Harvard Journal of Law & Technology
Volume 24, Number 1 Fall 2010

THE COMPUTER FRAUD AND ABUSE ACT: HOW COMPUTER SCIENCE CAN HELP WITH THE PROBLEM OF OVERBREADTH

*Cyrus Y. Chung**

TABLE OF CONTENTS

I. INTRODUCTION 233

II. THE CFAA AND JUDICIAL THEORIES OF CFAA INTERPRETATION 236
A. Statutory Language of the CFAA 236
B. Legislative History of the CFAA 237
C. The Agency-Based Theory 239
D. The Contract-Based Theory 240
E. Criticism of the Agency- and Contract-Based Theories 242

III. THE "CODE-BASED" THEORY OF INTERPRETATION 243
A. The Code-Based Theory 244
B. Limitations of the Code-Based Theory 246

IV. A COMPUTER SECURITY MODEL OF CFAA INTERPRETATION 247
A. Access Control Lists 248
B. The Computer Security Model 249
C. Justifications for the Computer Security Model 253

V. CONCLUSION 256

I. INTRODUCTION

On May 15, 2008, a federal grand jury indicted Lori Drew for violations of the Computer Fraud and Abuse Act ("CFAA") with charges alleging that Drew had created a fake MySpace[1] account for "Josh Evans," a fictitious 16-year-old boy.[2] Drew used the MySpace account to contact thirteen-year-old Megan Meier, with whom her daughter had shared a brief friendship. Meier later committed suicide at "Evans's" behest.

---

* J.D., Harvard Law School, 2010. I would like to thank Professor Phil Malone for early guidance with this Note and the editors of the *Harvard Journal of Law & Technology* for their careful eyes and helpful suggestions. Thanks also to my wife, Ina, for her unending support.

1. MYSPACE, http://www.myspace.com (last visited Dec. 21, 2010) (MySpace is a social networking website. Each user has a profile that can be used to contact other users of the website.).

2. Jennifer Steinhauer, *Missouri Woman Accused of Driving Girl to Suicide Is Indicted in California*, N.Y. TIMES, May 16, 2008, at A15.

Although Drew's conduct was reprehensible, the decision of the U.S. Attorney's Office to prosecute under the CFAA, which criminalizes "intentionally access[ing] a computer without authorization,"[3] drew criticism in both the popular press and scholarly journals.[4] The government's theory of the case based the charge on Drew's violation of MySpace's Terms of Service, rarely-read contractual terms to which MySpace users agree when they create a profile on the site. After a jury convicted Drew of misdemeanor CFAA violations, the trial judge overturned the conviction, granting Drew's motion for acquittal on the grounds that the CFAA, as applied in the case, was void for vagueness.[5] Criminalizing such violations, he wrote, would render the CFAA so broad as to "afford[] too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[6]

The Ninth Circuit also rebuffed a broad interpretation of the CFAA in *LVRC Holdings, LLC v. Brekka*.[7] There, the plaintiff's theory was that the defendant violated the CFAA when he "accessed the company computer . . . to further his own personal interests," which breached his duty of loyalty to his employer and rendered his access "without authorization" under the CFAA.[8] Noting "the care with which we must interpret criminal statutes to ensure that defendants are on notice as to which acts are criminal," the court declined to adopt the plaintiff's theory of the CFAA, finding that the CFAA failed to provide such notice.[9]

Both the prosecution in *Drew* and the plaintiff in *LVRC*, however, had precedent on their sides. "Access" and "authorization" are without statutory definitions in the CFAA, and courts have adopted multiple theories, including the contract-based theory of the *Drew* prosecutors and the agency-based theory of the *LVRC* plaintiff, in attempting to interpret these ambiguous terms.[10]

Such interpretations have some grounding in the language of the CFAA but also give the criminal statute incredible breadth. Commen-

---

3. 18 U.S.C.A. § 1030 (West 2006 & Supp. II 2008).

4. *See, e.g.*, Ryan Patrick Murray, Comment, *MySpace-ing Is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act*, 29 LOY. L.A. ENT. L. REV. 475, 475–77 (2009); Steinhauer, *supra* note 2, at A15 (noting the "highly unusual use of a federal law").

5. United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

6. *Id.* at 467 (second alteration in original) (quoting City of Chicago v. Morales, 527 U.S. 41, 64 (1999)).

7. 581 F.3d 1127 (9th Cir. 2009).

8. *Id.* at 1132.

9. *Id.* at 1135.

10. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (suggesting that breach of a confidentiality agreement would constitute a CFAA violation); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000) (employing an interpretation of the CFAA based on the RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

tators have proposed various solutions to this problem.[11] Professor Orin Kerr's influential "code-based" theory, for example, predicates violations of the CFAA on the circumvention of a computer code barrier.[12] Although commentators have noted many positive policy implications of Kerr's theory,[13] it has received some criticism[14] and has yet to be adopted by the courts.[15]

In attempting to resolve the definitions of "access" and "authorization" in the CFAA, this Note turns to a heretofore ignored discipline: computer science. In creating operating systems, computer scientists devised security models designed to control the accessibility of files in a networked system with multiple users. Understanding these models can inform our understandings of "access" and "authorization" in the CFAA, just as understanding digital rights management can inform our understanding of copyright infringement and the design of cable television systems can inform our understanding of cable theft.[16]

In particular, this Note uses the concept of access control lists in the UNIX operating system, a common security model, to illustrate the primary features of security in the computer science context. It then argues for an interpretation of "access" and "authorization" in the CFAA that is based on an understanding of these features. This approach provides many of the policy benefits of Kerr's code-based approach while also better tracking the statutory language of the CFAA.

---

11. *See, e.g.*, Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395 (2007) (proposing a CFAA interpretation theory analogous to the two-part reasonable expectation of privacy test under the Fourth Amendment outlined in *Katz v. United States*, 389 U.S. 347 (1967)); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 849–52 (2009) (proposing a hybrid theory combining code-based and contract-based approaches).

12. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1644–60 (2003). A computer code barrier is one that relies on computer code to prevent a user from exceeding his or her privileges on a computer system. *See id.* at 1644.

13. *See* Field, *supra* note 11, at 841; Nicholas R. Johnson, Recent Development, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 581–83.

14. *See, e.g.*, Winn, *supra* note 11, at 1419–21.

15. *See* United States v. Drew, 259 F.R.D. 449, 460 (C.D. Cal. 2009) ("[W]hile defining 'access' in terms of a code-based restriction might arguably be a preferable approach, no case has adopted it and the CFAA legislative history does not support it." (footnote omitted)). Kerr's theory is discussed below. *See infra* Part III.

16. *See, e.g.*, Paul J. Mass & Carl S. von Mehren, *Cable Theft: The Problem, the Need for Useful State Legislation, and a Proposed Solution for Georgia*, 35 EMORY L.J. 643, 644–49 (1986) (describing the design of cable television systems and how cable theft operates on those systems); Gideon Parchomovsky & Philip J. Weiser, *Beyond Fair Use*, 96 CORNELL L. REV. 91, 114–23 (2010) (describing various digital-rights management schemes in support of the authors' proposal regarding the fair use doctrine).

This Note proceeds in four parts. Part II describes the CFAA, its legislative history, and current judicial attempts to interpret "access" and "authorization" in the CFAA. Part III describes Kerr's code-based theory and details the scholarly and judicial reactions to it, both positive and negative. Part IV proposes a new theory of interpretation of the CFAA, based on access control lists, that can unify the diverse interpretations of the CFAA while also closely tracking the statutory language. Part V concludes.

II. THE CFAA AND JUDICIAL THEORIES OF CFAA INTERPRETATION

A. Statutory Language of the CFAA

Courts and commentators have struggled to find a clear interpretation of the CFAA.[17] The statute originated as part of the Comprehensive Crime Control Act of 1984[18] and was directed toward the deterrence of hackers, representing an attitudinal change toward the still-nascent concept of computer hacking.[19] It originally criminalized various offenses where the perpetrator "knowingly accesse[d] a computer without authorization, or having accessed a computer with authorization, use[d] the opportunity such access provides for purposes to which such authorization does not extend . . . ."[20]

Today, despite several subsequent amendments, the CFAA still retains the "access" and "without authorization" language of the original 1984 statute, and both terms remain undefined by the statute.[21] The latter half of the original requirement has since been replaced with the phrase "exceeds authorized access," which is statutorily defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[22]

Accessing without authorization or exceeding authorized access are among the elements of several provisions of the CFAA. Specifically, the CFAA provides for criminal penalties for whomever accesses a computer without authorization or exceeds authorized access and (1) by means of such conduct, obtains national security information,[23] (2) thereby obtains information contained in a financial record,

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

18. Pub. L. No. 98-473, 98 Stat. 1837 (1984).

19. H.R. REP. NO. 98-894, at 10–12 (1984).

20. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2006)).

21. 18 U.S.C.A. § 1030 (West 2006 & Supp. II 2008).

22. *Id.* § 1030(e)(6).

23. *Id.* § 1030(a)(1).

information from any department or agency of the United States, or from any protected computer,[24] or (3) does so with intent to defraud, and by means of such conduct furthers the intended fraud and obtains anything of value.[25] To fulfill the scienter requirement, accessing without authorization or exceeding authorized access must be done knowingly or intentionally for all of these provisions; section 1030(a)(5)(A), however, requires intent to "cause[] damage without authorization."[26]

"Without authorization" is used alone in several provisions of the CFAA. Section 1030(a)(3) criminalizes accessing without authorization (but not exceeding authorized access to) a nonpublic computer of the federal government,[27] and sections 1030(a)(5)(B) and (C) prohibit intentionally accessing a protected computer without authorization and recklessly causing damage, or causing damage and loss, respectively.[28]

