12-2016

Consenting to Computer Use

James Grimmelmann
Cornell Law School, james.grimmelmann@cornell.edu

Consenting to Computer Use

*James Grimmelmann**

ABSTRACT

The federal Computer Fraud and Abuse Act ("CFAA") makes it a crime to "access[] a computer without authorization or exceed[] authorized access." Courts and commentators have struggled to explain what types of conduct by a computer user are "without authorization." But this approach is backwards; authorization is not so much a question of what a computer user does, as it is a question of what a computer owner allows.

In other words, authorization under the CFAA is an issue of consent, not conduct; to understand authorization, we need to understand consent. Building on Peter Westen's taxonomy of consent, I argue that we should distinguish between the factual question of what uses a computer owner manifests her consent to and the legal question of what uses courts will deem her to have consented to. Doing so allows us to distinguish the different kinds of questions presented by different kinds of CFAA cases, and to give clearer and more precise answers to all of them. Some cases require careful fact-finding about what reasonable computer users in the defendant's position would have known about the owner's expressed intentions; other cases require frank policy judgments about which kinds of unwanted uses should be considered serious enough to trigger the CFAA.

TABLE OF CONTENTS

INTRODUCTION

The federal Computer Fraud and Abuse Act ("CFAA")[1] makes it a crime to "access[ ] a computer without authorization or exceed[ ]

---

* Professor of Law, University of Maryland. I presented earlier versions of this Article at the "Hacking into the Computer Fraud and Abuse Act: The CFAA at 30" Symposium and to a faculty workshop at the University of Maryland. Thanks to the participants, and to Aislinn Black, BJ Ard, Julie Cohen and the students in her Technology Law and Policy Colloquium, David Gray, Orin Kerr, Christopher Newman, Jonathan Mayer, Paul Ohm, Rebecca Tushnet, and Peter Winn.

1 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

authorized access."[2] This simple phrase has proven surprisingly controversial. Courts and commentators have sharply debated whether violating terms of service, sharing passwords, guessing URLs, changing one's IP address, or using information for a disloyal purpose can render access unauthorized.[3] These analyses have proceeded on the assumption that "authorization" either bears a determinate meaning or can be given one that will answer such questions.

This entire approach seems to me to be fundamentally misguided. The term "without authorization" as used in the CFAA does not refer to what a *computer user does*; it refers to what a *computer owner says* about those uses. The CFAA does not of its own force define a class of prohibited conduct, because literally any conduct in relation to a computer could be either authorized or unauthorized. It all depends on what the computer owner chooses to allow. Reformatting a computer's hard drive may be an unauthorized act of wanton vandalism when carried out by a prankster, but it is all in a day's authorized work for a company's IT contractor. Questions of the form, "Does the CFAA prohibit or allow *X*?" are posed at the wrong level of abstraction. The issue is not whether *X* is allowed, but whether *X* is allowed *by the computer's owner.*

---

2 *Id.* § 1030(a)(2). The various prongs of the CFAA also include jurisdictional, circumstantial, mental state, and result elements. *See id.* § 1030(a). But for reasons not here relevant, "authorization" has done most of the hard work of defining the CFAA's boundaries of criminality. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1628–40 (2003).

3 The literature is extensive. *See, e.g.*, Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2216–18, 2228–30 (2004) (IP addresses and terms of service); Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 24, 26 (2012) (passwords); Kerr, *Cybercrime's Scope*, *supra* note 2, at 1622–24 (authorization); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1178–79 (2016) [hereinafter Kerr, *Norms of Computer Trespass*] (password sharing); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1578–87 (2010) [hereinafter Kerr, *Vagueness Challenges*] (internet terms of service and disloyal purposes); Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453 (2016) (workplace computer use and commercial disputes); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 921–23, 929–30 (2013) (terms of service and passwords); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1432 (2007) (passwords); Mary W. S. Wong, *Cyber-trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience*, 15 INT'L J.L. & INFO. TECH. 90 (2007); 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, 240, 250 (2010) (terms of service and passwords); Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 755–61, 768–72 (2013) (terms of service and workplace computer use).

That is, authorization under the CFAA is a defense in the same way that consent is a defense to torts and crimes including trespass, battery, and rape.[4] To access a computer with "authorization" is to access it with the properly given consent of its owner.[5] To access a computer "without authorization" is to access it when the owner has not so consented. Everything turns on the "moral magic" of consent.[6]

This Article analyzes "authorization" under the CFAA using the conceptual building blocks of consent. The punch line is that "without authorization" does not refer to a fixed category of conduct, because legally sufficient consent has always been something that courts create rather than find. Part I sets the stage by describing what is distinctive about consent to use a computer, as opposed to consent to surgery, consent to sexual relations, consent to entry on land, or consent to any of the many things that people may do only with someone else's permission. Computer use is technically and temporally intermediated, so an owner cannot approve or reject proposed uses as they happen. Instead, she will typically need to give prospective consent, leaving it to users and courts to interpret the scope of that consent and to apply it to conduct the owner may not have anticipated.

With that background, the rest of the Article follows Peter Westen's careful taxonomy of the various meanings of "consent," with emphasis on the particular features that are often salient in CFAA cases.[7]

---

4 *See generally, e.g.*, 86 C.J.S. *Torts* § 38 (2016) ("A person who consents to another's conduct cannot bring a tort claim for the harm that follows from that conduct; no wrong is done to one who consents. The existence of consent means that the defendant did not commit a tort."); 6 AM. JUR. 2D *Assault and Battery* § 7 (2016) ("[I]f a victim consents to the touching, the touching is not unlawful and is not battery."). There are some crimes, such as murder, to which consent is not a defense. PETER WESTEN, THE LOGIC OF CONSENT: THE DIVERSITY AND DECEPTIVENESS OF CONSENT AS A DEFENSE TO CRIMINAL CONDUCT 111–19 (2004). Unauthorized computer use is not this sort of crime.

