Authority and Authors and Codes

Michael J. Madison

University of Pittsburgh School of Law
3900 Forbes Avenue
Pittsburgh, Pennsylvania 15260-6900

www.law.pitt.edu
412.648.7855
E-mail: madison@pitt.edu

First published in 84 Geo. Wash. L. Rev. 1616 (2016)

Authority and Authors and Codes

*Michael J. Madison**

Abstract

Contests over the meaning and application of the federal Computer Fraud and Abuse Act ("CFAA") expose long-standing, complex questions about the sources and impacts of the concept of authority in law and culture. Accessing a computer network "without authorization" and by "exceeding authorized access" is forbidden by the CFAA. Courts are divided in their interpretation of this language in the statute. This Article first proposes to address the issue with an insight from social science research. Neither criminal nor civil liability under the CFAA should attach unless the alleged violator has transgressed some border or boundary that is rendered visible or "imageable" in the language of the research on which the argument draws. That claim leads to a second, broader point—emphasizing the potential "imageability" of computer networks, including the Internet, has implications that go beyond one statute because of what that emphasis may teach those who create and implement those networks and who shape the authority that relevant computer code exercises. "Authority" and "authorization" are social practices, continuing negotiations between those who produce them and those who acknowledge and recognize them. "Imageability" is a way of translating that observation into a normative claim in a specific statutory context. Recognizing the social dimensions of "authority" implicates both what kind of Internet society wants and what kind of Internet society will get.

Table of Contents

* Professor of Law and Faculty Director, Innovation Practice Institute, University of Pittsburgh School of Law, Pittsburgh, PA, USA. Email: michael.j.madison@gmail.com. ORCID: orcid.org/0000-0001-6503-754X. For my title, I am indebted to Judy Garland, the star of the film version of *The Wizard of Oz*. The reader is invited to supply the concluding "oh my!"

December 2016 Vol. 84 No. 6

INTRODUCTION

Hidden in plain sight amid contests over the meaning and application of the federal Computer Fraud and Abuse Act ("CFAA")[1] are long-standing, complex questions about authority in law and culture. Accessing a computer network "without authorization" and "exceeding authorized access" are forbidden by the CFAA.[2] Courts are divided in their interpretation of this statutory language.[3] Divining a better answer to the statutory interpretation question involves some exploration of social science, eventually to find that the answer was there all along, in traditional, even conventional, thinking about authority and law. "Authority" and "authorization" are social practices, continuing negotiations between those who produce them and those who acknowledge and recognize them. The authority of law, the authority of a particular law, and the concept of authority embedded in a particular law, such as the CFAA, depend to a significant degree on how those practices evolve and are recognized cognitively and culturally. Authority is not a manufactured thing, but it has a material existence all the same, in human belief and behavior.

That teaching comes from a number of sources, including linguistics and research about social life in cities and on the Internet, and it is bolstered by broader themes in jurisprudence and copyright law. And it has some specific payoffs. For the CFAA, it means that neither criminal nor civil liability should attach unless the alleged violator has transgressed some border or boundary that is rendered visible, or "imageable" in the language of the social science on which the argument draws.[4] Bigger and broader payoffs lie beyond the CFAA, amid debates about law generally and especially law in online contexts. Questions about authority and practice implicate more than details of

1 18 U.S.C. § 1030 (2012).

2 *Id.* § 1030(a).

3 *Compare* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (broadly interpreting the CFAA to mean that an employee exceeds authorization when accessing a computer or information on a computer for purposes adverse to his or her employer), *with* United States v. Nosal (*Nosal I*), 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc) (interpreting the terms "without authorization" and "exceeds authorized access" narrowly). A recent opinion from the Ninth Circuit makes the claim that the phrase "without authorization" is uncontroversial in its application while the phrase "exceeds authorized access" has divided courts. *See* United States v. Nosal, Inc. (*Nosal II*), 828 F.3d 865, 873 (9th Cir. 2016).

4 *See* 18 U.S.C. § 1030(a) (making criminal or civil liability contingent on whether someone lacks or exceeds authorization, thus crossing the border or boundary made visible by authorization to access information).

statutory interpretation or construction and more than rules that define lawful or unlawful behavior. Understanding authority in law and practice implicates normative questions about the design and shape of our environment. In the context of this Article, that means: what kind of Internet do we want, and what kind of Internet will we get?[5]

"Authority," which is conventionally understood to represent the power of one institution or individual to command obedience from another by virtue of the former's status,[6] and "authorship," which is the conceptual foundation of contemporary copyright law, share a terminological affinity.[7] But there is more: both concepts are deployed as instruments of governance. In property law, generally, each is tied closely to governance of resources or "things," taking things as the proper starting point for understanding property rights and relationships.[8] "Authorship" is a copyright term of art that plays a central role in the governance of creative and expressive things called copyright "works."[9] "Authority" is used in a variety of legal settings, some but not all of them conventionally characterized as "property," to describe the power to compel recognition of and obedience to rules regarding control of access to and use of things.[10]

Authority also shares a conceptual affinity with the idea of "code" in at least two senses. "Code" is often shorthand for law itself, particularly statutory law. In computer science, "code" is a catchall term for the technological product of people who write computer programs, which run computers, computer networks, and related machines.[11] "Code" was once known generically as software or computer

---

5 Much of the CFAA-related argument in this Article draws on Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. Rev. 433 (2003).

6 *See infra* notes 104–09 and accompanying text.

7 *See infra* notes 110–15 and accompanying text.

8 *See, e.g.*, Henry E. Smith, *Property as the Law of Things*, 125 Harv. L. Rev. 1691, 1693–94 (2012) (arguing that property law "starts by taking advantage of the fact that some connections among people, uses, and attributes of things are more important than others"). The thingness of things should not be taken for granted. Things may be the proper starting point for analyzing property claims, but the attributes and character of things can be and should be considered contestable. *See* Michael J. Madison, *Law as Design: Objects, Concepts, and Digital Things*, 56 Case W. Res. L. Rev. 381, 475–78 (2005) (advocating for the interrogation of thingness in law generally).

9 *See infra* notes 111–15 and accompanying text.

10 *See, e.g.*, 35 U.S.C. § 271(a) (2012) ("Except as otherwise provided in [the Patent Act], whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent.").

11 *See, e.g.*, Charles Petzold, Code: The Hidden Language of Computer Hardware and Software 1 (1999). Confusingly, within computer science, "to authorize" may mean

programs;[12] the emerging ubiquity of digital devices—the so-called "Internet of Things" being its most salient contemporary example—demonstrates that "code" is no longer just the province of computer programmers and computers themselves. Digital content that operates "things" is everywhere: in cars, refrigerators, entertainment streams, pets, and even within human bodies as part of implantable medical devices.[13]

The link between code's legal usage and its technological usage is this: many scholars, policymakers, and advocates argue that "code is law."[14] The general sense of the phrase has typically equated the regulatory power of law with the regulatory potential of technology. In a society where digital computer networks are commonplace, the code that operates the networks also governs both individual and social behavior in ways that are analogous to the ways in which traditional law governs behavior. One should question the nature of code's authority and legitimacy much as one should question the nature of the law's authority and legitimacy.