Some sections of the CFAA do not require that one access a computer without authorization or that one exceed authorized access. Section 1030(a)(5)(A), for example, punishes knowingly causing the transmission of code that intentionally causes damage "without authorization" to a protected computer, so that the unauthorized activity is causing damage rather than accessing the computer.[29] Other sections of the CFAA punish trafficking in passwords or extortion based on a threat to a protected computer.[30]

B. Legislative History of the CFAA

Because of the inherent ambiguity in the terms "access" and "authorization," courts have often turned to the CFAA's legislative history to aid in interpreting the statute.[31] The legislative history of the CFAA does not specifically delineate the situations in which access ought to be considered without or exceeding authorization, nor does it provide conclusive evidence for any particular interpretation of "authorization" and "access" under the CFAA.[32] Congress, in fact, appar-

---

24. *Id.* § 1030(a)(2). "Protected computer" is statutorily defined to be coextensive with the reach of Congress' Commerce Clause power. *Id.* § 1030(e)(2)(B).

25. *Id.* § 1030(a)(4).

26. *Id.* § 1030(a)(1)–(5).

27. *Id.* § 1030(a)(3).

28. *Id.* § 1030(a)(5)(B)–(C).

29. *Id.* § 1030(a)(5)(A).

30. *Id.* § 1030(a)(6) (password trafficking); *Id.* § 1030(a)(7) (extortion).

31. *See, e.g.*, United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007); Clarity Servs. v. Barney, 698 F. Supp. 2d 1309, 1315 (M.D. Fla. 2010); Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007).

32. *See* Field, *supra* note 11, at 830 ("[B]ecause the legislative history contains independent support for each approach, no single approach is justified on the grounds that it represents the congressionally dictated interpretation of authorization.").

ently believed that the term "exceeds authorized access" would be "self-explanatory."[33] The legislative history does, however, provide some general principles that are useful in interpreting these terms.

First, the legislative history of the CFAA shows that the statute was intended to apply only to crimes of computer misuse and not to crimes incidentally involving the use of a computer.[34] The House Report accompanying the original 1984 statute commented that

> [i]t is noteworthy that section 1030 deals with an "unauthorized access" concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense.[35]

Professor Kerr elaborated on these two categories of computer crime, noting that "traditional crimes committed using computers raise few new issues for criminal law," and therefore do not warrant special treatment.[36] In contrast, crimes of computer misuse, which he defines as "conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks," do "pose fresh challenges for criminal law," and therefore creating a separate crime for such conduct would be appropriate.[37] The Senate Report accompanying the 1986 amendments to the CFAA expressed a similar desire not to include crimes that merely use a computer incidentally within the statute's scope.[38]

Second, motivated by concerns about hackers and the inadequate deterrent effect of existing criminal statutes, Congress intended that the CFAA fill gaps in the criminal statutory framework.[39] The 1984 House Report specifically cited, as examples of such gaps, two wire fraud cases that would not have been amenable to prosecution had computer access calls not been made across state lines.[40] The report also noted that "[i]t [was] obvious that traditional theft/larceny statutes [were] not the proper vehicle to control the spate of computer

---

33. *See* S. REP. NO. 99-432, at 13 (1986) ("Section (2)(g) establishes definitions for . . . the term 'exceeds authorized access,' and the term 'department of the United States,' all of which are self-explanatory.").

34. H.R. REP. NO. 98-894, at 32 (1984).

35. *Id.*

36. *See* Kerr, *supra* note 12, at 1603.

37. *Id.*

38. *See* S. REP. NO. 99-432, at 9 (1986) ("The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud. . . . [T]he use of the computer must be more directly linked to the intended fraud.").

39. *See* H.R. REP. NO. 98–894, at 4 (1984).

40. *Id.* at 6.

abuse and computer assisted crimes."[41] The 1996 Senate Report also cited gaps left by traditional theft and extortion laws as reasons for expanding the reach of the CFAA.[42]

At the same time, Congress, at least in early versions of the CFAA, evinced an intent to defer to traditional remedies when they would be effective. The 1984 House Report, for example, specifically instructed that the prohibitions in the CFAA ought not be interpreted to include "time stealing," urging that such behavior "should be handled privately or at the state or local level."[43] The 1986 Senate Report, in addressing the possibility that the CFAA would fail to cover some instances of computer "trespass," noted that such instances "may be subject to other criminal penalties if, for example, they violate trade secrets laws . . . ."[44]

C. The Agency-Based Theory

Since the CFAA's text and legislative history do not define either "authorization" or "access," courts have turned to other areas of the law to develop theories of interpretation of this language in the statute. Many of the judicial interpretations of the CFAA have arisen in suits brought by an employer against a disloyal or self-dealing employee.[45] Such civil suits are authorized under section (g) of the CFAA, which permits civil suits for certain violations of other sections of the CFAA.[46] Two major theories have arisen out of these cases that borrow from other areas of the law: one based on the principles of agency, and the other based on contract.

