the internet rather than legislative history.[439] His argument also cannot withstand the dictates of trespass law. In the physical world, malls, parks, and stores are presumptively open to the public, but criminal trespass laws still apply to those public areas.[440] A person ordered to leave must do so.[441] The presumption of license has been revoked for that individual.[442]

VII. CRIMINAL TRESPASS: A POOR MODEL

The bulk of this Article takes the CFAA as it is and proposes the best interpretation based upon ordinary interpretative tools. This proposed interpretation happens to address many of the unjust

437. LAFAVE, *supra* note 22, § 21.1(c).
438. *Id.* § 21.2(b).
439. Kerr, *supra* note 11, at 1161, 1171.
440. *See* LAFAVE, *supra* note 22, § 21.2(b).
441. *Id.* § 21.2(a).
442. *See id.*

applications that courts and scholars have identified. But even my interpretation leaves many potential unjust applications that cannot be interpreted out of the ambit of the statute according to any ordinary principle.

This problem leads to a more radical proposal, in tension with the foregoing, but nevertheless important: we should abolish the trespass provision of the CFAA. Others have argued for major amendments to the provision,[443] or to abolish it,[444] and I will not repeat those strong arguments here. Instead, I will add only one particular argument that we can draw from a survey of the state criminal trespass laws.

To be clear, I do not argue that we should abolish the entirety of the CFAA. Quite the contrary, we can safely abolish the simple trespass provision, section (a)(2)(C), precisely because other provisions of the CFAA readily address trespasses accompanied by true harms, such as unauthorized access to steal money, financial information, health information, or classified information.[445] Similarly, section (a)(5) prohibits causing damage to the target computer, such as deleting information or making it crash.[446] Even with respect to simple trespass to a computer to view information, to the extent we want to afford protection to information such as medical records or nude photos, we can craft carefully tailored laws to address those particular types of privacy invasion—but likely as part of a privacy law rather than a computer-specific law.

This Part very briefly sketches what we can learn from ordinary trespass cases in particular to support abolishing the trespass provision of the CFAA. I present criminal trespass at its worst to illustrate its pathology. Its abuse by states for segregation[447] or massive urban social control[448] may seem far afield from accessing

---

443. *See, e.g.*, Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013); Kadri, *supra* note 403 (arguing Congress should exempt public platforms from protection under the CFAA).

444. *See, e.g.*, Matwyshyn & Pell, *supra* note 89, at 511-12, 514; Simmons, *supra* note 273, at 1712-14 (arguing the CFAA is overbroad, is vague, and fails to grade according to culpability, whereas agency regulations would better adapt to changing technology with better definitions).

445. 18 U.S.C. § 1030(a)(1), (a)(2)(A), (a)(4).

446. *Id.* § 1030(a)(5).

447. *See, e.g.*, City of Greenville v. Peterson, 122 S.E.2d 826, 828 (S.C. 1961), *rev'd*, 373 U.S. 244 (1963).

448. *See, e.g.*, Ligon v. City of New York, 925 F. Supp. 2d 478, 518, 544-45 (S.D.N.Y. 2013).

a computer, scraping data, and violating terms of service. In some ways, it is. Nonetheless, the worst of the criminal trespass cases and the problem with criminalizing mere computer trespass share one similarity: they basically criminalize mere presence without a showing of some other harm, such as theft, fraud, or damage.[449]

During the Jim Crow era, one of the methods states and local businesses used to enforce segregation, and particularly to exclude protestors, was criminal trespass.[450] In case after case, stores,[451] playgrounds,[452] and other areas kicked out Black people or their white allies, whether they were protesting or simply living, using trespass law. The supreme courts of these states regularly upheld the right of these property owners to enlist the police to forcibly remove these visitors or protestors.[453] The same courts affirmed the criminal trespass convictions.[454] A property owner had an unfettered right to exclude, even if based on race or speech.[455]

As the Supreme Court of North Carolina held: "[A]lthough the general public have an implied license to enter a retail store, the proprietor is at liberty to revoke this license at any time ... and to eject such individual ... if he refuses to leave when requested to do so."[456] The court made clear that property owners may exclude for any reason, including race, and that the involvement of the police and courts in the arrest does not amount to state action triggering the Equal Protection Clause.[457]

---

449. *See* Matwyshyn & Pell, *supra* note 89, at 511.

450. State v. Goldfinch, 132 So. 2d 860, 861 (La. 1961), *rev'd sub nom*. Lombard v. Louisiana, 373 U.S. 267 (1963); State v. Avent, 118 S.E.2d 47, 57 (N.C. 1961), *vacated*, 373 U.S. 375 (1963); *Peterson*, 122 S.E.2d at 828; Randolph v. Commonwealth, 119 S.E.2d 817 (Va. 1961), *vacated*, 374 U.S. 97 (1963); *see also* John Silard, *A Constitutional Forecast: Demise of the "State Action" Limit on the Equal Protection Guarantee*, 66 COLUM. L. REV. 855, 863 (1966); *The Supreme Court 1962 Term: Maintaining Racial Segregation Through State Criminal Trespass Prosecutions*, 77 HARV. L. REV. 127, 127 (1963).