In short, authority, authors, and codes are intertwined, and they create and define the resources and institutions of which they are parts. They constitute the governance referred to above just as governance both expresses and shapes them. Relationships among culture, law, and authority are recursive, not linear. As a specific illustration of the point, this Article considers authority in the context of the CFAA, which structures governance of access to a particular type of resource or thing: computer networks, including the networks that form the Internet. The CFAA relies heavily on two related statutory phrases, "without authorization" and "exceed[s] authorized access,"[15] as predicates for imposing liability on computer hackers and/

---

that a computer program permits a user to undertake a specific action, and in a purely technical sense that action is possible or is not possible as a feature of the computer program itself. *See* James Grimmelmann, *Computer Crime Law Goes to the Casino*, CONCURRING OPINIONS (May 2, 2013), http://concurringopinions.com/archives/2013/05/computer-crime-law-goes-to-the-casino.html. James Grimmelmann points out that it makes no sense to import this meaning of "authority," or any other purely computer-based sense "authority" into the CFAA. *See id.*

12 John M. Conley & Robert M. Bryan, *A Unifying Theory for the Litigation of Computer Software Copyright Cases*, 63 N.C. L. REV. 563, 564 (1985).

13 *See* ELLEN P. GOODMAN, THE ASPEN INST., THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS 1, 20 (2015), http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf.

14 Lawrence Lessig coined the aphorism. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

15 18 U.S.C. § 1030(a) (2012).

or computer trespassers.[16] The meaning of those phrases has been the subject of debate in the courts[17] and in secondary literature.[18] Resolving that debate is linked closely to what sort of Internet society has and what sort of Internet society will get in the future. It is a legal question with a legal solution, but with essential governance implications. A very specific immediate debate about the application of the CFAA[19] exposes a very general, continuing debate about how law and culture shape the very thing that the law governs.

The intertwining of questions of authority, authors, and code highlights that the proposition that these governance questions and any possible answers—about the CFAA, or about the Internet generally—are inescapably normative as well as descriptive.[20] How is the Internet governed, and how should it be governed? These are not mere questions of Congressional intent, nor questions of the intent of owners of computer networks. And the normative questions are not limited to more or less traditional questions of "what sort of conduct does society wish to discipline, encourage, or recognize, and why?" but also extend to more provocative questions of resource design: what kind of Internet does society want?

Part I reviews the problem of authority in the context of the CFAA and offers a framework for solving it. Part II explains how the problem of authority in that statute both relates to and is illuminated by exploring authority, authorship, and code in legal and other contexts. That discussion leads to the final point: there is no true answer to any of these questions in detailed analysis of either statute or con-

---

16 *See* United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015) (citing S. REP. NO. 99-432, at 3 (1986); H.R. REP. NO. 98-894, at 10–11 (1984)) ("Congress enacted the CFAA in 1984 to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data."). The fact that both views appear in the same legislative history is not surprising. Nor is the fact that no one in Congress in the mid-1980s took the time to parse possible distinctions. It was easy to characterize both hackers and trespassers as thieves. In its recent opinion in *Nosal II*, the Ninth Circuit noted precisely that equivalence in its recitation of the CFAA's history and purposes. *Nosal II*, 828 F.3d at 874–75. See STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1st ed. 1984) for a notable discussion of the practices and semantics of hacking. Levy's rehabilitation of the positive Hacker Ethic was published in the same year that the CFAA was originally enacted, 1984, which is a coincidence of Orwellian dimensions.

17 *See infra* notes 38–39 and accompanying text.

18 *See infra* notes 45–50 and accompanying text.

19 *See infra* notes 38–39 and accompanying text.

20 *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345, 355 (1991); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3, 8 (2015); Frederick Schauer, Essay, *Authority and Authorities*, 94 VA. L. REV. 1931, 1934–40, 1956–57 (2008).

cept. Instead, what matters is the normative answer to the question: what sort of thing is the Internet going to be?

I. What to Do with the CFAA

"Authority," for present purposes, refers specifically to part of the governance rules for computer networks set out in the CFAA, which creates civil liability for and imposes criminal sanctions on people who access relevant computer networks "without authorization" or who "exceed[ ] authorized access" to relevant networks.[21]

The CFAA was enacted before the commercial development of the Internet to help secure government and related special-purpose computers from hackers.[22] As the reach of computer networks extended and the phenomenon of the Internet emerged, the statute now reaches many different kinds of unwanted intrusion into almost any computer connected to the Internet and arguably touches almost any kind of unwanted appropriation of information from those computers.[23] The CFAA was originally designed to keep "bad" information and "bad" people out of computer systems and applications by denying access to hackers, competitors, and even consumers except on terms set by the proprietor of the system.[24]

Two notes concerning this brief overview must be addressed before turning to the relevant statutory text and the interpretive questions that continue to challenge courts and litigants. First, the CFAA makes a series of assumptions about ownership of computer systems and the presumptive property-like claims that accompany that status. In the early 1980s, when the CFAA was being drafted and enacted, those assumptions had a reasonable empirical foundation. Computer systems came in boxes that consisted of hardware and software, those boxes had owners, and those owners had legal property rights.[25] The data or information that those boxes stored and processed were present technically, conceptually, and legally, but their presence and significance were relatively easy to understate, largely because computer

---

21 18 U.S.C. § 1030(a)(1) (2012).

22 H.R. Rep. No. 98-894, at 10–12 (1984); *see also* Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 Harv. J.L. & Tech. 233, 236 (2010).

23 *See* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. Crim. L. & Criminology 907, 909 (2013).

24 *See id.* at 913–14.

25 *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1577 (2010).

systems had so little storage relative to their processing power.[26] Computer networks as they are known in the twenty-first century were essentially unheard of at that time.[27] It was sensible, conceptually and linguistically, to speak of a computer system owned by *A*, and conclude that *A* owned everything about it.

In the early twenty-first century, simple assumptions about integrated computer systems and networks, and their owners, are more difficult to maintain. Hardware is regularly unbundled from software (code); the network depends on links established via shared and standardized protocols; information and data may fairly be characterized as the most important property-like resource in the relevant environment; and "ownership" of a computer system or network, and the corresponding power to exercise property-like claims over its contents, is far less certain.[28] *A* may own the hardware components; both *B* and *C* may own separate interests in the software (the copy of the code and the related copyright); *D* (or no one) may own the protocol; *E*, *F*, and *G* may own the stored data or information; and *H* and *I* may have an interest in the information for reasons related to privacy, security, financing, or by virtue of one's status as a consumer or user.[29] Both technologists and theorists speak of the "architecture" of computer networks.[30] Conceptually, the CFAA was enacted to regulate an architecture that has since been demolished and rebuilt—using brand new blueprints.

Second, even the casual language of that brief description hints at the tangle of conceptual and definitional problems that plague the statute. The CFAA relies on a conceptual framework for computer systems that imagines them having an "inside" and an "outside"; computer users do not have the power to go inside—to access the innards

---

26 For a compelling illustration of that moment in computer history, see TRACY KIDDER, THE SOUL OF A NEW MACHINE (1981), which tells the story of the development of the minicomputer marketed by Data General Corporation as the Eclipse MV/8000. That computer attempted to leapfrog the minicomputer market with new technology. It sold for more than $100,000 (in early 1980s dollars) and came with 512 KB of permanent memory. Tim Scannell, *DG Brings Out 32-Bit Mini More Powerful than 4341*, COMPUTERWORLD, May 5, 1980, at 6 ("A basic MV/8000 system with 512K bytes of memory, battery backup, tape drive[,] and 96M-byte disk costs $153,150 without software.").