The agency theory was first advanced in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[47] In *Shurgard*, one of the plaintiff's employees, after having received an employment offer from

---

41. *Id.* at 9.

42. *See* S. REP. NO. 104-357, at 3 (1996).

43. H.R. REP. NO. 98-894, at 22 (1984) ("There is also an exclusion in this offense if the defendant has authorization to use the computers and merely abuses that authorization by means of use of 'time stealing.' This latter offense should be handled privately or at the state or local level."). "Time stealing" involves being paid for doing work, but not actually performing any work during the time period in question. *See, e.g.*, Moore v. Dolgencorp, Inc., No. 1:05-CV-107, 2006 WL 2701058, at *6 (W.D. Mich. Sept. 19, 2006) ("The act of being idle while clocked in is commonly referred to as 'stealing time.' Ordinarily this occurs when an employer clocks in but does not begin to perform her duties until some time later."). The report also excluded from criminalization the conduct of one authorized to access a government computer who "merely exceeds such authorization by the use of a computer in, for example, doing one's homework or playing computer games." Such conduct was to "be handled administratively" instead. H.R. REP. NO. 98-894, at 22 (1984).

44. S. REP. NO. 99-432, at 8 (1986).

45. *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001); Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007).

46. 18 U.S.C.A. § 1030(g) (West 2006 & Supp. II 2008).

47. 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

the defendant, sent e-mails to the defendant containing the plaintiff's trade secrets and proprietary information.[48] The court, purporting to interpret the plain language of the statute, relied upon the Second Restatement of Agency, which states that "[u]nless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[49] Because the employee in question had "bec[o]me [an] agent[] of the defendant[,] . . . [he] lost [his] authorization and [was] 'without authorization' when [he] allegedly obtained and sent the proprietary information to the defendant via e-mail."[50] *Shurgard*'s approach to interpreting "authorization" spread to other district courts as well.[51]

The agency theory gained further credibility when the Seventh Circuit adopted it in *International Airport Centers, L.L.C. v. Citrin*.[52] There, the defendant was in the employ of the plaintiff when he decided to go into business for himself. Before returning a laptop the plaintiff had given him for work, Citrin loaded a secure-erasure program onto the laptop and used it to delete all of the data on the laptop.[53] In reversing the district court's dismissal of the action under the CFAA, Judge Posner relied on agency principles and cited *Shurgard* as authority.[54] Because Citrin "resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes," his authorization to use the laptop had ceased and he was in violation of the CFAA.[55]

D. The Contract-Based Theory

Courts hearing CFAA cases in the employment context have also used a contract-based theory of interpretation.[56] The contract-based theory has also been frequently applied to cases involving violations of the terms of service of a network service provider.[57] Under the contract-based theory, once someone uses a computer in a way that vio-

48. *Id.* at 1123.

49. *Id.* at 1125 (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

50. *Id.*

51. *See, e.g.*, Int'l Sec. Mgmt. Grp., Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537, at *20–21 (M.D. Tenn. June 6, 2006); HUB Grp., Inc. v. Clancy, No. Civ.A. 05-2046, 2006 WL 208684, at *3 (E.D. Pa. Jan. 25, 2006); George S. May Int'l Co. v. Hostetler, No. 04 C 1606, 2004 WL 1197395, at *3 (N.D. Ill. May 28, 2004).

52. 440 F.3d 418 (7th Cir. 2006).

53. *Id.* at 419.

54. *Id.* at 420.

55. *Id.*

56. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (finding a CFAA violation in an employee's breach of a confidentiality agreement).

57. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).

lates his contract with the provider of his computer or network service, he has "exceeded authorized access" and therefore violates the CFAA.

Early in the development of CFAA case law, the First Circuit endorsed this theory in dicta in *United States v. Czubinski*.[58] In *Czubinski*, primarily a case dealing with wire fraud charges, an IRS employee had signed a contract acknowledging the IRS's policy of prohibiting his access to files in the IRS's database "for other than official purposes."[59] Because Czubinski had used his access to peruse files for personal purposes, the court assumed without discussion that he "unquestionably exceeded authorized access to a Federal interest computer."[60] Despite the lack of analysis in *Czubinski*, the First Circuit continued to use the contract-based theory of CFAA interpretation in future cases involving employer-employee relationships.[61]

Later, however, the contract-based theory of CFAA interpretation moved beyond the employer-employee relationship to clickwrap contracts in the Internet context.[62] For example, some district court cases have held that the use of automated software to obtain information from Internet sources exceeded authorized access when it violated the terms of use of a website or service provider.[63] Under this incarnation of the theory, a website owner or service provider can establish criminal liability through its terms of service, which are rarely read by patrons of the website or service.[64] In *America Online, Inc. v. LCGM, Inc.*, for example, the defendants, who were America Online members, used extractor software programs to acquire large numbers of e-mail addresses to which they sent unsolicited spam.[65] The court found that such actions "violated AOL's Terms of Service," which prohibited sending unsolicited bulk e-mail advertisements, "and as

58. 106 F.3d 1069 (1st Cir. 1997).

