Measuring Computer Use Norms

*Matthew B. Kugler**

Abstract

Unauthorized use of computer systems is at the core of computer trespass statutes, but there is little understanding of where everyday people draw the line between permissible and impermissible computer use. This Article presents a study that measures lay authorization beliefs and punishment preferences for a variety of computer misuse activities. Though perceived authorization is strongly predictive of punishment preferences, many people view common misuse activities as unauthorized but not deserving of any meaningful punishment. Majorities also viewed as unauthorized many activities—such as ignoring a website's terms of service, surfing the news while at work, or connecting to a neighbor's unsecured wireless network—that scholars have argued are implicitly licensed. This divergence between perceived authorization and desired punishment presents a challenge for the trespass framework.

Table of Contents

Introduction

The Computer Fraud and Abuse Act ("CFAA")[1] allows for the criminal prosecution of any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[2] Though this "unauthorized access" wording has been copied widely in state and foreign codes,[3] it is largely undefined, leaving it substantially unclear

* Assistant Professor, Northwestern Pritzker School of Law.

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

2 *Id.* § 1030(a)(2)(C).

3 Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1597 (2003).

what the statute actually prohibits. Writing in 2003, Professor Orin Kerr observed that "[t]he result is an odd situation in which nearly every Anglo-American jurisdiction has an unauthorized access statute that carries serious felony penalties, but no one seems to know what these new laws cover."[4] This ambiguity in the scope of the statute has real consequences. In one case, for example, a company brought a counterclaim in a disgruntled employee's pregnancy discrimination suit on the grounds that she visited "personal websites such as Facebook" on company time.[5]

Courts and scholars have proposed numerous tests for evaluating whether a given use of a computer should be viewed as unauthorized access under the statute. Some have suggested that access is unauthorized when it circumvents a computer code-based restriction—hacking in the lay sense.[6] Others have proposed that this is really an issue of contract law: access is unauthorized when it exceeds the terms of service. Courts have sometimes taken this position in the employment law context.[7] Finally, a third group has argued that the test instead should turn on the social norms of internet users: conduct exceeds authorized access when most people understand that it is not acceptable.[8]

This Article seeks to shed light on norm-based approaches by presenting the findings of an empirical study that examined what actions people actually believe are authorized and what degree of punishment people believe is warranted by various types of unauthorized access. Currently, even those advocating for a social-norm standard are hesitant to take firm positions on what conduct it would prohibit.[9] Their reluctance is understandable: evaluating societal customs and understandings is hard. And, although several scholars have taken up the challenge of measuring social norms in the context of Fourth Amendment searches,[10] no one had previously attempted to do so in

---

4 *Id.* at 1598.

5 Lee v. PMSI, Inc., No. 8:10–cv–2904–T–23TBM, 2011 WL 1742028, at *1 (M.D. Fla. May 6, 2011).

6 *See* Kerr, *supra* note 3, at 1649.

7 *See* 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, 240–42 (2010) (reviewing cases). *But see* United States v. Nosal, 676 F.3d 854, 860–63 (9th Cir. 2012) (rejecting this approach).

8 *See infra* notes 13–15 and accompanying text.

9 Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1436–37 (2007).

10 *See*, *e.g.*, Matthew B. Kugler & Lior Jacob Strahilevitz, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory*, 2015 SUP. CT. REV. 205,

the domain of computer misuse. Commentators therefore have had little objective data on which they can rely when making their assessments of acceptable and unacceptable conduct.

The Article proceeds as follows. The first Part outlines the role of social norms in this area of law and describes the methods and overall results of the empirical study. Following this overview, the study considers three independent domains of computer misuse. The first of these domains is that of employee misuse, drawing on the substantial body of caselaw that has arisen in that area. The next Part considers the problem of accessing Wi-Fi networks without explicit permission. Though there have only been a few cases in this area, there has been extensive speculation about the social norms implicated by accessing unsecured Wi-Fi networks. The final substantive Part considers accessing a business's website in violation of its terms of service and in manners that may prove disruptive. The Article concludes by considering how everyday people appear to be relating authorization to criminalization and the extent to which unauthorized use by itself should serve as a trigger for criminal liability.

I. The Role of Social Norms in Computer Use and Study Design

Broadly speaking, there are two reasons why social norms are important in the context of the CFAA. The first of these is the instrumental advantage inherent in congruence between the criminal law and community norms. People are less likely to cooperate with law enforcement when exposed to accounts of the criminal justice system inflicting unjust punishments or failing to impose just punishments.[11] Additionally, people often draw assumptions about what society believes is right and proper from the content of laws, so there is dissonance if the law and their own moral evaluations conflict.[12]

Further, and specific to the context of the CFAA, some have proposed using social norms to define the limits of authorized use in a quasi-empirical fashion. Peter Winn, for instance, has argued that for a use to count as unauthorized it must be subjectively unauthorized (perhaps the computer owner having clearly told the user so) and any

240–44 (2016); Christopher Slobogin & Joseph E. Schumacher, *Rating the Intrusiveness of Law Enforcement Searches and Seizures*, 17 Law & Hum. Behav. 183, 198–99 (1993).

11 *See, e.g.*, Paul H. Robinson & John M. Darley, *Intuitions of Justice: Implications for Criminal Law and Justice Policy*, 81 S. Cal. L. Rev. 1, 18–28 (2007); Paul H. Robinson et al., *The Disutility of Injustice*, 85 N.Y.U. L. Rev. 1940, 1995–97 (2010).