5 The owner might delegate this power to authorize to someone else, as when a cloud service provider hosts websites for its customers. The service provider owns the computer, but the website operators determine which website users are authorized. I will refer to "the owner" for simplicity. A party might also be "authorized" by law; this is a form of authorization that does not depend on consent. The CFAA itself states that it "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency." 18 U.S.C. § 1030(f). Here, "authorized" refers to the authority of the United States, not of the computer owner. Stewart Baker has argued that the owner of data stored on a computer is also empowered by the CFAA to determine the scope of "authorization," an argument that has been thoroughly and persuasively debunked by Orin Kerr. *See generally* Stewart Baker et al., *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ [https://perma.cc/322T-NN4Z] (collecting blog posts on the issue).

6 Heidi M. Hurd, *The Moral Magic of Consent*, 2 LEGAL THEORY 121 (1996); Larry Alexander, *The Moral Magic of Consent (II)*, 2 LEGAL THEORY 165 (1996).

7 WESTEN, *supra* note 4, at 111. For more on consent in law, see generally DERYCK

Westen's fundamental distinction is between *factual* consent and *legal* consent. Factual consent (discussed in Part II) is a state of the world; it exists when a person acquiesces in conduct by another that affects her. But legal consent (discussed in Part III) is a conclusion of law: it exists where the law decides to treat a person as acquiescing in another's conduct. Legal consent is defined in terms of factual consent, but factual consent is neither necessary nor sufficient for legal consent. Different types of CFAA cases raise different types of issues about the scope of consent, and we should take care to distinguish them. Part IV discusses some of the confusion that results when factual and legal consent are conflated.

I. COMPUTERS

I would like to start by considering what, if anything, sets consent-to-use-a-computer problems apart from other problems of consent in criminal and tort law. The answer, a little tautologically, is that consent to use a computer involves the use of computers. A user's conduct takes place within a space that is regulated, in the first instance, by software rather than by humans. Two characteristic features of software therefore come into play.

The first is *automation*: once created and made available, software can run on its own, without further human control.[8] This creates a distinctive sequencing in computer-use cases. Except in some trivially easy cases—like a burglar who first breaks into a home and then sits down at the homeowner's computer to check Facebook—the user always uses a computer program knowingly and voluntarily made available by the computer's owner.[9] In typical rape and robbery cases and a great many theft and trespass cases, the subject (and potential victim) is present and conscious. She can wait until an actor proposes a course of action to decide whether to grant or withhold consent and to take actions that thwart or enable his actions. But in most computer-misuse cases, the owner is absent: she provides the software and some indicia of consent and then waits for the user to

---

BEYLEVELD & ROGER BROWNSWORD, CONSENT IN THE LAW (2007); 3 JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW: HARM TO SELF (1986); ALAN WERTHEIMER, CONSENT TO SEXUAL RELATIONS (2003).

8 James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1723 (2005).

9 *See* Orin Kerr, *Norms of Computer Trespass*, *supra* note 3, at 1153–55 ("understanding the concept of authorization to computers ends up being surprisingly hard"). In CFAA terms, most interesting cases involve "exceeding authorized access" rather than "access without authorization."

act.[10] Often, the software itself will react to the user so quickly that there is no conceivable way that the owner can respond in time.[11] Even if the user's course of conduct extends over a significant (to a human) span of time, the owner may be monitoring the computer only virtually, and so may not know what the user is doing until afterwards. In all these cases, the owner's consent to computer use is necessarily prospective rather than contemporaneous.

Prospective consent is not unique to computer-misuse cases.[12] Patients who will be unconscious during surgery typically give prospective consent to being cut open with knives, to the risk that something will go wrong with the cutting, and to being cut further if something does.[13] And people regularly give prospective consent to what would otherwise be trespasses and conversions: "The key is under the mat" and "I hereby authorize direct withdrawal of my $9.99 monthly donation" are both forms of prospective consent.[14] Prospective consent to computer use has features characteristic of prospective consent by *absent* owners to uses of property in trespass and theft cases, and features characteristic of prospective consent by *incapacitated* surgical patients in battery cases.

The law has typically approached such cases with an eminently sensible pragmatism. Recognizing the subject's prospective consent facilitates autonomy by extending the range of voluntary transactions she can prospectively consent to. Zipcar, surgery, and roller coasters would be impossible without prospective consent. But the limits the subject specifies are also respected, to prevent others from taking advantage of her inability to respond.[15]

A nineteenth-century case illustrates both concerns. In *Mitchum v. State*,[16] a storekeeper left a box of matches on a countertop "to be used by the public in lighting their pipes and cigars in the room."[17] Mitchum took the whole box.[18] He was convicted of larceny, and rightly so.[19] The storekeeper's generosity would have been futile if

---

10 *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.

11 *See* Grimmelmann, *Regulation by Software*, *supra* note 8, at 1723, 1744.

12 WESTEN, *supra* note 4, at 248–54.

13 *Id.* at 249.

14 *See id.* at 251.

15 *See id.* at 253–54.

16 Mitchum v. State, 45 Ala. 29 (1871).

17 *Id.* at 30.

18 *Id.*

19 *Id.*

everyone who took a single match was guilty of larceny. It would have been equally fruitless if Mitchum was allowed to make off with the whole box. Only recognizing both the prospective consent and its limits makes it possible for storekeepers to leave unattended boxes of matches for their customers.

So far, so good, but a second distinctive feature of software complicates the story. "Software is *plastic*: Programmers can implement almost any system they can imagine and describe precisely."[20] This fact vastly increases the complexity of people's interactions with software. In particular, it means there will almost always be cases in which software behaves in a way its programmers neither expected nor intended.[21] Software is buggy, and automation plus bugginess makes software hackable.[22]

This is not entirely a new problem. A nineteenth-century English case, *Regina v. Hands*,[23] presents the issues in embryonic form. I cannot improve on Lord Coleridge's statement of the case and holding:

> In this case a person was indicted for committing a larceny from what is known as an "automatic box," which was so constructed that, if you put a penny into it and pushed a knob in accordance with the directions on the box, a cigarette was ejected on to a bracket and presented to the giver of the penny. Under these circumstances there is no doubt that the prisoners put in the box a piece of metal which was of no value, but which produced the same effect as the placing a penny in the box produced. A cigarette was ejected which the prisoners appropriated; and in a case of that class it appears to me there clearly was larceny. The means by which the cigarette was made to come out of the box were fraudulent, and the cigarette so made to come out was appropriated.[24]

In modern terms, Hands and his codefendants hacked a cigarette vending machine. The most sensible analysis is that there was never consent to the taking. The owner of the machine made his consent conditional on depositing a penny; no penny was deposited. The de-

---

20 Grimmelmann, *Regulation by Software*, *supra* note 8, at 1723.

21 *Id.* at 1723, 1741–42.