59. *Id.* at 1071 n.1.

60. *Id.* at 1078. This statement is dicta because, despite the defendant having supposedly exceeded authorized access, the court ruled for the defendant on the grounds that he did not gain any information of value through this access. *Id.* at 1078–79.

61. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (holding that plaintiff exceeded authorized access by violating his employment confidentiality agreement).

62. A clickwrap contract is one in which a computer user indicates assent with a mouse click rather than a signature. Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1597 (2006).

63. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998); *see also* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–63 (1st Cir. 2003). *But see* United States v. Drew, 259 F.R.D. 449, 462–67 (C.D. Cal. 2009) (rejecting the contract-based theory as void for vagueness).

64. *See* Kerr, *supra* note 17, at 1582 ("Few people bother to read [terms of service], much less follow them."); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 463 (2006) (noting that "people rarely read the terms of use").

65. 46 F. Supp. 2d at 448.

such [were] unauthorized."[66] Since the CFAA is primarily a criminal statute, in these contexts the contract-based theory effectively allows private network service providers to have broad discretion in choosing which uses of their services could subject a user to criminal sanctions.

E. Criticism of the Agency- and Contract-Based Theories

Because both the agency and the contract theories of CFAA interpretation provide an employer or service provider with considerable power to define criminal violations, there has been significant scholarly and judicial concern over the potential overbreadth of the CFAA under these theories. In particular, shortly after the announcement of the Lori Drew indictment, commentators added numerous articles to the scholarly literature decrying the prosecution's contract-based interpretation of the CFAA and its potential to criminalize conduct in which normal law-abiding citizens regularly engage,[67] a contention ultimately accepted by the *Drew* court.[68]

Courts and commentators have also expressed a number of concerns about the agency theory. First, some courts have held that an agency theory reading of the CFAA is contrary to the plain language of the statute.[69] According to these decisions, the *Citrin-Shurgard* line of reasoning reads the CFAA "as if it said 'exceeds authorized use' instead of 'exceeds authorized access,'"[70] an improper reading since "[n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer."[71] These courts also noted that a narrower reading of the CFAA is especially appropriate in light of the rule of lenity, which counsels construing any ambiguity against a reading favoring the government.[72]

---

66. *Id.* at 448, 450.

67. *See, e.g.*, Kristopher Accardi, Comment, *Is Violating an Internet Service Provider's Terms of Service an Example of Computer Fraud and Abuse?: An Analytical Look at the Computer Fraud and Abuse Act, Lori Drew's Conviction and Cyberbullying*, 37 W. ST. U. L. REV. 67 (2009); Johnson, *supra* note 13; Murray, *supra* note 4.

68. *See Drew*, 259 F.R.D. at 462–67.

69. *See, e.g.*, LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009); Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1314–16 (M.D. Fla. 2010) (quoting Lockheed Martin Corp. v. Speed, 81 U.S.P.Q. 2d 1669, 1673–74 (M.D. Fla. 2006)); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 934–35 (W.D. Tenn. 2008); Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007); *see also* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 611–13 (M.D. Tenn. 2010) (quoting *LVRC*, 581 F.3d at 1135, and *Black & Decker*, 568 F. Supp. 2d at 934–36).

70. *Brett Senior*, 2007 WL 2043377, at *4.

71. *LVRC*, 581 F.3d at 1135.

72. *See, e.g., id.*; *Clarity Servs.*, 698 F. Supp. 2d. at 1316. Some courts also cite the CFAA's legislative history in support of a narrower reading of "without authorization," but this is based on an apparent misreading of the legislative history. One decision, for example, cites legislative history as evincing a Congressional intent to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,' thereby

Second, the application of agency law in CFAA cases tends to render the statute's scope broad and uncertain. Under the agency theory, relatively innocent workplace conduct can constitute a violation of the CFAA simply because it does not align with the employer's interest and is therefore considered unauthorized.[73]

Finally, both the agency and contract theories have the potential to extend jurisdiction beyond the CFAA's originally intended scope, thereby disturbing established policy preferences. Specifically, the contract theory has the potential to encroach on federal copyright law and First Amendment law.[74] More generally, both theories can interfere with state regulation of employer-employee relations[75] and with established policy preferences in trade secret law.[76]

III. THE "CODE-BASED" THEORY OF INTERPRETATION

Professor Orin Kerr expressed concerns similar to these in 2003, noting that the logical extension of the contract- and agency-based

---

'remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.'" *Clarity Servs.*, 698 F. Supp. 2d at 1315 (alterations in original) (quoting S. REP. NO. 99-432, at 21 (1986)). The quoted passage, in fact, reflects only the views of two senators, not the entire committee. S. REP. NO. 99-432, at 20 (1986). Moreover, it refers specifically to section 1030(a)(3) of the CFAA and to federal employees' attempts to comply with the Freedom of Information Act, not the CFAA more generally. *Id.*

73. *Clarity Servs.*, 698 F. Supp. 2d at 1316 ("Furthermore, if an employee's authorization terminates at the moment the employee acquires an interest adverse to the employer, an employee who checks personal email at work commits a federal crime."); Field, *supra* note 11, at 845 ("[A] court that finds authorization to be totally terminated . . . would impose CFAA liability on an employee for carrying out normal employment duties . . . .").

74. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act To Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 323 (2004) (noting that the contract-based theory has "allowed website owners to utilize the CFAA to override the carefully balanced provisions of the copyright laws and improperly restrict speech in violation of the First Amendment").

75. *See* Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *5 (E.D. Pa. July 13, 2007) ("It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract.") (quoting S. REP. NO. 99-432, at 4 (1986)); *see also* Sarah Boyer, Note, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661, 688 (2009) ("It is unlikely that . . . the legislature . . . intended for claims to be brought in federal court relating to employees who view and steal information which they are permitted to have access to on a regular basis. There are already appropriate [state] remedies for such situations . . . .").

76. *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 429–30 (noting the potential for broad CFAA interpretations to disturb policy choices made in trade secret law); Boyer, *supra* note 75, at 688 (listing state trade secret law remedies as a more appropriate option than a CFAA remedy); Field, *supra* note 11, at 845–46; *see also* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) ("It would be imprudent to interpret the CFAA, in a manner inconsistent with its plain meaning, to transform the common law civil tort of misappropriation of confidential information into a criminal offense.").

theories of CFAA interpretation could potentially lead to untenable results.[77] In particular, Kerr cautioned that the agency theory could "criminalize an employee's use of an employer's computer for anything other than work-related activities,"[78] and that the contract theory places too much power in the hands of private actors to determine criminal liability.[79]

To address these problems, Kerr proposed a new "code-based" theory of interpreting "access" and "authorization" in the CFAA. This Part examines this influential code-based theory: Part III.A outlines the basics of the theory and justifications for it, and Part III.B discusses the theory's limitations.

A. The Code-Based Theory

Kerr, arguing that the current judicial theories of interpreting the CFAA are inadequate, suggested a new approach to the CFAA: reject contract- and agency-based theories of authorization entirely and only recognize CFAA violations where the potential offender has circumvented code-based restrictions.[80] Kerr explains that a user can circumvent code-based restrictions in two ways: first, the user can "trick the computer" by entering another user's username and password to log onto the system, and second, the user can exploit software vulnerabilities to elevate his privileges on the system.[81] Although other commentators have proposed different approaches to dealing with the overbreadth problem,[82] Kerr's code-based theory remains the leading academic theory of CFAA interpretation.[83]

Kerr justifies his approach on a number of grounds. First, a code-based theory would "encourag[e] users to protect their privacy in the way most likely to be technically effective . . . rather than by attempting to establish privacy via mere contractual agreements."[84] Such an

77. *See* Kerr, *supra* note 12, at 1633–34, 1650–51 (noting that the agency theory is "strikingly broad" and that the contract-based theory "grants computer network owners too much power to regulate what Internet users do").

78. *Id.* at 1634.

79. *See id*. at 1650–51. Professor Kerr has since reiterated his concerns about contract-based CFAA interpretation, noting that "criminalizing [terms of service] violations would for the most part give the government the ability to arrest anyone who regularly uses the Internet." Kerr, *supra* note 17, at 1582.

80. *See* Kerr, *supra* note 12, at 1649.

81. *Id.* at 1644–45.

82. *See supra* note 11 and accompanying text.

83. *See, e.g.*, Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2258 (2004) ("Courts would better serve both the statutory intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access."); Sara M. Smyth, *Back to the Future: Crime and Punishment in Second Life*, 36 RUTGERS COMPUTER & TECH. L.J. 18, 41 (2009) ("Professor Kerr, a leading scholar on cybercrime, has observed that regulation by code is ultimately far more effective than regulation by contract.").

84. Kerr, *supra* note 12, at 1651.

approach would draw a "more balanced line between openness and privacy [than contract-based theories]."[85]

Second, the theory draws on the common-law distinction of fraud in the inducement, which is typically not criminalized in consent-based crimes, and fraud in the factum, which typically is criminalized. Kerr argues that contract-based theories are more analogous to the former, and the code-based theory is more analogous to the latter.[86] The computer is "tricked" into thinking the user is someone else when the user circumvents code-based restrictions, but when a user merely violates a contract-based restriction, the computer rightly "believed" the user's stated identity.[87]

Third, Kerr notes that criminalizing the circumvention of code-based restrictions is more justifiable than criminalizing contract violations when considering the retributive purpose of punishment.[88] Whereas a contract violation involving a computer involves a "lesser invasion [of privacy] based on an assumption of risk," the "circumvention of code-based restrictions threatens more substantial privacy interests," akin to the "breaking in" element of burglary.[89] The code-based theory, therefore, protects against more culpable conduct than does the contract theory.