12 *See generally* Richard H. McAdams, The Expressive Powers of Law: Theories and Limits (2015).

belief that the use *was* authorized must be in conflict with "an objective norm, reflecting the customs, practices and values of a society."[13] Orin Kerr takes a different norm-based approach, instead preferring that courts choose the "best" norms for the internet.[14] He posits a norm of inherent openness that, in his view, creates a presumption that a use is not unauthorized unless it circumvents an authorization barrier (such as a password lock), with mere violations of terms of service being grounds to kick a user out of a site, but not prosecute them for trying to enter.[15]

One fundamental question that arises when considering the question of computer use norms is which group's norms are most relevant.[16] Though there are types of computer misuse that are only possible with specialized knowledge and for which the norms of experts are most relevant, everyday people also engage in many activities that, rightly or wrongly, may fall within the scope of the CFAA—recall the example of the hapless employee who was forced to defend herself from a charge that she spent too much time on Facebook.[17] This Article considers three domains in which nontechnical people may skirt the bounds of legality. Because the focus here is on the types of activities in which common people can engage, normal American adults are the group whose norms are most relevant.

Adult American participants were assigned to one of four blocks of computer misuse questions. These blocks concerned: use of a private employer's computer in ways that arguably violate a given computer use policy, use of a government employer's computer in the same ways, use of a neighbor's Wi-Fi network without permission, and use of a business's website in ways that violate its terms and conditions. Because the same questions, with one exception, were asked regarding the private and government employer cases, those two domains are discussed together in the first Part.

A. Participants, Procedure, and Measures

A representatively-weighted sample of adult Americans was recruited by Toluna, a commercial survey firm with an established panel of respondents. The final sample contained 593 participants;[18] 97.5%

---

13 *See, e.g.*, Winn, *supra* note 9, at 1399.

14 Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146–47 (2016).

15 *Id.* at 1147, 1161.

16 Winn, *supra* note 9, at 1419.

17 *See supra* text accompanying note 5.

18 The survey instrument contained two questions directing participants to show that they

were U.S. citizens. The median age was 51 (range = 18–90, M = 49.25, SD = 17.39). Slightly more of the sample than the national population as a whole had completed at least some college coursework and far fewer participants had less than a high school education, but the sample represented a diversity of educational backgrounds.[19] When asked to rate their political orientation on a scale ranging from 1—Very Liberal to 7—Very Conservative, the mean response was 4.18 (SD = 1.83), indicating a politically moderate sample.

Each block of questions asked participants to picture a particular named individual engaging in various activities with a computer. For each activity, participants rated the extent to which the actor had authorization to use the computer in that way, the extent to which it was morally blameworthy to do so, and how, if at all, the actor should be punished. Participants rated authorization and blameworthiness on response scales that ranged from 1—Not at all to 6—Very much. Punishment ratings were made on a four-point scale with options labeled: 1—It should not be possible to punish him [and] this should not be a crime; 2—It should be punished with the equivalent of a parking ticket; 3—It should be punished like a minor crime, like petty theft; and 4—It should be punished like a major crime, like burglary of a home.

Though it is helpful to compare the mean punishment ratings assigned to each scenario, it is more important from a policy standpoint to know how many people were willing to impose each level of punishment. The basic level of punishment for exceeding authorized access or accessing without authorization under § 1030(a)(2) is a fine or imprisonment of no longer than one year. This is a misdemeanor level offense that elevates to the felony level given certain enhancements (recidivism or causing harm in excess of $5000, for example).[20] Therefore when answering the theoretical question "which of these acts does the average person think should be a crime?" it is important to remember that crimes come in varying levels of severity. If a majority

---

were paying attention by selecting a particular answer choice. Only participants who responded correctly to both questions were included in the analysis.

19 In the sample 13.8% had graduate degrees, 27% had four-year college degrees, 25.8% had two-year college degrees, 31.4% had high school degrees, and 2% had not completed high school. To compare, see *Educational Attainment in the United States: 2012—Detailed Tables*, U.S. CENSUS BUREAU, http://www.census.gov/hhes/socdemo/education/data/cps/2012/tables.html [https://perma.cc/PQ9L-XBRN] (last visited Sept. 17, 2016). (9.8% had graduate degrees, 18.4% had four-year degrees, 9.2% had two-year college degrees, 19.5% had some college with no degree, 30% had high school degrees, and 13.2% had not completed high school).

20 18 U.S.C. § 1030(c)(2) (2012).

of participants assign a given scenario either "no punishment" or "no punishment greater than a parking ticket," then that is not a validation of the level of punishment required by the CFAA.

B. Overall Relationships Between Authorization, Blameworthiness, and Punishment

Past research has shown that moral evaluation is a strong predictor of punishment severity; people punish what they find morally objectionable.[21] Conduct that is seen as more morally blameworthy should therefore be more likely to be criminalized. Since unauthorized use of a computer is at the core of the CFAA, perceived authorization should also correlate with both moral blameworthiness and punishment.

There are two ways to conceive of these relationships. First, authorization may be associated with blameworthiness and punishment across scenarios. This was tested by generating mean scores on the authorization, blameworthiness, and punishment ratings for each of the nineteen scenarios, creating a new dataset in which each scenario was its own case. These three mean scores were then correlated with each other. As can be seen in Table 1A, authorization was significantly linked to blameworthiness and punishment. When the behavior described in a scenario was seen as less authorized, it was seen as more blameworthy and deserving a greater punishment. There correlations are very strong; most of the variance in blameworthiness ($r = -.886$, $r^2 = .785$) and punishment ($r = -.736$, $r^2 = .542$) can be predicted from authorization.

The other way of evaluating the relationships between these three measures is at the individual level. Here, the question is whether differences among individuals in how they perceived authorization in a given case were related to differences in their blameworthiness and punishment judgments. Correlational analyses were therefore conducted looking at the relationships of authorization with blameworthiness and punishment for each individual scenario. These nineteen sets of correlations were then averaged to create Table 1B.[22] These correlations are weaker than those in Table 1A, but they are still substantial and still statistically significant. To the extent that person A perceived the conduct in a particular case as more authorized

---

21 *See, e.g.*, Adam L. Alter et al., *Transgression Wrongfulness Outweighs Its Harmfulness as a Determinant of Sentence Severity*, 31 LAW & HUM. BEHAV. 319, 334 (2007).