22 *Id.* at 1742–43 (discussing hackability, in which "if Program *X* regulates some activity, a hacker who succeeds in replacing Program *X* with Program *X'* of her own devising will have gained the same absolute control over that activity that the original programmer once enjoyed"); *see generally* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327 (2008) (contrasting rhetoric and reality of hacking).

23 Regina v. Hands [1887] 16 LRCCR 188 (Eng.).

24 *Id.* at 190.

fendants succeeded in taking a cigarette while leaving only a worthless slug; that they did so by exploiting a mistake in the cigarette box's logic rather than by punching a hole in the side is of no moment.[25] Modern computers differ from the vending machine in *Hands* only in the degree of their plasticity: they are far easier to program with far more complicated logic, which in turn makes it possible to find more complex and more catastrophic bugs.[26]

These observations suggest two general principles that should inform any theory of consent to use a computer—not just under the CFAA but in any context where unauthorized use of a computer is legally prohibited.[27] On the one hand, the law will need to respond to a distinctive risk of opportunism on the part of ill-intentioned computer users. They can observe in detail how the software works and then arrange their interactions with it for maximum benefit—quite possibly at the owner's expense.[28] Just as it is impractical for owners to perfectly secure their computers, it is impractical for them to perfectly specify *ex ante* the scope of consent to use them.[29] Courts applying the CFAA must make allowance for the difficulties facing computer owners. But on the other hand, computer owners who have second thoughts about a use someone has made of their computers—or who anticipate having second thoughts—will themselves be tempted to behave opportunistically either by arguing after the fact that they were deceived about some relevant fact or by setting out ahead of time a disingenuously broad statement of what constitutes unauthorized use.[30] This creates a risk of arbitrary enforcement, and courts interpreting the CFAA must also make sure that users are

---

25 *See id.* at 190–91. Indeed, a purely mechanical case like *Hands* shows the folly of trying to draw too sharp a line between software and hardware. The court's use of "fraudulent" also deserves a raised eyebrow; query who was deceived by the fraud. But the holding is sound: as in *Mitchum*, the result is necessary if vending machines are to be possible.

26 *See* Grimmelmann, *Regulation by Software*, *supra* note 8, at 1742.

27 There are many examples of non-CFAA contexts where unauthorized use of a computer is prohibited. *See, e.g.*, Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)(A) (2012) (digital rights management); Stored Communications Act, 18 U.S.C. § 2701(a)(1) (2012) (communications privacy); Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (trespass to chattels); Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004) (breach of contract). The details of legal consent under these various regimes will vary with their relevant policy concerns, but they share a common core of consent.

28 *Cf.* Henry E. Smith, *Equity as Second-Order Law: The Problem of Opportunism* 12–15 (Harvard Pub. Law, Working Paper No. 15-13, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2617413 (arguing that opportunists can take advantage of the inherent limitations of laws expressed as rules, and that standards-based equitable discretion responds to this risk).

29 *See id.* at 7–8.

30 *See id.* at 12–13.

clearly informed about which conduct the law will treat as "unauthorized." This tension—between the need to give clear *ex ante* notice of what is allowed and the need to respond *ex post* to unanticipated abuse—is not unique to computer-misuse law.[31] But the technical complexity of modern software makes both halves of the problem distinctively more difficult.

In short, interpreting consent to use a computer poses a problem of prospective consent. Courts need to ensure that computer users receive fair notice of the scope of allowable use, and that computer owners are protected against unforeseen misuses. This is a more challenging task online than off, because software systems are subtler and more complex than their offline analogs.

II. FACTUAL CONSENT

Now that we are clear on the nature of the problem, we can be clear on the nature of the relevant consent. Philosophers disagree on whether the fact of consent is subjective—a mental state of consenting—or objective—an expression of consenting.[32] For legal purposes, the answer is that it could be either: for example, some jurisdictions define consent for purposes of rape law in terms of a victim's subjective mental state of consent while others define it in terms of a victim's objective manifestations of consent.[33] Westen calls the first *attitudinal* consent and the latter *expressive* consent.[34] A subject S gives attitudinal (factual) consent to conduct x by an actor A when she adopts an attitude of acquiescence toward x;[35] she gives expressive (factual) consent when she represents that she has such an attitude.[36]

"Authorization" under the CFAA refers to expressive rather than attitudinal factual consent. To authorize is to invest with authority; this is an act, not an attitude.[37] It is implausible to say that a computer owner secretly "authorized" a use without telling anyone about it, not even the user. Conversely, a CFAA prosecution based on the owner's secret withdrawal of authorization would fail because the user did not "intentionally" or "knowingly" use the computer without authoriza-

---

31 *See id.* at 14–15.

32 *See* Peter Westen, *Some Common Confusions About Consent in Rape Cases*, 2 OHIO ST. J. CRIM. L. 333, 334–35 (2004).

33 *See* WESTEN, *supra* note 4, at 27.

34 *Id.*

35 *Id.*

36 *Id.* at 27, 67.

37 *See Authorize*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("to give legal authority" or "empower").

tion.[38] For this reason, I will refer simply to "factual" consent except when the distinction between attitudinal factual consent and expressive factual consent matters. Consider a simple example:

> *House Guest*: *A* is staying with *S*. She tells him, "I'm going to run some errands. Feel free to use my computer while I'm gone." *A* uses *S*'s computer to check his email.

Here, *A* is authorized because *S*'s statement to *A* constitutes explicit factual consent. Compare:

> *Starbucks*: *S* leaves her laptop computer open on a table at a Starbucks while she gets up to use the restroom. *A* goes over to the computer and starts browsing through *S*'s emails.

Here, by contrast, *A* acts without authorization because he uses *S*'s computer without her factual consent. *Starbucks* shows that the default is no authorization; unless a computer owner affirmatively expresses consent to use, there is none. But consent need not be given in so many words:

> *Weather Website*: *S* connects a computer to the Internet and creates a website that enables users to input a ZIP code and then tells them whether to bring an umbrella with them. *A* visits the site, inputs his ZIP code, and views the resulting advice.