27 *See generally History of the Internet - 1980s*, NEW MEDIA INST., http://www.newmedia.org/history-of-the-internet.html?page=3 (last visited Aug. 24, 2016); *Internet History 1962 to 1992*, COMPUT. HIST. MUSEUM, http://www.computerhistory.org/internethistory/1980s/ (last visited Aug. 3, 2016).

28 *See, e.g.*, Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63, 73–75 (2003).

29 *See id.*

30 *See id.* at 149.

of the system, in other words—unless they have appropriate authority or authorization. Inside and outside are metaphors, of course, and they hint at the deeper metaphorical framework by which the CFAA operates. More on metaphors follows a tour of the statute and its problems.[31]

A. The Problems of the CFAA

Against that background, there are several problems with the current statutory interpretation of the CFAA. The CFAA contemplates both criminal and civil liability; only some conduct that supports criminal liability also supports civil claims.[32] Though the CFAA contains several subsections setting out different elements that might be met to establish liability, every application of the statute involves a prosecutor or plaintiff proving that the defendant accessed the computer "without authorization or exceed[ed] authorized access."[33] The statute fails to define "access," "authorized access," or "authorization."[34] There is one relevant definition: "'[E]xceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[35] A moment's reflection reveals the unhelpfulness of that language: at most, the statute defines "exceeds," and nothing more.

Perhaps the lack of clarity was purposeful,[36] but in any event, over the past thirty years and in particular since the Internet became a commercially interesting and broadly used set of technologies, courts have created a disturbing lack of clarity regarding the basic meaning of the CFAA's text. The inside/outside framework, highlighted above,[37] suggests that the relevant computer system has a border or boundary that has been crossed in some illegitimate way. But what form must that breach take? In broadest terms, what does access mean? What does "authorization" mean? In narrower terms, do "access" and "authorization" have to relate to one another in a particular setting in some technological sense? In some conceptual sense? Most narrowly, must "access" and "authorization" relate specifically to the

---

31 *See infra* Section I.B.1.

32 *See generally* 18 U.S.C. § 1030 (2012).

33 *Id.* § 1030(a)(1).

34 *See id.* § 1030(e).

35 *Id.* § 1030(e)(6).

36 *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (holding that "authorization" is a word "of common usage, without any technical or ambiguous meaning").

37 *See supra* Part I.

computer user's relationship to the computer system in question or might they relate instead to the user's logical, legal, or conceptual relationship to the system's owner?

Courts today do not share a basic framework for answering these questions. The most salient conflict today arises at a level in between the broadest and narrowest sets of questions set out in the preceding paragraph: How should the CFAA treat a defendant who has authorized access to a computer system, perhaps as an employee of the company that owns the system, but who accesses the computer system for a purpose that is not within the scope of that authority? Is the employee's use of the computer system "authorized" for purposes of the CFAA? For example, *A*, an employee of a bank, has access to computerized customer records in order to investigate the creditworthiness of customers who ask to borrow from the bank. Using those records, *A* looks up the phone number and address of customer *B* because *A* wants to ask *B* for a date. Has *A* violated the CFAA?

Courts are split. The First, Fifth, Seventh, and Eleventh Circuits would likely answer "yes" to this simple hypothetical; a defendant "exceeds authorized access" or acts "without authorization" when the defendant accesses a computer system to which that defendant has authorized access in general, but for a purpose beyond the scope of the authorization.[38] The Second and Fourth Circuits have held that an "improper purpose" standard is not part of the definitions of "without authorization" or "exceeds authorized access"; if *A* is authorized to access the computer system, but does so in pursuit of an improper purpose, *A* is not liable under the CFAA.[39] The Ninth Circuit recently concluded that *A* acts "without authorization" if *A* accesses a computer system after having *A*'s access "revoked" explicitly by the sys-

---

38 *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that defendant exceeded his authorized access when he used a database to obtain personal information that was not in "furtherance of his duties"); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (holding that "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded"); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that because defendant's only authority to access the laptop was his agency relationship, he exceeded his authority to access the laptop after the agency relationship terminated); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001) ("[W]hatever authorization Explorica had to navigate around EF's site (even in a competitive vein), it exceeded that authorization by providing proprietary information and know-how to [a competitor].").

39 *See, e.g.*, United States v. Valle, 807 F.3d 508, 511–12 (2d Cir. 2015) (holding that an individual "'exceeds authorized access' only when he obtains or alters information that he does not have authorization to access for *any* purpose" (emphasis added)); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205 (4th Cir. 2012) (holding that CFAA does not mandate "liability for the improper *use* of information that is accessed with authorization").

tem owner, though "revocation" must take some form other than a general notice to all potential users, such as a Terms of Use policy, that indicates proper and improper purposes of the system.[40] And the Ninth Circuit observed that such post-revocation behavior by *A* might not constitute a CFAA violation under the statute's "exceeds authorized access" prong.[41]

The split and associated uncertainty have hardly gone unnoticed by commentators. In 2008, a Missouri woman was indicted under the CFAA for accessing information about another person using the MySpace social networking system in a way that was technologically enabled by the platform, but that violated its Terms of Service—to which the woman had allegedly agreed when she acquired an account.[42] The Electronic Frontier Foundation filed an amicus brief with the district court that argued that violating the terms of an online Terms of Service agreement should not constitute "exceeding authorized access" or acting "without authorization," because such an interpretation would cause the CFAA to be impermissibly and unconstitutionally vague.[43] Who reads Terms of Service on the Internet?[44]

Notable efforts by legal scholars to cabin the statute include works by Orin Kerr[45] and Patricia Bellia.[46] Their arguments collectively share a view of the CFAA inspired by the idea that the statute is meant to deter computer hackers. One might call this view the "security-based" view of authorization, and within this framework, technology-based controls and circumventing them play key roles in interpreting the CFAA. In a recent, widely read, and respected blog post, James Grimmelmann critiqued reliance on code-based restrictions as giving meaning to the statutory phrase "without authorization,"[47] and Kerr has updated his position by arguing that the phrase

40 *See* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1077–79 (9th Cir. 2016).

41 *See id.* at 1076–77.

42 United States v. Drew, 259 F.R.D. 449, 452–53 (C.D. Cal. 2009).

43 *See* Brief of *Amici Curiae* Electronic Frontier Foundation, et al., in Support of Defendant's Motion to Dismiss Indictment for Failure to State an Offense and for Vagueness at 26–34, *Drew*, 259 F.R.D. 449 (No. CR-08-0582-GW), https://www.eff.org/files/filenode/US_v_Drew/drew_amicus.pdf.

44 *See id.* at 28–31; *see also* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012).

45 *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1599–1600 (2003) (arguing that only evading code-based restrictions on system access should form the basis for CFAA claims).

46 *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2272 (2004) (sharing Kerr's view of code-based restrictions, but emphasizing the role of actual notice to computer users).

47 *See* Grimmelmann, *supra* note 11.

should be defined with regard to social norms of computer users.[48] In this Symposium issue, Josh Goldfoot and Aditya Bamzai argue that the CFAA should be treated as a property-like trespass statute, reviving and refining an idea articulated earlier by Peter Winn.[49] In his Symposium contribution, James Grimmelmann proposes evaluating authorization by construing the existence and scope of consent granted by the computer system owner.[50] These arguments share a collective view of the CFAA, inspired by the idea that the statute is meant to deter trespassers. One might call this view the property-based view of interpretation.