22 Specifically, the nineteen sets of correlations were converted to Fisher's z-scores, averaged, and then converted back into standard correlation coefficients.

than did person B, they also generally saw the conduct as less blameworthy and less deserving of punishment.

TABLE 1. OVERALL RELATIONSHIPS BETWEEN AUTHORIZATION, BLAMEWORTHINESS, AND PUNISHMENT.

1A. CORRELATIONS AT THE SCENARIO LEVEL

	Authorization	*Blameworthiness*	*Punishment*
Authorization		-.886	-.736
Blameworthiness	-.886		.891
Punishment	-.736	.891	

1B. THE RATINGS OF INDIVIDUALS WITHIN SCENARIOS

	Authorization	*Blameworthiness*	*Punishment*
Authorization		-.319	-.367
Blameworthiness	-.319		.395
Punishment	-.367	.395	

NOTE: Numbers are correlation coefficients, and all coefficients are significant at the $p < .001$ level.

These two sets of analyses support the proposition that assessments of authorization are related to judgments of blameworthiness and punishment. This is a useful validation of the general approach of the CFAA: authorization is certainly one of the key factors in determining whether computer use is wrongful. As will be seen, however, there is a substantial complication: the mere fact that conduct is viewed as unauthorized will not suffice to establish that it should receive CFAA-level punishment.

II. MISUSE OF AN EMPLOYER'S COMPUTER

Likely the most active area of CFAA litigation is between employers and their former employees. Whether the CFAA claim is standing in for a trade secrets claim,[23] being used as a threat to counter a discrimination suit,[24] or is being used to punish freestanding bad conduct,[25] litigation in this area appears to be ubiquitous.[26] Due to this emphasis in the caselaw, the largest block of computer misuse

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

24 Lee v. PMSI, Inc., No. 8:10–cv–2904–T–23TBM, 2011 WL 1742028, at *1 (M.D. Fla. May 6, 2011).

25 United States v. John, 597 F.3d 263, 271–73 (5th Cir. 2010).

26 *See* Stephanie Greene & Christine Neylon O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281, 284–85 (2013).

questions in the study concerned use of an employer's computer in violation of a company's stated policies. This Part begins with an overview of the questions and caselaw, and then turns to the experimental manipulations and results.

Participants were told to imagine a middle manager at a health insurance firm, XYZ Corporation, named John. XYZ Corporation has a computer use policy that clearly states that computers and other electronic devices provided by the company are to be used solely for company business and that use will be monitored. John is described as using his computer in five different ways that arguably violate this policy:

- Using his computer to check the weather for his commute home and to read the news for fifteen minutes before starting work.
- Storing a quantity of baseball videos on his employer's network drive so that he could watch them during his lunch break, when he is not expected to be working.
- Giving client information to a friend starting up a financial services company that would market to people like XYZ Corporation's customers.
- Copying confidential documents from the company's server and selling them to the company's competition.
- Looking up his neighbors in the XYZ Corporation database for his own amusement.

For two of these vignettes, participants were asked to rate low and high severity versions of the facts. For the baseball video hypothetical, they were asked to imagine a version in which the storage of the videos has no effect on the functioning of the computer equipment and costs the company no money and a version where the drain on computer resources prompts the company to spend money to upgrade the equipment. For the "giving client information to a friend" case, participants were asked to imagine versions in which the information is fairly limited (names and contact information) and a version in which the information includes sensitive medical and financial data.

The first vignette, where an employee uses the computer to spend a few minutes goofing around online, is based on a hypothetical that the Ninth Circuit considered in *United States v. Nosal*.[27] In declining to adopt a broad view of the CFAA, the court specifically noted that an expansive reading of "without authorization" could criminalize common exercises in workplace procrastination such as Gchatting,

[27] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

playing games, and shopping online.[28] Most companies forbid their employees from engaging in such activities, so, in a literal sense, they are unauthorized. As Judge Kozinski observed, "[w]hile it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be."[29]

The second vignette was inspired by *United States v. Collins*[30] and *State v. McGraw*,[31] each of which concerned an employee storing personal files on a work computer in violation of a computer use policy. Neither case was brought under the CFAA—both were litigated as trespass-style actions—but both arguably concern exceeding authorized access to an employer's computer system. In *McGraw*, the court specifically noted that the defendant's use of the employer's computer system did not inconvenience the employer or interfere with the employer's own uses of the system and that this lack of harm was important,[32] prompting the two versions.

Sharing client information and selling trade secrets are, in some sense, the bread and butter of expansive CFAA interpretation.[33] Courts have generally been sympathetic to employers' claims that using a computer in a way that was plainly against the employer's interests (an agency theory), or in violation of an explicit policy, amounts to a violation of the CFAA.[34] There has recently been some pushback against this position, however, most notably by Judge Kozinski in *Nosal*. He argued that extending the CFAA to cover trade secrets cases would open the door to the types of overreach described above and that employers should therefore rely on other remedies.[35]

Though browsing client information for personal amusement does not involve the obviously high stakes of trade secret theft, it nevertheless is extremely important, particularly in the context of medical service companies and government agencies. One case that raises this issue is *United States v. Czubinski*,[36] in which an IRS employee viewed the tax returns of friends and enemies for personal gratification.[37]

---

28 *Id.* at 860.

29 *Id.*

30 United States v. Collins, 56 F.3d 1416 (D.C. Cir. 1995).

31 State v. McGraw, 480 N.E.2d 552 (Ind. 1985).

32 *Id.* at 554.