Here, as in *Starbucks*, *S* has not explicitly stated that *A* does or does not have consent. But unlike in *Starbucks*, *A* does use *S*'s computer with her factual consent. The difference is that access takes place online, and *S* has done something—created a website apparently intended for public use—that manifests her factual consent.[39] Creating a website is a communicative act that would be understood by Internet users like *A* as implicitly inviting them to use the website.[40] A reasonable person in *A*'s position, knowing what *A* knows about websites, would believe that *S* acquiesced in his use of her website. Factual consent is not always this simple, but where it is simple, we should acknowledge it as such. A more interesting case is:

> *United States v. Morris*:[41] *S* connects a computer to the Internet and installs on it a program, SEND MAIL, that lets

---

38 *See* 18 U.S.C. § 1030(a)(2) ("intentionally"); *id.* § 1030(a)(4) ("knowingly").

39 *Cf.* WESTEN, *supra* note 4, at 76–87 (discussing nonverbal expressive consent and communicative conduct in the context of the rape law).

40 *Cf.* Christopher M. Newman, *"What Exactly Are You Implying?": The Elusive Nature of the Implied Copyright License*, 32 CARDOZO ARTS & ENT. L.J. 501, 518–21 (2014) (discussing implied factual consent in the context of copyright licenses).

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

> other computers deliver emails to it.[42] *A* writes a "worm" program that connects to *S*'s computer and transmits a sequence of commands that causes SEND MAIL to install and run a copy of the worm program on *S*'s computer.[43]

It is superficially temping to say of a case like *Morris* that *S*'s computer "consented" to *A*'s use by allowing him to install his worm program.[44] But this argument proves far too much. Any defendant could always claim that the computer "consented" to his use: indeed, the defendant in *Starbucks* could claim that the open laptop "consented."[45] The issue is not whether the computer consented but whether its owner did. That cannot be reduced to a purely technical question of what the computer actually does. What the computer enables a user to do is relevant to authorization only insofar as it informs the user about the owner's consent.[46] *A* had factual consent in *Weather Website* not because the website itself consented, but because the website was designed in a way that effectively communicated its designer's consent.

The better approach to *Morris*, then, is to ask directly whether *S* gave factual consent to the use *A* engaged in—using SEND MAIL to install his worm program. The answer is almost certainly "no." To be sure, *A* can argue that *S* connected a computer to the Internet that runs a program the world is free to use, and thereby implicitly expressed consent to use of that program. But for the same reason that *A* understood that he was permitted to use SEND MAIL to send mail, he understood that he was not permitted to use it to install a worm; the same interpretive conventions that communicate permission also communicate the limits of the scope of that permission. The guest in *House Guest* correctly interpreted the illocutionary force of *S*'s ex-

---

42 *See id.* at 505–06.

43 *See id.*

44 This is the type of argument memorably made by the defendant in the Australian case of *Kennison v. Daire*, (1986) 160 CLR 129 (Austl.). A bank customer who knew that an ATM would give him money even after he closed his account argued, unsuccessfully, that he had had not committed larceny because the ATM "consented" to his taking the money. *Id.* at 129–30.

45 *See* Grimmelmann, *Computer Crime Law Goes to the Casino*, *supra* note 10 ("In every interesting case, the defendant will have been able to make the program do something objectionable. If a program conveys authorization whenever it lets a user do something, there would be no such thing as 'exceeding authorized access.' Every use of a computer would be authorized.").

46 Of course, it is also relevant to the scope of "access" requiring authorization; a hacker who tries but fails to withdraw money from a victim's online banking account is guilty only of *attempting* to violate section (a)(4) of the CFAA, which prohibits "knowingly and with intent to defraud . . . obtain[ing] anything of value" by means of unauthorized access. *See* 18 U.S.C. § 1030(a)(4).

press acquiescence to mean that he could use her computer to check email but not drop it out a tenth-story window. Internet users similarly must interpret the illocutionary force of the implied acquiescence conveyed by making a program available. They are in the same situation as Mitchum, who understood that he was permitted to take one match but not the whole box, and Hands, who understood that he was permitted to take a cigarette by depositing a penny but not by depositing a slug.[47]

The Second Circuit almost got this point right in *Morris*. It upheld *A*'s conviction on the theory that he "did not use [SEND MAIL] in any way related to [its] intended function."[48] On this reasoning, *S*'s "intent" about the "function" of a program defines the limit of her acquiescence, and hence of her factual consent.[49] The problem is that "intent" connotes *S*'s subjective intent and thus suggests that *A*'s guilt turns on *S*'s attitudinal consent—her secret undisclosed goals in making SEND MAIL available. If, for example, she installed SEND MAIL with the privately held intent of transmitting only upbeat emails, *A* would, on this theory, act without authorization by sending a depressing email. The Second Circuit should instead have made the point in terms of expressive factual consent: e.g., that *A* "did not use [SEND MAIL] in any way related to *what a reasonable user would have understood as its* intended function." This intent, and thus the consent it signifies, is objective in the same way that a manifestation of assent to a contract is objective; it is what a hypothetical reasonable listener would understand the speaker to be intending to convey. Here, a hypothetical reasonable user would have understood that

---

47 *Cf.* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–63 (1st Cir. 2003) (rejecting "reasonable expectations" as test for authorization because a "website provider can easily spell out explicitly what is forbidden"). This is a channeling rule; it gives computer owners an unambiguous way to limit consent and encourages them to use it by denying CFAA protection unless they use it. *See generally* Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 801–03 (1941) (defining "channeling function" of formalities). Similar channeling rules are found all throughout the law of consent. *See, e.g.*, Stephen J. Schulhofer, *The Feminist Challenge in Criminal Law*, 143 U. PA. L. REV. 2151, 2181 (1995) ("But permission must be an affirmative indication of actual willingness. Silence and ambivalence are not permission."). They trade off the accuracy of fact-finding about consent in specific cases in order to encourage more general communicative practices that promote clearer understandings of when consent is present or absent. They function as "sticky default" and "information-forcing" rules. *See* Ian Ayres, *Regulating Opt-Out: An Economic Theory of Altering Rules*, 121 YALE L.J. 2032, 2035, 2045 (2012). Depending on whether the default is one of consent or nonconsent, they can encourage either the subject whose consent is at issue or the actor who requires consent to press for greater clarity.