Neither the security-based view nor the property-based view of the CFAA fully appreciates the roles and perspectives of computer system users as they explore computer networks, and both perspectives do not look beyond the statutory setting of the CFAA to the broader normative implications of their analyses. The following sections elaborate on that brief critique and offer a different perspective.

B. A Solution

As a starting point, and focusing initially on the interpretative questions posed by the CFAA itself, I revive and refine a proposal that I initially offered in a scholarly article published in 2003,[51] when debates about the proper interpretation of the CFAA were relatively novel and when other related debates about access problems, hacking, and trespassing on the Internet were also raging. The law of clickwrap agreements, too, was far less settled than it has since become; the meaning of the anti-circumvention provisions of the then-new Digital Millennium Copyright Act[52] was being worked out; and commercial website proprietors were trying out theories of liability for allegedly

---

48 *See generally* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016) (discussing the use of trespass norms as "a framework to distinguish between authorized and unauthorized access to a computer").

49 *See generally* Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1396 (2007). Interestingly, although Goldfoot, Bamzai, and Winn write in their individual capacities, each has experience as a federal prosecutor.

50 *See generally* James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500 (2016).

51 *See* Madison, *supra* note 5, at 436–37 (arguing that courts should use an "Internet-as-place metaphor, particularly in light of how users actually experience places on the Internet," instead of abstract property-based principles in cases involving the CFAA and other legal doctrines governing "access" to Internet resources).

52 Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

illegitimate information acquisition, aimed at competitors, based on a novel interpretation of the common law doctrine of "trespass to chattels."[53]

In that 2003 article, I aimed to unify thinking about all four of these areas of law because each of them was directed at closely related if not identical conduct—transgressing some kind of border or boundary that governed access to and use of information. I proposed to shift the conversation from an uncoordinated debate about "who" (Who owns the computer system? Who is trying to get in, and is that person authorized or not?) to a largely unitary conversation about "what" (What sort of computer system are we talking about? What should law have to do with computer system design?). I synthesized legal standards for all four fields by adapting the social science concept of "imageability":[54] the proposition that a boundary or border would matter, legally speaking, only in proportion to its salience as a "keep out" signal to nonowners.[55] That communicative salience might be embodied in physical, code-based restrictions or in conceptual, text-based restrictions, or in social norms and custom-based restrictions.[56] In general, salience would signify understanding on the part of computer network or system users, rather than consent or authorization by owners.[57]

I believe that the proposal still properly rounds out incompleteness in both the security-based view and the property-based view of the CFAA, and offers appropriate refinements and amendments to the doctrinal arguments that each view supports. To state it plainly: the phrases "without authorization" and "exceeds authorized access" in the CFAA should be interpreted and applied so that a defendant is liable under the statute if that defendant acquired or used information available via the relevant computer system, but without acknowledging, recognizing, or obeying the instructions of an "imageable" boundary or border that is part of that system.

This is, to be clear, a *normative* claim about how computer systems and networks should be governed. It goes well beyond what

---

53 *See* Madison, *supra* note 5, at 446–47.

54 *See id.* at 487–91.

55 *See id.* at 472, 491.

56 *See id.* at 490–94.

57 How "imageability" would be proved in practice, and how legal and evidentiary standards might be worked out in the context of specific statutes and common law doctrines were the subjects of additional commentary in my earlier article. *See id.* I do not repeat them here. It is not only possible but even likely that in 2016 these steps would be worked out differently than how I proposed to work them out in 2003.

courts applying the CFAA have considered, either with respect to the meaning of "authorization" (which is often considered to be plain or self-evident)[58] or with respect to the meaning of "exceeds authorized access" (as to which congressional purpose is deemed to be relevant, if not necessarily dispositive)[59] and the collected wisdom of the other circuits that have divided over the question.[60] This argument depends largely on taking a key implicit feature of the CFAA, already highlighted above—that it structures the relationships between the owners and managers of computer systems as interests representing "the inside" and users and consumers of those systems as interests representing "the outside"[61]—and making it explicit. "Authorization" and "authority," the primary concepts from which authorization is derived, are not about the rights of the owner, but instead are about communication in practice among multiple parties, and understanding and acknowledgment by recipients of signals or messages offered by the sender.

The argument is divided into three parts. The first addresses the central role that metaphors concerning place and space play in discussions of the Internet and computer networks. The second deals with research, investigating how individuals experience place and space as part of their social lives. The third links that shared social understanding of place and space to the claim that a similar shared social understanding of metaphorical, Internet-related place and space should inform application of the CFAA.

1. Place, Space, and Metaphor

Policymakers, lawyers, courts, experts, lay commenters, and users alike refer to the Internet and computer networks as if they are physical places and have spatial characteristics. The legislative history of the CFAA is replete with references to place-like attributes of computer systems.[62] During the 1990s, commentators focused on phrases such as "the Information Superhighway" and the then-new term

---

58 Some courts apparently do, that the meaning of "authorization" is obvious as a matter of common knowledge, or that it can be discerned simply by looking up the word in a general-purpose dictionary. *See* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).

59 *See, e.g.*, United States v. Valle, 807 F.3d 508, 524–25 (2d Cir. 2015) ("If this sharp division [over the meaning of the phrase "exceeds authorized access"] means anything, it is that the statute is readily susceptible to different interpretations. We therefore turn to the legislative history and motivating policies for further guidance.").

60 *See supra* notes 38–39 and accompanying text.

61 *See supra* Part I.

62 *Valle*, 807 F.3d at 525–26 (reviewing the relevant legislative history of the CFAA).

"cyberspace";[63] a decade ago it was "the blogosphere" and now it is "the Twitterverse."[64] The Internet as "a series of tubes" emerged as a popular meme a decade ago following the introduction of that phrase by Senator Ted Stevens.[65] "A series of tubes" morphed quickly into slang terms for the Internet—"Intertubes" and "Interwebs."[66] Even more ordinary computer network vocabulary—"websites," "surfing the web," "email," and "text" (noun or verb)—evokes and mimics the technologies and landscape of physical space and place. The explosion in recent years of computer storage "in the cloud" adds an "up" versus "down" dimension to what has long been both an "inside" versus "outside" and "side by side" dimensional world.

All of this material embodies a complex of related metaphors, but in the late 1990s and early 2000s, many critical commentators resisted the metaphorical alignment of computer networks and physical place and space.[67] Computer networks were different, they argued, and quite unlike "ordinary" place and space.[68] Or, if they were not completely different, then they *should* be treated differently by law and public policy.[69] Metaphors mislead, they argued.[70] Metaphors are often little better than uninformed rhetoric, guiding arguments and behaviors in both descriptively and normatively inappropriate ways.[71]

Research in language and social science suggests that this critique is largely mistaken. Language and metaphor do not control thought and lived experience.[72] Instead, language and metaphor are cognitive properties that reflect thought and lived experience.[73] That claim is

---

63 *See, e.g.*, Mitchel L. Winick et al., *Attorney Advertising on the Internet: From Arizona to Texas—Regulating Speech on the Cyber-Frontier*, 27 TEX. TECH L. REV. 1487, 1544 (1996).