33 *See* Greene & O'Brien, *supra* note 26, at 282–83.

34 *See generally* Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819 (2009).

35 United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

36 United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997).

37 *Id.* at 1071–72.

Though his conviction was ultimately overturned on other grounds, the First Circuit noted that he "unquestionably" had exceeded authorized access.[38] Similarly, an employee of the Social Security Administration exceeded authorized access when he looked up information on his ex-wife, ex-girlfriends, and a variety of others, generally women he appeared to be interested in dating.[39]

There were two additional wrinkles in the employee misuse questions. First, the same employee misconduct scenarios were posed to a separate group of participants in which the employee worked not for a private corporation but instead for the Department of Health and Human Services. This employee engaged in the same basic types of conduct (excepting the baseball videos, which were only included for the private corporation version), with appropriate modifications to suit the government context. For example, this employee gave information on Medicare beneficiaries (rather than clients) to a friend and sold department secrets (rather than corporate secrets) to a private corporation.

Interestingly, this difference between government and private misconduct did not affect any of the responses; there are no statistically significant differences across these conditions on any measure. Given cases like *Czubinski*, one can see why a rule that treats government employees more rigidly may seem appealing. These respondents, however, did not place any weight on the difference between government and private employees. This is a surprising result and may be worth examining in other contexts. Here, both the government agency and the private company were dealing with health data, which is inherently very sensitive. Misuse of this data by any actor may have been sufficiently troubling so as to drown out aggravation for government actors.

The second wrinkle concerned the way in which the employee was informed of the computer use policy. In one version of the study, the employee was described as learning of the computer use policy at the time he started his employment; the policy was one of many forms he completed on his first day. In the other version of the study (seen by a different set of participants), the computer use policy was printed on his screen every time he logged on, and he had to click to show that he had read and understood it. Participants did not differentiate between these conditions either. It is possible that these two notice conditions were not perceived as indicating different workplace norms,

---

38 *Id.* at 1078.

39 United States v. Rodriguez, 628 F.3d 1258, 1261–63 (11th Cir. 2010).

but that a more extreme manipulation (perhaps an in-person warning or a company training session) would have a different effect. This particular manipulation was chosen because many companies appear to opt for either a one-time policy document or a warning on the login screen, though obviously some take more elaborate measures.[40]

Since there are no significant differences between the government and corporation conditions or the two notice variants, all data is combined for analysis.[41] The results are shown in Table 2. First, nearly all participants did not seek to impose meaningful punishment on those who used their company computers to read the news before starting work, though 31.6% would have imposed parking ticket-level liability. This is strong support for Judge Kozinski's intuition in *Nosal*: it would be absurd to make this type of technical violation of a computer use policy a crime.[42] Yet, importantly, this conduct was still seen as unauthorized; the mean score was a full point below the scale's midpoint. The employee who used the system to look up information about his or her neighbors or sell trade secrets, on the other hand, was assigned at least misdemeanor-level liability by a majority of participants. In the trade secrets case, a full 77% opted for burglary-level punishment.

The scenarios in which an employee stored personal files on a work computer received different ratings depending on whether the misconduct interfered with the computer system.[43] When there was no interference, the overwhelming majority of participants either imposed no punishment (48%) or parking ticket-level punishment (37.8%), well under the minimum level required by the CFAA. When there was interference, however, a substantial minority imposed at least petty theft-level liability (41.2%), and very few participants im-

---

40 Christine A. Henle et al., *Designing Electronic Use Policies to Enhance Employee Perceptions of Fairness and to Reduce Cyberloafing: An Empirical Test of Justice Theory*, 25 COMPUTS. IN HUMAN BEHAV. 902, 903 (2009).

41 The analysis took the form of an analysis of variance ("ANOVA") with government versus corporation and daily versus one time notice as between subject factors. There were no significant main effects of either factor on any measure (all *p*s greater than .05). Because data was combined across the public/private factor and both had one fourth of the total sample, results in this block are therefore based on twice as many responses as results in the following two blocks.

42 *See supra* text accompanying notes 27–29.

43 A mixed ANOVA was conducted looking at the effects of warning type (daily or at time of hiring) and interference with company (either no cost or upgrade required). There were no effects related to warning type. The ratings of authorization $F(1, 146) = 11.32$, $p < .001$ $\eta^2 = .07$, blameworthiness $F(1, 146) = 53.26$, $p < .001$ $\eta^2 = .27$, and punishment $F(1, 146) = 114.21$, $p < .001$ $\eta^2 = .44$ are all significantly different across interference conditions, however.

posed no punishment (16.8%). Authorization and blameworthiness followed a similar pattern, with the conduct that interfered being seen as less authorized and more blameworthy. Given how context-dependent liability here appears to be, it is worth considering whether explicit warnings would have mattered here, even if they would not elsewhere. Though this scenario speaks to actual rather than expected consequences, one could easily imagine the alternative: an employer telling employees to not use their computers in a particular way because it might result in harm to the employer's system. Based on this data, one could expect such a warning to have a meaningful influence on liability judgments, despite the failure of the generalized notice condition, because the employee would then have acted with the knowledge that his or her computer use would cause direct harm.