48 *Morris*, 928 F.2d at 510.

49 *See id.*

SEND MAIL is for sending mail, not for installing worms. When *A* used SEND MAIL to install his worm, he failed to apply the appropriate interpretive canons of the relevant community of computer users.[50] He either misunderstood or ignored SEND MAIL's meaning.

I want to emphasize that factual consent is a function of both code and words; of how a computer is programmed and of its owner's expressions, such as oral instructions, terms of service, and employee handbooks.[51] Both are relevant sources of evidence about the owner's factual consent. First, consider a slight variation on *Morris*.[52] (The additional facts are *underlined.*)

> *Security Audit*: *S* connects a computer to the Internet and installs on it a program, SEND MAIL, that lets other computers deliver emails to it. *S* instructs *A* to conduct a security audit of the computer, including by attempting to install a "worm" program. *A* writes a "worm" program that connects to *S*'s computer and transmits a sequence of commands that causes SEND MAIL to install and run a copy of the worm program on *S*'s computer.

The only difference between *Morris* and *Security Audit* is *S*'s explicit instructions, but they make all the difference; *A* obviously acts with *S*'s factual consent. This shows that authorization is not a purely technical concept; it always potentially depends on the computer owner's words. Indeed, precisely because they convey meaning explicitly rather than implicitly like software, words will often provide the clearest indication of the uses to which the computer owner does and does not factually consent.[53] There is no reason to disregard such probative evidence.[54]

---

50 WESTEN, *supra* note 4, 71–75 (An actor's interpretive community consists of real or hypothetical observers "who know (i) everything that the actor himself knows regarding *S*'s words and conduct, (ii) all social conventions for expressing desires, preferences, and choices of which the actor himself is aware, and (iii) any further words or conduct on *S*'s part, as well as any further conventions for expressing desires, preferences, and choices, of which the actor would be aware if he paid appropriate or 'reasonable' attention to the interests of others.").

51 Orin Kerr calls these "code-based restrictions" and "contract-based restrictions," respectively. Kerr, *Cybercrime's Scope*, *supra* note 2, at 1600. The distinction is helpful, but the terms can be misleading in two ways. First, contracts are not the only way to communicate restrictions on computer use with words; a statement by a computer owner may be effective in manifesting the limits of her expressive factual consent even if it is not binding as a contract. And second, code and words can permit, not just restrict.

52 *See Morris*, 928 F.2d at 505–06.

53 *See* Grimmelmann, *Computer Crime Law Goes to the Casino*, *supra* note 10 ("Words work for saying things; that's why we use them. In contrast, code is a terrible medium for communicating permission and prohibition.").

54 Orin Kerr appears to believe that these "contract-based" restrictions on computer use

But code also matters, even when words are clear on their face. Consider:

> *Wink Wink*: *S* creates a website to discuss and trade model cars. The terms of service, to which users must click "I agree" when they create accounts, state that no one under the age of eighteen is permitted to use the site. *A*, who is fifteen, creates an account, and selects his true year of birth from a drop-down menu as part of the signup process. So do tens of thousands of other underage users over a period of five years. *S* takes no action against them.

Here, *S* has factually consented to *A*'s use of the site, but this time code rather than words provides the manifestation of factual consent. *S* is aware that *A* and other minors are using the site in violation of the stated terms of service and has continued to allow them to do so, even though she could straightforwardly have deleted their accounts or prevented them from signing up if they selected too recent a year of birth during the account creation process. She is like a restaurant patron who says "No tip for you!" while handing the waiter a $20 bill: her actions speak louder than her words. Any plausible theory of authorization under the CFAA must therefore be willing to take both code and words into account, or it will misunderstand cases like *Security Audit* and *Wink Wink*.

III. LEGAL CONSENT

Now for legal consent: the conclusion a jurisdiction reaches when it decides that it will regard *S* as having consented to *x*. Legal consent is based on factual consent, but can depart from it in one of two ways. On the one hand, a jurisdiction might say that factual consent is not *sufficient* to constitute legal consent because there are good reasons to treat *S*'s genuine factual consent as defective.[55] On the other hand, a jurisdiction might say that factual consent is not *necessary* for legal consent because there are good reasons to treat *S* as though she had factually consented, even though she did not.[56] Westen calls legal con-

---

are simply not relevant to the question of "authorization" under the CFAA. Kerr, *Cybercrime's Scope*, *supra* note 2, at 1600; Kerr, *Norms of Computer Trespass*, *supra* note 3, at 1175; *see* Kerr, *Vagueness Challenges*, *supra* note 3, at 1572. Skepticism towards such restrictions is a consequence of conflating factual and legal consent. *See infra* Part IV. Given Kerr's normative view of the CFAA's proper scope, he ought to admit terms of service and other such word-based restrictions at the factual consent stage, but limit their role in drawing the contours of (prescriptive and imputed) legal consent. *See infra* Part III.

55 *See* WESTEN, *supra* note 4, at 139–40.

56 *Id.* at 271.

sent *prescriptive* consent when it is based on *S*'s underlying factual consent[57] and *imputed* consent when it is not.[58]

Start with prescriptive consent. The three traditional reasons for treating factual consent as invalid are coercion, deception, and incapacity.[59] To use examples from rape law, factual consent need not provide legal consent when *A* threatens to kill *S*, when *A* lies about his HIV status, or when *S* is twelve years old. The common theme is that *S*'s consent is not "true" consent because it was not the product of a genuinely autonomous choice on her part.[60] Of these three, I will focus on deception, which is pervasive in CFAA cases.

Factual consent is, as the name implies, commonly a question of fact. *S* either does or does not express consent to x.[61] Conversely, legal consent inevitably requires contestable policy choices. To say that prescriptive legal consent is not present because factual consent was procured by fraud requires saying which kinds of mistakes the jurisdiction will regard as the product of culpable fraud.[62] This is not a purely factual question; it requires normative judgments about which matters are serious enough to void consent and which are not. A jurisdiction could say that consent to trespass is not knowingly given if *S* is mistaken about what day of the week it is; no jurisdiction does, because such deceptions are regarded as too trivial to worry about.[63]

In the cases above, prescriptive consent is simple. In *House Guest*, *Weather Website*, and *Security Audit*, there is no reason on the facts as given to look behind *S*'s factual consent, so *A* also acts with prescriptive legal consent. In *Wink Wink*, *S*'s long-standing practice of letting minors use the site is both knowing and freely chosen. And in *Starbucks* and *Morris*, *S* never gave factual consent, so the question of prescriptive consent does not even arise.