64 *See* Alex Kozinski & Robert Johnson, *Of Cameras and Courtrooms*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1107, 1124 (2010).

65 *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 621 (2011). Bambauer argues that the Internet really "*is* a series of tubes," in some relevant respects. *Id.*

66 *See, e.g.*, Wayne R. Barnes, *Social Media and the Rise in Consumer Bargaining Power*, 14 U. PA. J. BUS. L. 661, 683 (2012) (using the term "Intertubes"); Alan M. Trammell & Derek E. Baumbauer, *Personal Jurisdiction and the "Interwebs"*, 100 CORNELL L. REV. 1129, 1130 n.1 (2015) (identifying the meme "interwebs").

67 *See generally* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003). For important later work on the same theme, see generally Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007).

68 *See* Hunter, *supra* note 67, at 449–52; Lemley, *supra* note 67, at 523–26.

69 *See* Hunter, *supra* note 67, at 514; Lemley, *supra* note 67, at 522, 540.

70 *See* Hunter, *supra* note 67, at 459–62; Lemley, *supra* note 67, at 523.

71 *See* Hunter, *supra* note 67, at 459–62; Lemley, *supra* note 67, at 523.

72 *See* GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY 4 (2003).

73 *See id.* at 4–5.

associated with George Lakoff and Mark Johnson.[74] For the purposes of this Article, the work of anthropologist Edwin Hutchins, documenting how language and metaphor both facilitate and reflect the execution of complex operations by distributed teams of people, is highly relevant.[75] Like Lakoff and Johnson, Hutchins argued that language and metaphor are cognitive properties.[76] Going beyond their work, he argued that those cognitive properties are shared across a culture, rather than being limited to individuals, and therefore presumptively uncoordinated thought and action.[77] Metaphor is a collective phenomenon that reflects common experience.[78] Rather than one form (language or behavior) driving the other, the mental and material constitute conceptual blends of thought and action.[79] Following Hutchins, this Article argues that society's use of language and the collective interpreted experience reflect a common cognitive framework.

Legal scholars who reject metaphor on descriptive grounds are swimming against the tide of experience. Normative claims that metaphor should be ignored or resisted face a steep burden in the sense that it would be difficult to persuade millions of people that they are wrong to think about the Internet as a place. In some recent leading scholarship, reliance on precisely that sort of metaphor has quietly returned, though not necessarily in explicit terms. Orin Kerr's call for relying on norms of computer users in CFAA cases is premised in part on the idea that "[t]he protocols of the Web make websites akin to a public forum. To draw an analogy, websites are the cyber-equivalent of an open public square in the physical world. A person who connects a web server to the Internet agrees to let everyone access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale."[80] Recent CFAA opinions have embraced place-based metaphors. In *Facebook, Inc. v. Power Ventures, Inc.*, a Ninth Circuit panel supported its finding of CFAA liability with an elaborate story about an individual's permission (and the lack

74 *See, e.g.*, MARK JOHNSON, THE BODY IN THE MIND: THE BODILY BASIS OF MEANING, IMAGINATION, AND REASON xxxviii (1987); LAKOFF & JOHNSON, *supra* note 72; GEORGE LAKOFF & MARK TURNER, MORE THAN COOL REASON: A FIELD GUILD TO POETIC METAPHOR 2 (1989).

75 *See generally* EDWIN HUTCHINS, Cognition in the Wild (1995). *Cognition in the Wild* was based on the extensive ethnographic observation of the crew of a U.S. Navy ship. *Id.* at 1–6.

76 *See id.* at 6.

77 *See id.*

78 *See id.* at xiv.

79 *See id.* at xvii.

80 Kerr, *supra* note 48, at 1163.

thereof) to enter a bank and retrieve jewelry from a safe deposit box.[81] In its 2016 ruling in *United States v. Nosal* ("*Nosal II*"), a different panel of the same court distilled its affirming a CFAA conviction in the following: "once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door."[82]

The claim that metaphors of this sort are inescapable does not translate necessarily into a conclusion that they are wisely used. In *Facebook* and *Nosal II*, the court's metaphoric reasoning is simplistic, even clumsy. If websites are akin to public fora—and they may be, or may not be—then that is so not by declaration or assumption but instead by virtue of evidence of an extended amount of experience and practice. Next, therefore, this Article addresses how metaphor can and should be explored as part of legal reasoning in the context of computer networks.

2. Imageability in the City

If metaphor matters in computer networks, then the important issues are how it matters, and how it should matter. If Internet and computer networks users experience computer systems as places and spaces, then where does that sensibility come from, and what does that mean? What does it mean and what should it mean to experience something as a place or space? The descriptive claim about the meaning of the CFAA and the normative claim about its impact on computer networks and the Internet should be linked in some sensible way.

Long ago, researchers in urban planning learned that humans experience actual physical space as much in cognitive, metaphorical terms as they experience it in literal, more directly representational terms. In *The Image of the City*, the urban planner Kevin Lynch pioneered ideas of mental mapping and environmental psychology by studying how people take in and understand information about the urban environment.[83] Using Boston, Los Angeles, and Jersey City as case studies, Lynch's data showed that users understood their surroundings in consistent and predictable ways, though those ways dif-

---

81 *See* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1078 (9th Cir. 2016).

82 United States v. Nosal (*Nosal II*), 828 F.3d 865, 868–69 (9th Cir. 2016).

83 *See generally* KEVIN LYNCH, THE IMAGE OF THE CITY (1960).

fered from "objective" representations of those environments.[84] Mental maps were dominated by five things: paths, edges, districts, nodes, and landmarks.[85] Salience mattered more than precision.[86] "Imageability," as defined by Lynch, is "that quality in a physical object which gives it a high probability of evoking a strong image in any given observer."[87] An urban environment characterized by more and clearer salient features was more easily navigable and therefore was "imageable."[88]

Not surprisingly, basic property law aligns in many related respects with this idea of salience, including salience with respect to boundaries and boundedness, and particularly with Lynch's idea of social or shared salience as a feature of a material landscape that is mapped onto mental representations of that landscape.[89] But in both Lynch's recounting of the data and in properly nuanced understandings of property law, the shared mental or cognitive framing of the place has much to do with whether a person is properly in that place.[90] Even at common law, this is something more than notice that one's presence is welcome or unwelcome. Judge Posner's famous opinion on the tort of trespass in *Desnick v. American Broadcasting Cos.*[91] illustrates the proposition that the property owner's nominal consent or its absence does not determine liability for trespass to real property; the question instead is whether the defendant's conduct is inconsistent with the shared social understanding of the interests that the tort is designed to protect.[92] "Imageability" is likewise a shared cognitive attribute of a material environment.[93]

---

84 *Id.* at 14–15.

85 *Id.* at 46–48.

86 *See id.* at 46.

87 *Id.* at 9.

88 *Id.*

89 Salience is important in multiple ways to the history and practice of property law, particularly in property law theories that treat property forms as matters of social convention, *see* George H. Taylor & Michael J. Madison, *Metaphor, Objects, and Commodities*, 54 CLEV. ST. L. REV. 141, 157, 169–70 (2006), and in theories that dwell on "information costs" as determinants of the scope of property rights, *see* Smith, *Property as the Law of Things*, *supra* note 8, at 1691–98, 1716–25.

90 *See* LYNCH, *supra* note 83, at 4; Smith, *supra* note 8, at 1717–18.