The sharing of client information was seen as maximally unauthorized and blameworthy regardless of whether the information shared was limited or extensive, and there were no significant differences across conditions on those measures. This is likely due to a range restriction; participants had such extreme reactions to the more "mild" of these vignettes on blameworthiness and authorization that there was no room to show aggravation for the more "severe" one. Participants were inclined to punish the sharing of more detailed information more severely,[44] however, which is consistent with the CFAA's provision for imposing felony punishment on acts that cause damage in excess of $5000.[45]

TABLE 2. ATTITUDES TOWARD USING AN EMPLOYER'S COMPUTER FOR VARIOUS NONWORK PURPOSES

	Checking Weather and News	***Examining Files of Neighbors***	***Selling Trade Secrets***
Authorized	2.32 (1.60)	1.44 (1.17)	1.43 (1.23)
Blameworthy	3.37 (1.64)	5.21 (1.46)	5.40 (1.40)
Punishment	1.51 (0.70)	3.08 (0.93)	3.65 (0.74)
- No Punishment	59.5%	7.6%	3.8%
- Parking Ticket	31.6%	16.5%	4.8%
- Petty Theft	7.6%	36.8%	14.4%
- Burglary	1.4%	39.2%	77.0%

44 $F(1, 287) = 130.47$, $p < .001$ $\eta^2 = .31$.

45 18 U.S.C. § 1030(c)(4)(A) (2012).

	Sharing		*Storing Private Files*	
	Client Names	***Sensitive Client Information***	***No Interference/ Cost to Company***	***Interference/ Cost to Company***
Authorized	1.51 (1.22)	1.43 (1.17)	2.05 (1.59)	1.70 (1.39)
Blameworthy	5.15 (1.42)	5.20 (1.54)	3.66 (1.72)	4.65 (1.56)
Punishment	3.02 (0.90)	3.44 (0.83)	1.70 (0.80)	2.33 (0.86)
- No Punishment	7.2%	4.5%	48.0%	16.9%
- Parking Ticket	17.2%	8.9%	37.8%	41.9%
- Petty Theft	41.6%	24.4%	10.8%	32.4%
- Burglary	34.0%	62.2%	3.4%	8.8%

NOTE: Means (standard deviations in parentheses) for the authorization, blameworthiness, and punishment measures, as well as the percentage of participants choosing to impose each level of punishment. Authorization and blameworthiness were rated on 1–6 scales with higher numbers indicating more authorization and blameworthiness.

When considering these data, it is important to remember that the participants were not indicating a desire to punish the actor under a particular statute. But if the actor in these vignettes is liable under the CFAA, then that statute's punishment scheme should serve as a floor for his ultimate level of liability. These data support imposing that sort of punishment for breaches of confidentiality, theft of trade secrets, and use of employer computer equipment in ways that interfere with business operations. They draw a distinction, however, for the procrastinating employee who reads the news and the employee who uses their employer's computer in a way that does not interfere with the employer's business. For those cases, this sample rejects assigning CFAA-level liability.

Importantly for the CFAA statutory scheme, none of the employee conduct in these cases is actually seen as authorized. Recall that authorization is rated on a 1–6 scale. Though some conduct is not criminalized by most participants, even the most favorable case only receives an authorization level of 2.32 out of 6, which is significantly below the midpoint of 3.5.[46] This presents something of a puzzle for the CFAA. All the conduct is, in absolute terms, unauthorized. Yet participants are criminalizing only some of the unauthorized conduct. Authorization is plainly related to the desire to impose punishment—consider the correlations reviewed in Section I.B—but more is needed to merit criminal sanction. Considering the various scenarios, it appears that the combination of unauthorized conduct with either harm

[46] $t(149) = 9.00$, $p < .001$.

to the employer or a violation of the privacy rights of customers is sufficient to give rise to meaningful liability. Unauthorized conduct alone, however, does not.

III. Accessing a Neighbor's Wi-Fi Network

It has been suggested that the epitome of CFAA overreach would be a prosecution for connecting to a neighbor's unsecured Wi-Fi network without explicit permission.[47] That case has, thankfully, not yet been brought. But a case that raised a closely-related question of law has. In *United States v. Ahrndt*,[48] the defendant's neighbor accessed the defendant's unsecured home wireless network and then, opening iTunes, observed that the defendant was sharing a number of files that appeared to be child pornography.[49]

The CFAA was not at issue in *Ahrndt*; the key question was whether the neighbor's actions amounted to a Fourth Amendment search. There is concern, however, that many interpretations of exceeding authorized access would stretch to include use of a person's unsecured wireless network.[50] After all, people like the defendant in *Ahrndt* certainly do not mean to authorize their neighbors to view their files. Any effort to argue that the access *was* authorized would have to accept as valid factors that have been rejected in other contexts—for example, that lack of security counts as implicit license—or turn on an examination of the social norms of Wi-Fi use. This block of vignettes therefore sought to test the question of whether accessing an unsecured network and then performing various activities is viewed as authorized by everyday people and whether it should give rise to CFAA-level liability. The main scenarios involved:

- Accessing a neighbor's unsecured Wi-Fi network.
- Accessing a neighbor's secured Wi-Fi network by guessing the password.
- After having accessed the neighbor's unsecured network, looking at the files they share via iTunes (music and playlists).
- After having accessed the neighbor's unsecured network, looking at the files they share with their home network ("My Pictures" and "My Documents").

---

47 *See, e.g.*, Robert V. Hale II, Esq., *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 Santa Clara Computer & High Tech. L.J. 543, 544–50 (2005); Ryan Singel, *Burning Question: Is Wi-Fi Squatting Illegal?*, WIRED (Mar. 29, 2011, 12:00 PM), http://www.wired.com/2011/03/pr_burning_wifi_squatting/.

48 United States v. Ahrndt, No. 3:08-CR-00468-KI, 2013 WL 179326 (D. Or. Jan. 17, 2013).

49 *Id.* at *3–5.

50 Hale, *supra* note 47, at 544–50.

The latter two cases had two variants. In one variant, the actor, named Jim, only looked at the list of shared files. This is closely analogous to the initial conduct in the *Ahrndt* case. In the other variant, Jim opened and examined the shared files. This was intended to create two different levels of privacy invasion.