---

57 *Id.* at 139. It is "prescriptive" in the sense that the jurisdiction *prescribes* the conditions it requires to treat factual consent as legally effective.

58 *Id.* at 271.

59 *Id.* at 179–91.

60 *Id.* at 191.

61 A jurisdiction might specify the interpretive rules to be used in analyzing *S*'s putative expressions of consent. Examples include a requirement of "affirmative" consent to sexual conduct or of written consent forms for consent to participate in experiments. When these rules incorporate substantive policy views or channeling rules that aim to improve the quality of expressions of consent in general, rather than being directed to ascertaining a particular *S*'s attitude toward x, they are to that extent rules of legal consent, not just of factual consent.

62 *See* Saul Levmore, *A Theory of Deception and then of Common Law Categories*, 85 TEX. L. REV. 1359, 1363 (2007).

63 *See id.* at 1362–74 (discussing fraud that does and does not vitiate consent, with examples drawn primarily from civil trespass).

For a more interesting example from the CFAA, disloyal employee cases are naturally described in terms of the employee's concealment of how she intends to use the data she acquires from company computers. For example:

> *United States v. Nosal*:[64] *S*, an executive search firm, maintains a database on its internal corporate network containing information about potential candidates.[65] *A*, an employee of *S*, copies information from the database and gives it to one of *S*'s competitors.[66]

Here, *A* uses the database with *S*'s factual consent; indeed, *S* did not merely acquiesce in *A*'s use of the database but affirmatively instructed him to use it. But this is not to say that *A* had legal consent. *A* deceived *S* about how he intended to use the information he sought to obtain from the database. Whether this deception should be regarded as vitiating *S*'s factual consent is a policy question, one that requires a court to decide whether the CFAA's statutory goals would be better served by holding *A* liable or not. Some courts regard *A* as having acted with authorization, some without.[67] Both views are plausible; neither can be deduced from first principles.

Now for imputed legal consent, in which a jurisdiction regards *S* as having given consent to *x* even when she has not (f)actually consented. The most important species of imputed consent for CFAA purposes is *constructive* consent, in which *S* is irrebuttably regarded as having consented to conduct *x* by virtue of having consented to some other conduct *y*.[68] Westen gives the hypothetical example of a "fastidious fan" *F* who stands in the middle of a stadium exit at the end of a game, shouting, "I *do not* consent to be touched!" as the crowd surges past.[69] Even if *A* could easily avoid making contact with *F*, she is under no obligation to do so; she may pass by with the usual elbow bumping associated with any densely packed crowd. *F* has consented to harmless intentional batteries of this sort by virtue of consenting to attend the game and leaving when everyone else does.

To understand constructive consent, it helps to contrast it with the other two species of imputed legal consent—*informed* consent, in

---

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

65 *See id.* at 856.

66 *See id.*

67 *Compare id.* at 864 (finding no CFAA violation), *with* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (finding CFAA violation).

68 WESTEN, *supra* note 4, at 272–75.

69 *Id.* at 322–23.

which *S* consents to a known risk of *x*,[70] and *hypothetical* consent, in which the jurisdiction assumes that *S* would have consented to *x* had she been able to.[71] A football player is deemed to give informed consent to the known risk of a broken spine from a hard hit—but this is consent only to the risk of one, not consent for an opposing linebacker to break his spine deliberately. An unconscious accident victim is deemed to give hypothetical consent to an emergency blood transfusion—but this is only a default rule, which a Jehovah's Witness can override with advance instructions to the contrary on a medical bracelet. In contrast, note that the fastidious fan's constructive consent subjects him to intentional batteries and that he can withhold it only by staying home in the first place.

Like prescriptive legal consent, imputed legal consent is invented rather than discovered. It is a legal fiction, one that the courts entertain because desirable social consequences flow from it. Informed and hypothetical consent are implied as a matter of fact; they can be justified by looking to *S*'s own interests.[72] Informed consent promotes autonomy by letting people make their own decisions about whether the benefits of a package deal are worth the risks.[73] Hypothetical consent promotes wellbeing by giving people what most of them are likely to want, while preserving autonomy for those who make clear they do not want the same thing others do.[74] But constructive consent is implied as a matter of law, because it necessarily has broader aims than just *S*'s. Getting out of the stadium at the end of sporting events would be more frustrating for everyone if fans could carry legally enforceable personal space bubbles with them. Constructive consent uses the fiction of consent because, as Westen explains, "[the subject] chose to take advantage of the benefits of a social practice that, in the state's judgment, could not justly exist and otherwise might not exist in its present form without the concomitant burdens . . . ."[75] This is the same kind of justification Baron Bramwell gave in *Holmes v. Mather*[76] for rejecting strict liability in unintentional injury cases: "For the convenience of mankind in carrying on the affairs of life, people as

70 *Id.* at 280–84.

71 *Id.* at 284–93.

72 *See* Westen, *supra* note 4, at 108, 122.

73 *See id.* at 108.

74 *See id.*

75 *Id.* at 278.