Finally, a code-based theory avoids the constitutional questions of overbreadth and void for vagueness concerns raised by a contract-based approach.[90] Unlike a contract-based approach, which would "allow a computer owner . . . to control authorization by contract as a tool to criminalize any viewpoint or status the owner wishes to target," including acts protected by the First Amendment, a code-based approach would result in a narrower interpretation of the CFAA that does not leave the unilateral power to criminalize in a computer owner's hands.[91] A contract-based approach invites void for vagueness concerns because it can criminalize violations of terms of service that are rarely read and often difficult to interpret, whereas a code-based approach avoids these concerns by ignoring the terms of service.[92] Other commentators who have praised the code-based approach have consistently lauded the theory's ability to avoid these constitutional concerns.[93]

---

85. *Id.*
86. *Id.* at 1655.
87. *Id.* at 1654–55.
88. *Id.* at 1657–58.
89. *Id.* at 1657.
90. *See id.* at 1658–59.
91. *Id.* at 1658.
92. *See id.* at 1659.
93. *See, e.g.*, Bellia, *supra* note 83, at 2258 (advocating a variant of Kerr's theory in part because "an interpretation that tied liability to activities inconsistent with [contractual] limitations would criminalize a broad range of conduct"); *see also* Field, *supra* note 11, at

B. Limitations of the Code-Based Theory

The code-based theory, however, is not without problems. The main criticism leveled against Kerr's theory is that it runs contrary to the statutory language and legislative history, which clearly distinguish "without authorization" and "exceeds authorized access."[94] Kerr suggests that policy-based considerations favor the code-based interpretation of the CFAA, but acknowledges that by applying the single criterion of code-based restriction circumvention to both "without authorization" and "exceeds authorized access," the different phrases are essentially collapsed into a single meaning.[95] Such an interpretation would run counter to the Supreme Court's admonition to courts "to give effect, if possible, to every word Congress used."[96] Kerr justifies the approach of collapsing the two statutory phrases by insisting that the alternative, "interpret[ing] the phrase 'exceeds authorized access' to include breaches of contract," would "create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment."[97] Because of the concern about overbreadth, instead of using this provision to target employee computer misuse, Kerr argues that "[t]he better approach is for legislatures to enact new criminal statutes focused directly at the problem of employee database abuse."[98] Therefore, "considerations of policy" favor a code-based interpretation of "exceeds authorized access" under this theory.[99]

Other criticisms have also been leveled at the code-based theory. In some cases, for example, the code-based theory may be underinclusive because it respects only computer code as a method of protecting one's data.[100] Such a limitation may "artificially restrict[] the

836, 843–46 (advocating Kerr's approach as the default interpretation of the CFAA and criticizing the manipulability of the agency theory).

94. *See* Winn, *supra* note 11, at 1419 ("Unfortunately, code based readings of unauthorized access are flatly inconsistent with the explicit language of an unauthorized access statute such as the CFAA, which makes a clear distinction between 'unauthorized access' and 'access in excess of authorization.'"); *see also* United States v. Drew, 259 F.R.D. 449, 460 (C.D. Cal. 2009) (noting, in dismissing Professor Bellia's variant of Kerr's theory, that "while defining 'access' in terms of a code-based restriction might arguably be a preferable approach, no case has adopted it and the CFAA legislative history does not support it." (footnote omitted)). *But see* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (noting that while "[t]he difference between 'without authorization' and 'exceeding authorized access'" is "not quite invisible," it is nevertheless "paper thin").

95. *See* Kerr, *supra* note 12, at 1662–63.

96. Nken v. Holder, 129 S.Ct. 1749, 1766 (2009) (quoting Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979)).

97. Kerr, *supra* note 12, at 1663.

98. *See id.*

99. *Id.*

100. *See* Winn, *supra* note 11, at 1420 ("[A] code based model of unauthorized access would nonetheless yield inappropriate results. Intuitively, a homeowner who simply fails to secure a personal computer should still be entitled to the protection of [the CFAA] against an unwanted intrusion into his or her home computer system.").

set of norms to which courts are permitted to look, to the norms prevalent among computer programmers — what we might call a system of 'norms by nerds.'"[101] That is, a code-based theory limits data owners' flexibility in the ways they might choose to protect their data and enshrines computer code as the only legitimate means of protection.