Though many people are familiar with routers and wireless networking, some are not. Therefore, the first of these scenarios was introduced with the following context:

> Many people have wireless routers in their homes. Though these routers are often secured with passwords, sometimes they are not. Imagine a person named Jim. Jim notices that his neighbor has an unsecured wireless network and, without his neighbor's permission, tells his computer to connect to it. Jim then browses the Internet normally.

It was therefore clear to participants that the user was able to access the network with a simple mouse click and also that this access was not explicitly permitted by the neighbor.

Unsurprisingly, accessing the secured network by guessing the password is seen as significantly less authorized, more blameworthy, and deserving of greater punishment than accessing the unsecured network (see Table 3).[51] Only 31.6% of participants would impose less than petty theft-level liability on a person accessing a secured network, but a thin majority (51.7%) would for accessing an unsecured network. Again, interestingly, the case in which a majority of participants did not wish to impose petty theft-level liability was still seen as unauthorized (2.10 < 3.50).

This willingness to impose punishment on an actor using an unsecured Wi-Fi network is both informative and surprising. It has been argued that leaving a home network unsecured gives implicit permission to those passing by to use it, and there are good policy arguments in favor of this perspective.[52] Here, however, it was viewed by nearly half the sample as deserving at least petty theft-level punishment and by only a third of the sample as deserving no punishment at all. This is a surprisingly clear statement of perceived social norms: most survey respondents believe that accessing the network is unacceptable. To these respondents, not installing a password is like not locking

---

51 A within-subjects ANOVA was conducted. The ratings of authorization $F(1, 148) = 14.90$, $p < .001$ $\eta^2 = .09$, blameworthiness $F(1, 148) = 37.51$, $p < .001$ $\eta^2 = .20$, and punishment $F(1, 148) = 51.08$, $p < .001$ $\eta^2 = .26$ are all significantly different across network scenarios.

52 *See* Stacy Nowicki, *No Free Lunch (or Wi-Fi): Michigan's Unconstitutional Computer Crime Statute*, 13 UCLA J. L. & TECH. 1, 38–39 (2009).

one's door or not putting a fence around one's yard: it may be imprudent, but it is not an invitation to trespass.

Another analysis looked at the four conditions that involved viewing the files shared on the neighbor's network. This took the form of a 2-by-2 analysis of variance ("ANOVA") examining, first, whether looking at general files was different than looking at iTunes files and, second, whether opening files was viewed as different than merely viewing the list of them. Results showed that looking at iTunes files was seen as significantly less blameworthy and deserving of less punishment than looking at general files,[53] though it was no more authorized. Actually opening the files (of either type) was seen as less authorized, more blameworthy, and deserving of more punishment than merely viewing a list of them.[54]

TABLE 3. ATTITUDES TOWARD USE OF NEIGHBOR'S WI-FI NETWORK

	Unsecured Network	***Secured Network***
Authorized	2.10 (1.66)	1.58 (1.39)
Blameworthy	4.52 (1.72)	5.34 (1.31)
Punishment	2.23 (1.02)	2.81 (0.90)
- No Punishment	33.6%	10.1%
- Parking Ticket	18.1%	21.5%
- Petty Theft	39.6%	46.3%
- Burglary	8.7%	22.1%

	iTunes		***General Files***	
	List	***Open***	***List***	***Open***
Authorized	1.70 (1.39)	1.66 (1.36)	1.74 (1.43)	1.62 (1.30)
Blameworthy	4.79 (1.49)	4.94 (1.51)	5.02 (1.47)	5.17 (1.35)
Punishment	2.26 (0.97)	2.55 (1.00)	2.40 (1.01)	2.68 (1.00)
- No Punishment	28.2%	21.5%	24.2%	18.1%
- Parking Ticket	26.8%	18.1%	26.2%	16.1%
- Petty Theft	36.2%	44.3%	35.6%	45.0%
- Burglary	8.7%	16.1%	14.1%	20.8%

53 Blameworthiness $F(1, 148) = 11.18$, $p < .001$ $\eta^2 = .07$ and punishment $F(1, 148) = 8.99$, $p = .003$ $\eta^2 = .06$.

54 The ratings of authorization $F(1, 148) = 4.90$, $p < .05$ $\eta^2 = .03$, blameworthiness $F(1, 148) = 10.84$, $p < .001$ $\eta^2 = .07$, and punishment $F(1, 148) = 46.35$, $p < .001$ $\eta^2 = .24$ are all significantly different across condition.

The sample was effectively evenly split between those who wanted to impose at least petty theft level-liability in the cases where the actor merely viewed the list of shared files and those who did not. It may be that participants believed that seeing that files were shared was an inevitable byproduct of accessing the network, and therefore deserving of no additional punishment. Compare the proportion of participants imposing less than petty theft level-liability for simply accessing the network (51.7%) to the proportion doing so for looking at the list of iTunes files (55.0%). The numbers are virtually identical and, to the extent they differ, it is in the wrong direction. Opening the files, however, was viewed substantially more negatively. Slightly less than 40% of participants imposed less than petty theft level-liability even to an actor opening the iTunes files.

These data provide a challenge to those who wish to treat uninvited Wi-Fi access as an easy question. From a policy standpoint, there may be many good reasons to treat unsecured networks like public water fountains.[55] But it is hard to reach this result given authorization norms. Adding a harm requirement would be quite useful here. Since accessing a Wi-Fi network does not inflict meaningful damages unless other action is taken, it will likely escape CFAA liability.