76 Holmes v. Mather, [1875] 10 LR Exch. 261 (Eng.).

they go along roads must expect, or put up with, such mischief as reasonable care on the part of others cannot avoid."[77]

Let us return to the CFAA. In *Starbucks*, there is no more reason to impute *S*'s legal consent to *A*'s use of her computer merely because she left it open on a table than there is to say that a person who leaves her wallet lying around should be deemed to consent when someone else walks off with it. No good, and much mischief, would follow from such a rule. Likewise, no useful purpose would be served by letting customers grab entire boxes of matches from shop counters or letting petty hooligans walk off with whatever they can extract from a vending machine by hook or by crook. Similar considerations apply to *Morris*; unleashing worms that crash the Internet is not something society cares to encourage. For a case raising a more interesting issue of imputed consent, consider:

> *Craigslist v. 3Taps*:[78] *S* runs a classified-ads website.[79] *A* periodically uses a program to scrape information from *S*'s website about its listings.[80] *S* sends *A* a cease-and-desist letter stating that *A* is "no longer authorized to access . . . [*S*'s] website or services for any reason."[81] *A* continues to scrape information from *S*'s website.[82]

Here, *A* scrapes *S*'s website without factual consent. *S* has made its nonacquiescence in *A*'s use completely explicit. But just as above, this is not the end of the matter. Even if *A* did not have *S*'s factual consent, there may be good reasons to impute *S*'s constructive legal consent. For example, one might argue that information on a website is publicly accessible and that allowing website owners to selectively exclude individual users would chill speech and innovation. Whether those reasons are compelling or not is a policy question, one that again requires a court to decide whether the CFAA's statutory goals would be better served by holding *A* liable or not. Some courts regard *A* as having acted with authorization,[83] some without.[84] Both views are plausible; neither can be deduced from first principles.[85]

---

77 *Id.* at 267.

78 Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013).

79 *See id.* at 966.

80 *See id.*

81 *See id.* at 967.

82 *See id.*

83 *E.g.*, Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932–33 (E.D. Va. 2010).

84 *E.g.*, *3Taps*, 942 F. Supp. 2d at 969–70.

85 *Cf.* Negro v. Superior Court of Santa Clara Cty., 179 Cal. Rptr. 3d 215, 221–25 (Cal Ct. App. 2014) (holding that consent to disclosure of email under the Stored Communications Act

If you are skeptical of the claims that the defendant in *Nosal* has factual consent and the defendant in *3Taps* does not, try taking the online aspect of the cases out of the picture. Imagine that *A* is physically seated at a computer and that the CEO of *S* is standing beside him. Immediately before he starts typing, *A* turns to *S* and asks, "May I use this computer?" In the offline version of *Nosal*, the CEO would say something like, "Yes, get started, you have dozens of calls to make and I don't have all day!" That is expressive factual consent. True, the CEO doesn't know that *A* is planning to turn around and betray *S*. But the CEO acquiesces in the computer use itself, and *A* quite rightly understands that she does.[86] On the other hand, in the offline version of *3Taps*, the CEO would say something like, "No, of course not, I already told you to stop!" That is expressive factual nonconsent. The CEO does not express an attitude of acquiescence in the computer use, and *A* quite rightly understands that she does not.

Note the relationship between prescriptive and imputed consent. They are opposites: one applies to remove factual consent where it exists, while the other applies to replace factual consent where it does not exist.[87] Only one is in play in any given case, but one or the other is always in play. The consequence is that whether *S* gives factual consent or not, there is always a live legal question of whether a court should treat *A* as acting with *S*'s consent. If factual consent is present, there is a normative question whether to regard it as prescriptively valid. If factual consent is absent, there is a normative question whether to impute it. Either way, *legal consent is a normative question.*

IV. IMPLICATIONS

Factual and legal consent are distinct. But both are indispensable concepts: trying to do without one or the other leads to confusion. So does conflating them.

"is not satisfied by consent that is merely constructive, implied in law, or otherwise *imputed* to the user by a court").

86 Even if the CEO explicitly purports to make his consent conditional on *A*'s loyalty, it is still factual consent because *S*'s agent manifests acquiescence to *A*'s access at the moment of access. The purported condition goes instead to the question of prescriptive consent. By showing that the CEO regarded *A*'s loyalty as a necessary precondition of consenting to *A*'s access, it provides a reason, though not necessarily a conclusive one, to deny that *A* has legal consent. *Cf.* WESTEN, *supra* note 4, at 199–201 (criticizing theories under which consent "is not a valid defense if [*S*] is mistaken about anything that causes her to acquiesce when she would otherwise not do so").

87 *See id.* at 108–09.

The inevitability of asking about legal consent does not mean that factual consent is irrelevant, because legal consent incorporates factual consent. Some conditions of legal consent can be rewritten without reference to *S*'s consent, some cannot.[88] For example, a jurisdiction could define statutory rape either by defining minors to be categorically incapable of giving (prescriptive legal) consent or by making it is a crime to have sexual intercourse with a minor.[89] These are equivalent definitions; one uses a fiction of nonconsent and the other does not, but they punish identical conduct. Rape as a whole cannot be so redefined, because factual consent helps define the contours of the conduct to be punished; rape defined in terms of force is a different crime that punishes different conduct than rape defined in terms of nonconsent.[90]

But just as factual consent is indispensable, so is legal consent. Being clear about factual consent helps isolate the purely normative questions of legal consent. *Starbucks*, *House Guest*, and *Weather Website* are easy cases and there is no reason to complicate them. *Morris*, *Nosal*, and *3Taps* are harder cases, because they involve ambiguities about factual, prescriptive, and imputed consent, respectively.

Although disloyal employee cases like *Nosal* and web scraping cases like *3Taps* are similar in that both involve access that is allegedly rendered unauthorized by words rather than by code, they need not be treated alike. Disloyal employee cases are prescriptive consent cases, and the crucial question is whether the employee's fraud on the employer is so fundamental that it should be regarded as making the computer use itself wrongful. This is an issue that ought to be resolved in light of the policies of employment law, including employees' duty of loyalty, trade secret duties of confidentiality, employee mobility, freedom of contract, and collective bargaining. But web scraping cases are imputed consent cases, and the crucial question here is whether to give website owners the power to selectively exclude specific users or classes of uses. Other bodies of law, including common law trespass to chattels, copyright, and contract law, also purport to (sometimes) limit such access, and the CFAA should not give dramatically different answers than they do.[91]

Recognizing that legal consent is created and not discovered also directs attention toward the kinds of doctrinal distinctions courts are

88 *See id.* at 114–19.

89 *Id.* at 116–17.

90 *Id.* at 116–19.