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

92 *Id.* at 1352.

93 *See, e.g.*, HUTCHINS, *supra* note 75, at 129.

3. *From Social Life to Legal Life*

I conclude from these two steps that something quite similar should be done with the CFAA: interpretation and application of the statute should involve appropriating the metaphorical character of computer networks, already part of the statutory framework, giving accurate richness to the metaphor, and aligning that metaphor with the statute. A computer network or the Internet can be understood as more or less "imageable," that is, as having metaphorically clear or obscure paths, edges, districts, nodes, and landmarks.[94]

This Article claims that a shared cognitive and metaphorical salience concept—social cognition as applied to boundaries—could and should be applied usefully to interpretations of the phrases "without authorization" and "exceeds authorized access" in the CFAA.[95] Did an individual wrongfully cross a computer network-related boundary or border? The answer would depend on whether that boundary or border is "imageable," not merely whether that individual had notice or should be deemed to have had notice of a particular rule or technology granting or denying consent to enter.[96] The application of Lynch's work is far from seamless; one obvious possible complication is that a boundary or border might be "imageable," yet an individual's crossing that boundary might not be wrongful.[97] Social norms of computer network use might support such a conclusion, as Orin Kerr argues.[98] The metaphorical inference to be demonstrated, therefore, would be the proposition that "imageability" of the boundary at the shared level means "stop" at the individual level. In determining what exactly is understood to mean "stop," this Article now turns to normative connections among authority, authorship, and code.

II. Beyond the CFAA: Authority, Authorship, and Code in Conceptual Context

I argue a key and contestable point: the practice of place and space in shared social life should directly inform the meaning of "authority" and "authorization" in law and in the CFAA, even in the ab-

94 *See supra* notes 85–88 and accompanying text. Similar points have started to appear in other scholarship. *See, e.g.*, Simone Ferracina, Cyber-Imageability and the Incommensurable Future of Cities (Reyes Najera Cesar ed., 2013).

95 The original proposal also suggested applying equivalent standards to access controls expressed in law under the DMCA to clickwrap and browsewrap licenses and claims for trespass to chattels. *See* Madison, *supra* note 5, at 436–37.

96 *Id.* at 488.

97 *Id.* at 485–86.

98 *See generally* Kerr, *supra* note 48.

sence of a direct[99] statement by the legislature or the Supreme Court of the United States that this should be so. And in making that claim I have relied extensively on a small number of researchers from other fields.

This Article offers a somewhat naked normative point: a specific application of a broader argument about how the character of social life amid computer networks should both define legal regulation of that social life and that necessarily builds on itself. I acknowledge, but reject the contrary argument: social life amid computer networks might proceed in a purely frictionless and borderless manner,[100] or in a manner that dissociates borders and boundaries from the networks themselves, so that computer code and law operate in entirely independent spheres. That is not reality; borders and boundaries exist online as well as offline, and the two domains overlap in all sorts of ways. To advance the point yet one further step, code is law in some sense. How, exactly? The pragmatic questions are what kinds of borders and boundaries we want to recognize legally and socially, when and where, who should recognize them, and how? How should code and law be linked?

They are linked via the concept of authority, not simply as that concept is expressed in the CFAA, but also as that concept underlies broader questions of law and as the concept drives other legal domains, notably copyright. Code possesses authority of a sort; law possesses authority of a sort; authors in copyright possess authority of a sort. The linkage is not merely linguistic; it is functional. To state the point more precisely, authority casts a much longer normative shadow than any analysis of the CFAA suggests. Authority is both descriptively and normatively a matter of communication and understanding, not merely a matter of purpose and intent. What sort of authority and code we want depends on what sort of authority and code we get. The reverse is also true, in part: what sort of authority and code we get depends on what sort of authority and code we want. The three subsections of this Part explore the three pieces of this claim: the concept of authority, the concept of authors and authorship, and the concept of code. Together, they deliver the promise of the Introduction. If what is at issue is the character of law itself, then what is at issue, more concretely, is the character of the Internet.

---

99 Dare I say, "authoritative."

100 *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370–71 (1996).

A. Authority

Dialogue from the motion picture *Bull Durham*, featuring a young, hotheaded baseball pitcher (Ebby Calvin "Nuke" LaLoosh) and his older, wiser catcher and mentor (Crash Davis):

> *Crash Davis* (Crash): Why you shaking me off, huh?
> *Ebby Calvin "Nuke" LaLoosh* (Nuke): [*gets in Crash's face*] I wanna bring the heater to announce my presence with authority.
> *Crash*: To announce your what?
> *Nuke*: To announce my presence with authority.
> *Crash*: To announce your fucking presence with authority? This guy's a first ball fastball hitter.
> He's looking for heat.
> *Nuke*: Oh yeah? So what. He ain't seen my heat —
> *Crash*: [*Pauses*] Alright, Meat, give him your heat.
> [*Walks back towards the batter's box*]
> . . .
> *Crash*: [*to the batter*] Fastball.
> *[The batter hits a home run.]* . . .
> *Nuke*: [to Crash] Hah, that sucker teed off on it just like he knew I was gonna throw a fastball.
> *Crash*: He did know.
> *Nuke*: How?
> *Crash*: I told him.[101]

The fictional Nuke LaLoosh wanted to announce his presence "with authority" (a fastball, presumably difficult for the batter to hit), which was a great idea up to the point that the catcher made the game uncompetitive by telling the batter what pitch to expect. In tandem, the combination—what the pitcher throws and what the batter expects—defines the character of the game. The lesson is a generalized, popular culture version of this Article's claim relative to the CFAA and relative to the Internet more broadly. Authority is a matter of power (Nuke was trying to establish his power to determine the outcome of his confrontation with the batter), but it is likewise a question of shared understanding. Identifying and articulating that shared understanding reveals a critical outcome: the shape of "authority" has a direct impact on the character of the cultural environment in which that understanding is situated.

---

101 BULL DURHAM (MGM 1988). *Bull Durham* has been featured prominently in other scholarly debates about language and metaphor. *See, e.g.*, Steven L. Winter, Bull Durham *and the Uses of Theory*, 42 STAN. L. REV. 639 (1990).

To explore that point regarding authority in law itself, the legal philosopher Frederick Schauer offers perhaps the best place to begin. His recent summary of the state of modern thinking about authority in law and authority as law, *Authority and Authorities*,[102] is worth quoting at some length. Authority in law refers both to institutional and organizational arrangements (hierarchies of courts, relationships between courts and legislatures, and so on) and to the content of the law (the role of precedent, for example). It is constituted by collective practice and it exists in the continuing relationships of production and recognition among law's sources and its subjects. Authority, he writes, amounts to law itself:

> [L]aw is, at bottom, an authoritative practice, a practice in which there is far more reliance than in, say, mathematics or the natural sciences on the source rather than the content (or even the correctness) of ideas, arguments, and conclusions. . . . [T]he law's practice of using and announcing its authorities—its citation practice—is part and parcel of law's character. The various contemporary controversies about citation practice turn out, therefore, to be controversies about authority, and as a result they are controversies about the nature of law itself.[103]

That concept of authorities as practice nests within a broader concept of authority as practice:

> [T]he characteristic feature of authority is its content-independence. The force of an authoritative directive comes not from its content, but from its source. And this is in contrast to our normal decisionmaking and reasoning processes. Typically, the reason for an action, a decision, or a belief is one that is grounded in the content of the reason. I eat spinach because it is good for me, and it actually being good for me is a necessary condition for it being a good reason.[104]

The authority of law, for Schauer, is not like eating spinach. Conventionally, law's authority stems from its source rather than from its content.[105]

Deference to authority by virtue of the status of that institution (or person, or statement) can be problematic precisely because the idea of authority may chill reflection regarding normative arguments:

---

102 Schauer, *supra* note 20.

103 *Id.* at 1934–35 (footnote omitted).