IV. Accessing a Business's Website

Another major question in the CFAA context involves the permissibility of accessing a business's website in a way that is either explicitly prohibited by the website's terms of service or that is outside the intended uses of the site. One problem in this area involves the use of web scraping (or web crawling) tools. These are programs that automatically visit and monitor websites, perhaps to record pricing or contact information. This information is technically available to the public, but companies often object to having it systematically collected by their competitors. Sometimes this objection is rooted in a desire to not make their competitor's lives easier. Other times, however, the target company is concerned that such tools will slow down their sites for actual consumers. Some courts have been sympathetic to claims that the use of these tools, particularly when they circumvent a technological barrier, exceeds authorized access under the CFAA.[56] There is also the general issue of whether violations of a website owner's

---

55 *See* Nowicki, *supra* note 52, at 38–39.

56 Matthew Kapitanyan, *Beyond* WarGames*: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & Pol'y 405, 430–33 (2012).

stated terms and service are the business of the federal criminal law. If owners say that their websites can only be used for a particular purpose or by a particular kind of person, does that restriction create an enforceable access limitation?

This block of questions included six scenarios, five of which concerned the activities of Bob, the head of strategic planning at a large corporation. Bob was described as engaging in the following activities:

- Visiting the website of his competitor so that he could set his prices lower.
- Doing the same, but while ignoring a notice that states the website is to only be viewed by the competitor's customers and that all others should leave.
- Creating a web crawling program that periodically visits the competitor's website and extracts prices for a range of products, while correctly estimating that this program will not slow down the competitor's website.
- Creating such a program while correctly estimating that the program *will* slow down the website.
- Creating a program that is actively intended to overload the competitor's website so that other people cannot use it.

Because some participants might not understand the motivation behind using a web crawling program, the scenarios included the following description:

> Bob and his competitor both sell a wide range of products, and the prices of these products can change quickly. This would be true of airline tickets and stocks, for example. Bob therefore writes a program that checks his competitor's website for pricing information and automatically generates a report on their pricing trends.

This was intended to make clear that creating the web crawling program provided a valid business benefit to Bob.

Another scenario assessed participants' views of an everyday individual using a minor trick to circumvent a website's controlled access regime. This vignette described a person bypassing the *New York Times*'s free monthly article viewing limit. It explained that the article limit could be circumvented by using more than one browser or Google Chrome's incognito mode to make it appear that a new computer was visiting the site.

The first vignette, merely visiting the competitor's website, is plainly not a violation of the CFAA; there is not even a warning tell-

ing Bob that he is not allowed to do so. The second case, where Bob is ignoring a warning, is a hypothetical considered by Judge Kozinski in the *Nosal* case. Kozinski believed it would be absurd to treat commonly performed activities such as sharing a Facebook password or ignoring the MySpace terms of service as violations of federal criminal law.[57] The First Circuit made a similar observation in one of the web scraper cases described below, noting that there was a strong policy interest in not allowing merchants to exclude competitors from their places of business.[58] The *New York Times* scenario is different in that it involves both the violation of terms of service, like the ignoring a warning case, and also a trivial circumvention of a technological access barrier.

The web scraper vignettes were inspired by a pair of First Circuit cases that involved the same underlying set of facts: a web scraping program extracted price information from a travel-planning website, allowing the company to be undercut.[59] These cases turned on factual points that are not relevant to the current study,[60] but the problem of web scrapers is of general interest: there is much social value in allowing consumers (or, rather, consumer-oriented data aggregators) to automate price comparisons across vendors, and researchers use web scraping to assemble datasets for a wide range of purposes.[61] Of particular importance to the present study is the idea of implied license, which was discussed briefly in the later of the two First Circuit cases.[62] The court there declined to find an implicit prohibition on the use of web scrapers in the absence of an express ban. The three web scraper variants included in this study push at that possibility, seeking to determine whether participants sharply differentiate between the type of "harmless" scrapers at issue in the First Circuit cases and the more

57 *See* United States v. Nosal. 676 F.3d 854, 861–62 (9th Cir. 2012); *see also supra* text accompanying notes 27–29.

58 *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003) (citing the classic *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 516–18 (4th Cir. 1999) and *Desnick v. ABC, Inc.*, 44 F.3d 1345, 1351 (7th Cir. 1995) cases).

59 *Id.* at 59–60; EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–81 (1st Cir. 2001).

60 *See* Kapitanyan, *supra* note 56, at 430–33.

61 *See, e.g.*, Jeffrey Kenneth Hirschey, Note, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 BERKELEY TECH. L.J. 897, 898–901, 921–23 (2014) (describing the role of price aggregators in the airline industry, among other examples); Jim Snell & Derek Care, *Use of Online Data in the Big Data Era: Legal Issues Raised by the Use of Web Crawling and Scraping Tools for Analytics Purposes*, BLOOMBERG LAW (Aug. 28, 2013), http://www.bna.com/legal-issues-raised-by-the-use-of-web-crawling-and-scraping-tools-for-analytics-purposes/.

62 *Zefer Corp.*, 318 F.3d at 63.

technologically disruptive scrapers described in the second and third vignettes.

The first analysis in this Part compared the vignettes that involved visiting a website that either did or did not have a "customers only" warning. Ignoring the warning resulted in significantly less perceived authorization, more blameworthiness, and more punishment (see Table 4).[63] Notably, the scenario in which the actor visits the website lacking a "customers only" warning is the only one in this study that received a substantially above-midpoint rating on authorization. That scenario also received no punishment from almost two-thirds of participants. Merely ignoring the warning, however, was enough to persuade a meaningful number of people to change their position.