91 Fortunately, related concepts of consent are also at work in these other areas.

free to make. This is where the fictions of consent can do genuinely useful work. Take scraping. Online trespass to chattels has come to rest on the doctrine that "an electronic communication that neither damages the recipient computer system nor impairs its functioning" is not actionable.[92] This rule is phrased in terms of the results of *A*'s conduct, but it could just as easily be phrased in terms of *S*'s imputed consent. A reasonable computer owner who makes a website generally available could be regarded as having consented to harmless scraping, but not to scraping that causes loss of data or causes the computer to crash, just as the fastidious fan consents to being bumped up against but not to being slugged in the jaw. Such a distinction is almost impossible to derive through haruspicy on the entrails of the CFAA's tortured legislative history, but it is straightforward on a theory of authorization as consent.

Although factual consent and legal consent are distinct concepts, most academic and judicial discussion of the CFAA collapses the two. Orin Kerr's decade of work on the CFAA illustrates some of the resulting difficulties.[93] Consider his recent social norms theory of authorization under the CFAA: that "concepts of authorization rest on . . . broadly shared attitudes about what conduct amounts to an uninvited entry into another person's private space."[94]

In some places, Kerr describes social norms of offline trespass and computer misuses in ways that are appropriate when speaking of factual consent:

> The trespass norm governing a commercial store might be that entrance is permitted when a ready means of access is available that can be read in context as an open invitation. That principle limits on which means of access are allowed. An open window isn't an invitation to jump through the window and go inside. If there's an open chimney or mail drop, that's not an invitation to try to enter the store.[95]

This is a *descriptive* argument about what forms of entry a store owner factually consents to. Social norms help prospective visitors interpret the scope of the owner's consent. Kerr adds that owners can override this default against entering through the chimney by granting "explicit permission" to do so.[96] Authorization under the CFAA is the

92 Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).

93 *See supra* notes 2–3.

94 Kerr, *Norms of Computer Trespass*, *supra* note 3, at 1146

95 *Id.* at 1152.

96 *Id.*

same, Kerr argues; online or off, authorization is defined by "social signals of what entry is permitted or forbidden."[97]

But in other places Kerr describes social norms in ways that are appropriate when speaking of legal consent: "A computer owner cannot both publish data to the world and yet keep specific users out just by expressing that intent. It is something like publishing a newspaper but then forbidding someone to read it. Publishing on the Web means publishing to all . . . ."[98]

This is a *normative* argument about the proper scope of (imputed) legal consent: Kerr's "open norm of the World Wide Web" imputes consent to a specific user's access from the fact that the owner lets the public at large engage in the same form of access.[99] It is a rough online equivalent to a doctrine requiring nondiscrimination in public accommodations.

The problem is that there are cases where Kerr's descriptive and normative claims cut in opposite directions. Take *3Taps*, where the computer owner generally allowed access to a website but specifically forbade the defendant from using it. On the one hand, "[l]ife experience with common social practices creates shared understandings" that if someone tells you not to visit a website, you lack their permission to visit it.[100] On the other, "[p]ublishing on the Web means publishing to all."[101] Kerr seems to be arguing both that the owner consented to access and that it did not.

The paradox resolves itself when we recognize that Kerr is shifting between factual and legal consent. The first part of his article shows why the computer owner did not give factual consent in *3Taps*; the second part is a sustained argument that we should nonetheless impute legal consent. I previously thought that there was a contradiction between the two, but I was wrong. The two halves of his argument focus on different senses of consent.

Unfortunately, Kerr's equivocation between factual and legal consent undermines his appeal to social norms. If social norms are used descriptively, to inform computer users and courts about the scope of factual consent (as in *Weather Website* and Kerr's chimney example), they are incapable of resolving hard policy questions about the proper scope of the CFAA. But if social norms are used norma-

97 *Id.* at 1153.
98 *Id.* at 1169.
99 *Id.* at 1147.
100 *Id.* at 1150.
101 *Id.* at 1169.

tively, to tell courts when they ought to find legal consent (as in *Nosal* and *3Taps*), their use is highly problematic for precisely the reason Kerr himself pinpointed in a different paper: the contestability of online norms creates a substantial vagueness problem.[102] Kerr himself ducks the question by claiming that courts "cannot merely identify existing norms" but instead "must identify the best rules to apply."[103] This argument is not really an appeal to social norms at all; it merely restates the interpretive task facing judges but calls the resulting doctrines "norms."

Distinguishing the two kinds of consent at work allows for a weaker but more defensible version of Kerr's argument. On the one hand, the use of norms of computer use to understand factual consent is unproblematic; indeed, a social account of implicit meaning is necessary to any sensible account of expressive factual consent.[104] On the other, the most that norms of computer use can do for legal consent is to give force to policy arguments. The fact that there is a widely shared norm about a particular practice can tell courts that the practice is socially beneficial and that a decision allowing that practice will be accepted by computer users. But these are not conclusive: there is a widespread norm of driving faster than posted speed limits, and yet courts still enforce speeding laws, as they should.

CONCLUSION

I have been writing about the interpretation of a computer owner's expressions of consent, but statutes also require interpretation. "Authorization" under the CFAA is best understood as incorporating the traditional legal understanding of consent, as seen, for example, in the criminal law of trespass, theft, battery, and rape. In all of these areas, "consent" is a complex bundle of doctrines, built around factual consent but incorporating a variety of legal fictions. And they are different bundles: the same expression can manifest sufficient consent for one but not another. Computer misuse law will need its own bundle—one whose details derive not only or even primarily from congressional intent as expressed in the text of the CFAA

---

102 *See* Kerr, *Vagueness Challenges*, *supra* note 3.

103 Kerr, *Norms of Computer Trespass*, *supra* note 3, at 1147.

104 Grimmelmann, *Computer Crime Law Goes to the Casino*, *supra* note 10. "Norms" may not be the best term to describe these social facts. It might be better to speak of shared "conventions" or "expectations" about the scope of permitted use. But this is a minor point; Kerr's underlying intuition is sound.

but instead from extended judicial engagement with the facts of computer use.

Put another way, "authorization" in the CFAA requires *construction* rather than *interpretation*.[105] The linguistic meaning of "authorization" is almost completely exhausted by the observation that authorization incorporates the familiar legal concept of consent. Courts must instead construe the term by developing rules that capture the idea of a computer owner's consent effectively in light of the overall goals of the CFAA and the facts of specific cases. By using this term Congress has—dare I say it?—authorized courts to do so.

105 Lawrence B. Solum, *The Interpretation-Construction Distinction*, 27 CONST. COMMENT. 95, 100–08 (2010).