451. Adickes v. S. H. Kress & Co., 398 U.S. 144, 170 (1970).

452. Wright v. State, 122 S.E.2d 737, 741 (Ga. 1961), *rev'd*, 373 U.S. 284 (1963) (affirming breach of the peace convictions of six defendants for playing basketball in park while Black).

453. *See supra* notes 450-52 and accompanying text.

454. *See supra* notes 450-52 and accompanying text.

455. *Peterson*, 122 S.E.2d at 828.

456. State v. Avent, 118 S.E.2d 47, 52 (N.C. 1961) (internal quotations omitted), *vacated*, 373 U.S. 375 (1963).

457. *Id.* at 52-54.

The United States Supreme Court often overruled these cases but did not question the underlying principle—that a property owner may exclude at will.[458] Indeed, oddly, the Supreme Court never clearly held that a racist business that enlists a police officer to remove someone, and enlists the state machinery to prosecute for trespass, has triggered sufficient state action.[459] It did not violate the Equal Protection Clause for the police to arrest, juries to convict, and courts to sentence a person for criminal trespass even if the underlying reason for exclusion was race. The Court always required some plus factor to show a nexus between the state government's segregation policy and the store policy, and it was only this plus factor that allowed it to vacate many of these convictions.[460]

It took the Civil Rights Act to simply supersede the state law of criminal trespass when based on race. The Court held that once it was unlawful for a business to exclude based on race, it was unlawful to criminally convict a Black person for refusing to leave.[461]

Today, the same rule applies for the Free Speech Clause. Courts have regularly held that the Constitution does not prohibit private property owners, even owners of property open to the public, from excluding for any reason, including reasons related to speech[462]—though California is a notable exception under its state constitution.[463] When those property owners enlist the assistance of the police to arrest and the courts to convict individuals accused of trespassing, this assistance does not amount to state action.[464] However arbitrary the reason for exclusion, once a person trespasses in defiance of that order, enforcement by the government of the trespass laws is deemed neutral.[465]

---

458. *See, e.g.*, Peterson v. City of Greenville, 373 U.S. 244 (1963).

459. *See* Silard, *supra* note 450, at 865-66.

460. Adickes v. S. H. Kress & Co., 398 U.S. 144, 170 (1970); *Peterson*, 373 U.S. at 248.

461. Hamm v. City of Rock Hill, 379 U.S. 306, 308 (1964).

462. Lloyd Corp., Ltd. v. Tanner, 407 U.S. 551, 588 (1972).

463. Robins v. Pruneyard Shopping Ctr., 592 P.2d 341, 346 (Cal. 1979), *aff'd*, 447 U.S. 74 (1980).

464. Cape Cod Nursing Home Council v. Rambling Rose Rest Home, 667 F.2d 238, 243 (1st Cir. 1981); Williams v. Nagel, 643 N.E.2d 816, 820 (Ill. 1994); City of Sunnyside v. Lopez, 751 P.2d 313, 319 (Wash. Ct. App. 1988); State v. Horn, 407 N.W.2d 854, 860 (Wis. 1987).

465. *See, e.g.*, *Lopez*, 751 P.2d at 319.

These cases show that part of the problem lies with trespass laws themselves. Facially neutral, they afford property owners not only a right to exclude selectively and at will, but also the right to engage the machinery of the state to enforce that arbitrary will. Historically, the reason for exclusion was not merely arbitrary but also pernicious and racist.

We can turn this same critique to the computer trespass provision of the CFAA. It likewise criminalizes violating the unilateral terms of the platform, however arbitrary or eccentric they may be. The government has essentially delegated to the platform the power to declare what is or is not criminal by means of their terms of service. The platforms have enlisted the criminal authorities to enforce their policies.

We can potentially draw two conclusions from the above. The first is that of many scholars. They argue the CFAA must be unconstitutionally vague because it affords the power to private platforms to unilaterally criminalize conduct via arbitrary terms of service.[466] But the trespass cases both immediately above and throughout this Article make clear that this argument fails. Ordinary trespass cases allow owners of property open to the public to do just that—even when their reasons are based on speech and, historically, on race.

The second conclusion we can draw is mine: these problems are a good reason to abolish the computer trespass provision. As a matter of policy, computer platforms ought not have the power to unilaterally determine what conditions of access will expose visitors to criminal sanctions. I have argued above that the only defensible interpretation of the CFAA does give them that power; the only remaining solution is, therefore, repeal.