104 *Id.* (footnote omitted).

105 *See generally* JOSEPH RAZ, THE AUTHORITY OF LAW: ESSAYS ON LAW AND MORALITY (1st ed. 1979) (characterizing law as an authoritative practice).

> It is highly controversial whether authority in this precise sense is a good idea and, if so, in what contexts. A longstanding body of thinking argues that it is irrational for an autonomous agent to do something she would not otherwise have done on the balance of substantive reasons just because a so-called authority says so.[106]
>
> [T]here can be little doubt that authority exists, apart from the question of its desirability. We understand what authority is, and we can identify instances of its effect, even as we disagree about its normative desirability and the extent of its empirical prevalence in real-world decisionmaking. And thus we understand that authority provides reasons for action by virtue of its status and not by virtue of the intrinsic or content-based soundness of the actions that the authority is urging.[107]

"For in reality, the status of a source as an authority is the product of an informal, evolving, and scalar process by which some sources become progressively more and more authoritative as they are increasingly used and accepted."[108] Schauer concludes:

> Although H.L.A. Hart made famous the idea of a rule of recognition, it is rare that formal rules determine what is to be recognized as law or as a legitimate citation in a legal brief, argument, or opinion. Rather, as Brian Simpson has insightfully described, the recognition and non-recognition of law and legal sources is better understood as a practice in the Wittgensteinian sense: a practice in which lawyers, judges, commentators, and other legal actors gradually and in diffuse fashion determine what will count as a legitimate source—and thus what will count as law.[109]

The relevant points come together in the following way. The argument here is not about citations; it is about the nature of authority in law, how legal authority derives from source, and how the authority of sources emerges from the shared practice of treating sources as authority. Absent acknowledgement of authority as part of that practice, authority is not law, as Schauer describes it: authority is merely power.

---

106 Schauer, *supra* note 20, at 1937.

107 *Id.* at 1939.

108 *Id.* at 1956–57.

109 *Id.* at 1957 (footnotes omitted).

B. Authors

Schauer would not claim that the foregoing answers all questions regarding the nature of authority. He recognized early on that authority is neither irreducibly complex nor simple and straightforward: "[T]he questions concerning authority are numerous, and we will get no closer to answering any of them if we assume that all of the important issues surrounding the concept of authority can be collapsed into one and only one question."[110]

Here, I turn to an area of law where the idea of authority has less to do with what is given and more to do with what is created: copyright. Authority, authorization, and authors are conceptually linked, which means that the law of computer networks and the law of copyright have something to teach each other.

Authors and authorship refer to one of the key preconditions for granting legal protection to newly created expressive works under the United States Copyright Act.[111] An author is one who creates and therefore owns initial legal rights to an "original work[ ] of authorship fixed in any tangible medium of expression,"[112] the magic gateway to copyright protection under United States law.[113] Under the Constitution, only authors are eligible for copyright protection.[114] The very idea of modern copyright, usually traced to early eighteenth century English law, assumes the counterpart idea of the author.[115]

Authority and authorship and related words (authorize, authorization, author, and their cousins authentic and authenticity) share an etymon in the classic Latin *auctor*, according to the Oxford English Dictionary ("OED"). Explaining the origins of "author," the OED reports the meaning of *auctor* as a

> person with authority to take action or make a decision, guarantor, surety, person who approves or authorizes, person who has weight or authority, spokesperson, representative, advocate, supporter, adviser, witness, expert, writer regarded as an authority, originator, source, mover or pro-

110 Frederick Schauer, Lecture, *The Questions of Authority*, 81 GEO. L.J. 95, 115 (1992).

111 17 U.S.C. §§ 101–810 (2012).

112 *Id.* § 102(a).

113 *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 355 (1991); Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 243 (1903).

114 Trade-Mark Cases, 100 U.S. 82, 93 (1879) (noting that the eighth clause of the eighth section of the Constitution confers on Congress the power to secure rights for authors and inventors only).

115 *See generally* The Statute of Anne, 8 Ann. c. 19 (1710) (framing copyright with reference to authors).

> poser, person or thing responsible, prime mover, initiator, cause, agent, creator, divine creator, builder, inventor, person who has written a book, founder, ancestor.[116]

This definitional exercise is not novel, and dictionary definitions take one only so far.[117] Author and authority do not mean the same thing.[118] The point of the etymology is to show how this shared linguistic history is manifested today both in statutory language and in the conceptual structures in which that language is embedded. Authorship and authority overlap in signifying creation, control, and responsibility.[119] An author is one who originates, who controls, and who is responsible for a thing, particularly a book, and for the authority of its text.[120] An authority is similarly one (person or thing) who is the source of and is accountable for reliable (authentic) information, evidence, or moral, political, or legal power over a person (or group) or thing.[121] An "authority" grants permission, gives orders, and makes or justifies decisions.[122]

Author and authorship, like authority itself, are legal concepts that borrow from social life, and in so doing they switch back and forth between individual agency and recognition of individual contributions, on the one hand, and acknowledgement of those contributions in broader social contexts, on the other. Author and authorship signify instruments and institutions. To be the source—of a text, of meaning, of power, or of permission—is also to express a community, communal, or collective understanding of what "source" and "permission" mean in that context.

Historical and contemporary debates about the meaning of authorship reflect these dual perspectives. Mario Biagioli, the historian of science, notes that during the twentieth century, historical notions

---

116 *Author*, OXFORD ENGLISH DICTIONARY (online ed. 2016).

117 *See* William McBride, *The Fetishism of Illegality and the Mystifications of "Authority" and "Legitimacy"*, 18 GA. L. REV. 863, 877 (1984) (outlining a similar observation regarding the common etymology of these terms); Mark J. Osiel, *Ever Again: Legal Remembrance of Administrative Massacre*, 144 U. PA. L. REV. 463, 470 (1995) (same).

118 *Compare Author*, OXFORD ENGLISH DICTIONARY (online ed. 2016) [hereinafter *Author*, OXFORD ENGLISH DICTIONARY], *with Authority*, OXFORD ENGLISH DICTIONARY (online ed. 2016) [hereinafter *Authority*, OXFORD ENGLISH DICTIONARY].

119 *See, e.g.*, Mario Biagioli, *The Instability of Authorship: Credit and Responsibility in Contemporary Biomedicine*, 12 FASEB J. 3, 3 (1998) (discussing the link between authorship and responsibility).

120 *See* Christopher Buccafusco, *A Theory of Copyright Authorship*, VA. L. REV. (forthcoming 2016) (manuscript at 10); *see also Author*, OXFORD ENGLISH DICTIONARY, *supra* note 118.

121 *See Authority*, OXFORD ENGLISH DICTIONARY, *supra* note 118.