TABLE 4. ATTITUDES TOWARD ACCESSING A BUSINESS'S WEBSITE WITHOUT PERMISSION

	Visiting Website	***Visiting Website While Ignoring Warning***	***NYTimes Article Limit***
Authorized	4.15 (1.87)	2.66 (1.80)	2.55 (1.72)
Blameworthy	3.12 (1.80)	3.89 (1.83)	3.93 (1.77)
Punishment	1.67 (1.02)	2.07 (1.08)	1.81 (0.87)
- No Punishment	66.2%	44.1%	45%
- Parking Ticket	8.6%	16.4%	33.1%
- Petty Theft	17.1%	28.3%	17.9%
- Burglary	7.9%	11.2%	4.0%

	Use of Web Crawler		
	No Interference	***Expected Interference***	***Sabotage***
Authorized	3.53 (1.80)	2.28 (1.56)	1.44 (1.09)
Blameworthy	3.17 (1.66)	4.37 (1.64)	5.17 (1.59)
Punishment	1.69 (1.02)	2.46 (1.04)	3.34 (0.81)
- No Punishment	63.2%	25.2%	3.3%
- Parking Ticket	14.5%	19.9%	11.2%
- Petty Theft	13.2%	38.4%	33.6%
- Burglary	9.2%	16.6%	52.0%

63 The ratings of authorization $F(1, 150) = 89.85$, $p < .001$ $\eta^2 = .38$, blameworthiness $F(1, 150) = 26.03$, $p < .001$ $\eta^2 = .15$, and punishment $F(1, 150) = 33.49$, $p < .001$ $\eta^2 = .18$ are all significantly different across condition.

The individual actor in the *New York Times* scenario, who actively circumvents a website's access regime, actually receives less punishment than a corporation that merely ignores a website's terms and conditions. This could represent an anticorporate bias, similar to that observed in the torts context.[64] Regardless, merely ignoring the website warning or bypassing a de minimis security procedure was insufficient to give rise to CFAA-level liability in a majority of respondents. These results suggest that the more extreme versions of the code-bypass and contract terms of service views are not consistent with public attitudes; people want to see some additional wrongful conduct or harmful consequence before they impose substantial liability.

The web crawler questions also reveal interesting variations. The "no interference" condition was generally viewed as not deserving any punishment (63.2%). The punishment scores are comparable to simply viewing the website. The authorization rating was almost on the scale's midpoint (3.53 compared to 3.50), suggesting that use of the crawler was seen neither as plainly authorized nor plainly prohibited. The web crawler that was known to interfere with the target website was viewed as significantly less authorized, more blameworthy, and deserving of greater punishment, however, and the web crawler that was intended to have a sabotaging effect even more so.[65] Though deliberate sabotage drew the harshest sanction, participants assigned substantial punishment to use of even the web crawler that was known to interfere with the target. Therefore, participants did not object to the use of web scrapers per se, but did take a dim view of those that interfered with the operation of the host website.

CONCLUSION

Computer use has become ubiquitous in modern society. In 2012, an estimated 74.8% of American households had internet in the

64 *See generally* Robert J. MacCoun, *Differential Treatment of Corporate Defendants by Juries: An Examination of the "Deep-Pockets" Hypothesis*, 30 LAW & SOC'Y REV. 121 (1996) (showing that corporate status, more than deep pockets, explains large awards against corporations).

65 This analysis took the form of a three factor within-subjects ANOVA. There were main effects on $F(1.74, 264.64) = 94.16$, $p < .001$ $\eta^2 = .39$, blameworthiness $F(1.66, 248.22) = 74.12$, $p < .001$ $\eta^2 = .33$, and punishment $F(1.81, 271.53) = 187.49$, $p < .001$ $\eta^2 = .56$ (due to sphericity violations, Greenhouse Geisser results are reported). Comparison of means revealed that there were significant differences between each of the three conditions on each of the three measures ($p < .001$).

home,[66] and many of the rest may have had access to the internet at work, school, or in public libraries. It is perhaps unsurprising, then, that people have sophisticated and nuanced views of what constitutes appropriate and inappropriate computer use; this is an area where the overwhelming majority of Americans have repeated personal experience. And, if one truly wishes to consider the social norms of everyday Americans when deciding what is and is not unauthorized use, one needs to directly tap that experience. It is not enough to merely guess at what people will and will not find reasonable.

This Article is a first step in that direction. These data provide meaningful information about what is and is not viewed as authorized. They also show that people do strongly link perceived authorization to judgments of blameworthiness and criminality; those activities that are seen to be less authorized are more likely to be judged criminal and are assigned greater punishment.

But this finding should not be overinterpreted. Even though nearly all of the computer misuse scenarios were viewed as being more unauthorized than authorized, some of these were still not viewed as deserving criminal punishment at the level suggested by the CFAA. This divergence suggests an important qualification to the CFAA analysis: something more than mere unauthorized access is needed to make people willing to endorse criminal sanctions. So while these data help define authorization, they also raise questions about the fundamental unauthorized access framework.

One important question is whether there would be a similar pattern for relatively minor physical trespasses. It is possible that there, like here, people would view unauthorized entry as wrong (see blameworthiness) but be reluctant to impose meaningful liability absent harm. If that is the case, then the problem here is neither the definition of unauthorized access nor the parallel to physical trespass but instead only the lack of proportionality in damages.

It is also interesting to note, however, that this story is not entirely one of unexpected leniency. Nearly half the sample wanted to impose misdemeanor-level liability to a person who connected to a neighbor's unsecured wireless network. For many, this would be overreach in the extreme.[67] Yet a jury composed of members of this sample might well convict. Also, though it is presumably quite common for people to procrastinate at work or store a small number of per-

66 U.S. Census Bureau, Computer & Internet Trends in America (2014), https://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf.

67 *See* Hale, *supra* note 47, at 544–50; Singel, *supra* note 47.

sonal files on their work computers, people did not read this ubiquity as implying a degree of employer license. Few participants wanted to criminalize such conduct, but they stated that it was unauthorized and, to some extent, blameworthy. This complex interplay suggests that there could be a wealth of other unexpected findings awaiting further exploration and should serve to caution those who, like the Author, have been prone to speculate about societal norms in the absence of data.