Even today, criminal trespass law remains a tool of social control often leading to unjust enforcement and discrimination. In New York City, for example, the police operated a program called the Trespass Affidavit Program (TAP).[467] Private landlords for buildings serving poor and minority communities were encouraged to authorize police to enter and arrest anyone suspected of trespass—that is, of not being a resident or guest.[468] TAP was so widespread

466. *See* Kerr, *supra* note 38, at 1581-82.
467. Ligon v. City of New York, 925 F. Supp. 2d 478, 484 (S.D.N.Y. 2013).
468. *Id.* at 484-85.

nearly every private apartment building in some Bronx neighborhoods became enrolled.[469] The goal was to rid the building of drug trafficking and other crime. But too often, according to the court, police swept every floor and hallway, stopping or arresting people merely because they were close to one of the buildings, or had just entered or left it.[470]

A federal judge in *Ligon v. City of New York* enjoined the program; she found that this widespread practice violated the individuals' Fourth Amendment rights.[471] The police conducted stops without reasonable suspicion, and this violation was so widespread that the city was held responsible.[472]

Even for those not arrested, note that criminal trespass law became the mechanism for stopping, questioning, and frisking large numbers of poor and minority residents, guests, and others.[473] Note too that in many ways, criminal trespass itself does not result in harm. Rather, the law serves as a proxy to prevent other crimes that are harder to detect, such as burglary or drug dealing.[474] But as implemented, the police ended up using trespass to stop people innocent not only of trespass but certainly also of those more serious crimes.[475]

The *Ligon* litigation demonstrates that criminal trespass can be arbitrarily enforced on very large numbers of people engaged in innocent and routine daily behavior. Yet neither that court nor any other has held that criminal trespass laws are therefore themselves unconstitutional. Our answer here again lies not with finding trespass laws, or the CFAA, unconstitutional, but rather with repealing at least the online version of criminal trespass.

Now, admittedly, racial or other discrimination on platforms does not involve a direct prosecution of an individual under the CFAA in perfect analogy with the foregoing cases in the real world. But platforms can play host to discrimination.[476] Researchers who

469. *Id.*
470. *Id.* at 524.
471. *Id.* at 532.
472. *Id.*
473. *Id.* at 484-85.
474. *See* LAFAVE, *supra* note 22, § 21.2.
475. *See, e.g.*, *Ligon*, 925 F. Supp. 2d at 529.
476. Kadri, *supra* note 403 (citing research on the issue); Laurent Sacharoff, *Russia Gave*

uncover such discrimination in housing, employment, and other opportunities often must use scraping, fake accounts, and other methods that make their access to these platforms unauthorized under its plain meaning.[477] Some of this research apparently led the federal government to sue Facebook for housing discrimination in its ads.[478] These researchers sometimes fear criminal prosecution under the CFAA for computer trespass and desist in such important civil rights research, or at least curtail its scope.[479]

CONCLUSION

The dominant approach to the trespass provision of the Computer Fraud and Abuse Act seeks to limit its unjust sweep by focusing on the term "without authorization." The Ninth Circuit in *hiQ Labs* recently adopted the view that "without authorization" can never apply to a public platform when a user does not bypass a technological barrier that authenticates identity, such as a password login.[480] Nothing about the term "without authorization" supports this interpretation. Indeed, both scholars and courts have been seeking a solution in the wrong place, with the wrong methods.

This Article has shown how we must treat the CFAA as a *criminal* law. That means using ordinary criminal law interpretative techniques such as those announced in the Model Penal Code[481]—a source Congress expressly adverted to in its legislative reports on the CFAA. Those techniques include addressing each statutory element separately and, most importantly, determining and applying the appropriate mens rea for each.

Bots a Bad Name. Here's Why We Need Them More Than Ever, POLITICO (Aug. 14, 2018), https://www.politico.com/magazine/story/2018/08/14/russia-gave-bots-a-bad-name-heres-why-we-need-them-more-than-ever-219359 [https://perma.cc/B82L-ZL5F].

477. Sandvig v. Sessions, 315 F. Supp. 3d 1, 18-20 (D.D.C. 2018).

478. *See* Katie Benner, Glenn Thrush & Mike Isaac, *Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says*, N.Y. TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html [https://perma.cc/77H4-CDHZ] (noting that the Department of Housing and Urban Development brought the lawsuit after "nearly three years of scrutiny of Facebook's ad-targeting practices that started with a 2016 investigation by ProPublica").

479. *Sandvig*, 315 F. Supp. 3d at 18-20.

480. 938 F.3d 985, 1001-03 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020).

481. MODEL PENAL CODE § 2.02 (AM. L. INST. 1962).

When we focus on the statute's mens rea, we are able to eliminate many of the unjust cases under the CFAA. Its mens rea provides surprisingly powerful protection by requiring that defendants subjectively know their access is without authorization.

But we can go further. Congress fashioned the CFAA as a trespass provision. Its text parallels ordinary state criminal trespass laws, and its legislative history urged the analogy to trespass. This Article, therefore, draws inspiration from these trespass laws to propose a special rule for public platforms similar to that for public places such as malls or stores: the platform must provide to an individual personally communicated notice that their access rights are revoked before they can be held liable under the CFAA.

The final Part of this Article, a coda, took my argument in a different direction. Even the best interpretation of the CFAA leaves potentially unjust applications. This coda used ordinary trespass law to show why the only solution may be to simply repeal the computer trespass provision of the CFAA. Both ordinary and virtual trespass criminalize mere presence without further harm. Whether criminal trespass continues to serve a useful role in the real world, we should not import its serious flaws into the virtual one.