122 *See id.*

of scientific "authorship" as signifying credit and responsibility for work product produced by a research collective or collaborative ran up against modern notions of authorship as signifying individual entitlement to the economic returns associated with exercising exclusive rights in a market economy.[123] Regarding the closely related concept of authenticity, the copyright and trademark scholar Laura Heymann has written that the distinction between "authentic" and "inauthentic" regarding an artwork or a luxury good may depend on nothing more than a statement of authorship—the name "Andy Warhol" affixed to a canvas produced by a member of Warhol's famous "Factory."[124] Heymann notes (and the market value of "Warhol" canvases confirms) that such statements have value only if they are accepted as valid by the relevant audience, "a determination that depends on shared notions of what authenticity means as well as a common understanding of what authenticity designates."[125] Even scholars who endorse an "intentionalist" view of authorship acknowledge that an author is a human being who intends a certain result in someone else—an audience, a reader, a listener, a viewer, and so on.[126] Authorship, like authority, is at bottom a shared social practice that combines the perspectives of those who create and those who read, listen, watch, and play.

C. Codes

This last subsection articulates the final piece of the linked framework among authorship, authors, and codes. So much attention has been paid above to the cognition and communication that defines authority and authorship in small and large contexts that it is possible to lose sight of the mechanics of how these processes form and operate. To close, this Article turns to that question, specifically to code, codes, and signals. The conceptual and practical intersections of authority and code in its multiple senses are important in their own right.

Signals and codes—collecting, documenting, promulgating, perpetuating, and sometimes enforcing signals—are ubiquitous in daily life and in law. Traffic signage, for example, is a set of signals and codes that blend law and social life in sometimes unnoticeable ways. Signals and codes can and sometimes do more than simply facilitate

123 *See* Biagioli, *supra* note 119, at 3–6.

124 *See* Laura A. Heymann, *Dialogues of Authenticity*, 58 STUD. L. POL. & SOC'Y 25, 35 (2015).

125 *Id.* at 25.

126 *See, e.g.*, Buccafusco, *supra* note 120 (manuscript at 26–27).

navigation in the city or on the highway. Barton Beebe described historical practices of fashion that signaled and structured status and professional relationships in great detail.[127] In a given time and place, those signals were often bundled into a legally enforceable code, known as a sumptuary code.[128] Modern intellectual property law, he argues, has much the same effect with respect to signals communicated by status goods in contemporary culture.[129]

In the urban planning context, "imageability" acquires part of its persuasive power from the strength and simplicity of the key bits of information that city dwellers identify in their environments.[130] Paths, edges, districts, nodes, and landmarks are signals of an important sort; they are prominent in mental maps precisely because of their power and clarity as information regarding one's location.[131]

"Imageability" acquires another part of its persuasive power because it is possible in some sense to compare and contrast the shared mental map of a place with its true shape. The mental map can be interrogated and analyzed; mental maps are persuasive, rather than authoritative, in the sense of the latter that Schauer described.

Putting these points together yields the conclusion that signal reliability, or the accuracy of code in the context of its authoritative status, is a design choice, which is to say, in the content of this Article's argument, a normative one. Good design choices take into account the shared and collective practices of those who rely on signals and codes. Clear and powerful signals may not be accurate ones; they may mislead. As the media scholar Judith Donath writes:

> "Receiver costs" are an important component in communication dynamics: If a reliable signal is very costly to assess, receivers may choose to rely on one that is less reliable but easier to obtain . . . . A key design goal is thus to enable signals that are reliable yet not costly to assess.[132]

Legal signals, like social signals, may be stronger or weaker, clearer or more complex. "Imageability" depends on signaling; signaling grows into codes; and codes may be authoritative (grounded in

---

127 Barton Beebe, *Intellectual Property Law and the Sumptuary Code*, 123 HARV. L. REV. 809, 821–23 (2010).

128 *Id.*

129 *Id.* at 831–36.

130 *See* LYNCH, *supra* note 83, at 2.

131 *Id.* at 46–48.

132 *See* Judith Donath, *Signals in Social Supernets*, 13 J. COMPUTER-MEDIATED COMM. 231, 238 (2008) (citing Tim Guilford & Marian Stamp Dawkins, *Receiver Psychology and the Evolution of Animal Signals*, 42 ANIMAL BEHAV. 1, 1–14 (1991)).

authorities) or merely persuasive. "Imageability" may be compelling or problematic; in itself, it does not answer important normative questions. One may take these conceptual points back down to the level of the pragmatic with respect to legal doctrine. "Without authorization" and "exceeds authorized authority" cannot be interpreted and applied within the CFAA without a normative framework to guide the interpreters. For CFAA purposes, "imageability" is a function of the signaling performed by computer networks and the conceptual as well as material codes that result.

Conclusion

What sort of thing is the Internet going to be? That is the question that the Introduction raised. And this Article has not answered it. But it is the question that underlies both the specifics of the statute known as the CFAA and the general spirit of challenging and understanding authority and law.

This Article argues that the phrases "without authorization" and "exceeds authorized access" in the CFAA should be applied by identifying and interpreting computer system borders and boundaries from the perspective of the shared or collective user experience.[133] Is the relevant border or boundary "imageable" or salient to the user?

This Article is offered in a conceptual-questioning spirit as well as a pragmatic one. We casually equate authorization and authority with law, and we casually equate law with technology or code. If law is authority and authority is law—and if code is both of those things—then law and code are what we are obliged to obey. If the sources and character of that authority are not sufficiently explicit, then their normative foundations are questionable. The concern is illustrated here by the CFAA, but the concern is far broader in scope. Frank Pasquale's recent writing carefully chronicles precisely this problem in the contemporary information services context.[134] From determinations of health insurance eligibility to financial creditworthiness, individuals are subject to the results of authoritative analysis by complex systems that they neither understand nor have any power or means to interrogate.[135] Pasquale argues critically that living in the resulting "black box society"—which in terms of this Article, means the collective legal and policy determinations regarding what counts as "authority" and "authorization"—is having a decidedly pernicious effect on mod-

133 *See supra* Section II.B.

134 *See* Pasquale, *supra* note 20.

135 *See id.* at 4–5.

ern life.[136] If *A* bypasses a password mechanism to access data held by a credit rating organization that is wrongfully preventing *A* from obtaining a loan, then *A* has in all probability acted "without authorization" in accessing that computer system.[137] But the authority of that system is, from Pasquale's point of view, normatively questionable.[138] Donath's work on signals points to the importance of design relative to signaling effectiveness.[139] Pasquale's work on computer systems points to the importance of legitimate authority relative to system design.

A better view is this: law generates and regenerates the material conditions of its own authority. The Introduction above, which speaks of governance and recursiveness, is precisely what governance entails: processes of individuals and institutions repeatedly making their lives and experiences, and in the process making codes, laws, and authority out of that practice. A well-established point bears repeating: we cannot obey what we cannot see or hear or read or touch, and we cannot decide to obey it without having the power to understand its meaning. Statutes such as the CFAA can reinforce the power to understand, if they are interpreted and applied in ways that support that outcome. Can we see the Internet, literally or metaphorically? Do we want to?

136 *See id.* at 10.

137 *See supra* note 35 and accompanying text.

138 *See* PASQUALE, *supra* note 20, at 16 (arguing that transactions, which are too complex for a layperson to understand, should not be allowed to exist).

139 *See* DONATH, *supra* note 132.