Kerr counters this criticism by suggesting that a code-based theory would "encourag[e] users to protect their privacy in the way most likely to be technically effective, by creating accounts and password schemes."[102] However, Kerr's argument about incentives may prove ineffective because data subjects cannot always control the protection of their data, which may be in the possession of a third party.[103] This is increasingly true with the advent of cloud computing, a practice in which one's data is stored on a server of a third party who has control over the maintenance and security of that data.[104]

Finally, the code-based theory may even be overinclusive in some cases at the margin.[105] For example, in a case where an Internet user uses BugMeNot,[106] a website storing usernames and passwords enabling Internet users to bypass free compulsory registrations, he is "tricking" the computer at the point of a code-based barrier, but does so in a way that, intuitively, few would find worthy of criminal sanction.[107]

IV. A COMPUTER SECURITY MODEL OF CFAA INTERPRETATION

Although courts have begun to take notice of the problems with the agency and contract theories of CFAA interpretation, neither the code-based theory nor its variants have found widespread acceptance in the courts. This Part introduces a new theory of interpreting the CFAA, based on insights gained from a consideration of the computer security model of access control lists.

Part IV.A introduces the concept of access control lists. Part IV.B applies the concept to interpretation of the CFAA, and Part IV.C dis-

---

101. *Id.* at 1419.

102. Kerr, *supra* note 12, at 1651.

103. Winn, *supra* note 11, at 1420 ("[D]ata-subjects are rarely in a position to force third parties to adopt effective computer security measures."). Data subjects are "the individuals who were the subject of the information contained in the computer." *Id.* at 1415.

104. *See generally* Brad Stone & Ashlee Vance, *'Cloud' Computing Casts a Spell*, N.Y. TIMES, Apr. 19, 2010, at B1.

105. *See* Kerr, *supra* note 12, at 1646 (noting that in some cases the distinction between regulation by contract and regulation by code is unclear).

106. BUGMENOT.COM, http://www.bugmenot.com (last visited Dec. 21, 2010).

107. This would not be considered access "without authorization" under the computer security model presented in Part IV, *infra*, since free compulsory registrations do not attempt to verify a user's true identity.

cusses the justifications for this computer security model of CFAA interpretation.

A. Access Control Lists

In abstract terms, an access control list ("ACL") is a mechanism used by a computer's operating system that associates a set of rights (things one can do on a computer system) with a certain subject (such as a computer user).[108] ACLs allow many people to share the same computer system, while allowing each user to have his own measure of security on the system. The ACL is associated with a certain object (such as a file) in the computer system, and specifies which subjects have which rights with regard to that particular object.[109]

If a subject attempts to assert a right with which he is not associated on a particular object, the operating system will read the ACL for that object, find that the subject does not possess the requisite right, and will prevent him from asserting that right.[110] Traditional UNIX permissions are a simplified implementation of the general concept of ACLs, and are the type examined in this Note.[111] These permissions serve as the basic computer security model for UNIX-based operating systems, a widely-used operating system in computer servers and workstations.

Traditional UNIX permissions can be visualized in the following simplified manner:

Column:	1	2	3	4	5	6	7
	-rwxr-xr--	1	user1	group1	255	Sep 30 14:06	filename

Column 7 is the name of the file with which this ACL is associated, here, *filename*. One row appears for each user who has some access rights for the file in question. The last nine characters of Column 1 represent the rights of access various users have to this file.[112] Three types of permissions are available: *r*, representing read-permission (the right to look at the file), *w*, representing write-

108. MATT BISHOP, COMPUTER SECURITY: ART AND SCIENCE 381–82 (2003).

109. *Id.*

110. *See id.* at 382.

111. *See id.* at 382–83. There are many different variants of access control mechanisms in the computer science literature. The point of this Note is not to delve into the merits of any particular computer security mechanism, but to illustrate how a widely-used concept in computer science, such as the simplified ACL model of traditional UNIX permissions, can illuminate judicial interpretations of vague words like "access" and "authorization."

112. DEBORAH S. RAY & ERIC J. RAY, VISUAL QUICKSTART GUIDE: UNIX, 99–100 (3d ed. 2007). The first dash represents only that the file is a regular file. A "d" in that position would indicate that it is a directory.

permission (the right to alter the file), and *x*, representing execute-permission (the right to run a program contained within the file).[113] The three characters *r*, *w*, and *x* always appear in that order, and a dash where one of them should be indicates the absence of that privilege.[114]

The nine characters representing access rights consist of three sets of permissions of three characters each. The first set, "rwx," is associated with a particular user whose name appears in Column 3. Thus, this first set indicates that *user1* has the right to read, write, and execute the file *filename*. The second set, "r-x," is associated with a particular group, whose name appears in Column 4 above. Thus, the second set indicates that members of the group *group1* have the right to read and to execute *filename*, but not the right to alter that file. The third set, "r--," is associated with anyone else ("other" in UNIX terminology).[115] Anyone who is not *user1* or in *group1*, therefore, has the right to look at *filename* but not the right to alter it or to run it as a program on the computer.[116]

The rights that appear in this row represent the "base ACL" entries — those that must be defined for every file in a UNIX system. The file owner can give additional users and groups read, write, or execute privileges as he deems necessary; for example, if he gave "r--" privileges to *user2* on *filename*, then that user would have the right to read the contents of *filename*, but not to alter it or to run it as a program.

B. The Computer Security Model

Three critical components of the ACL model can inform our interpretation of "access" and "authorization" in the CFAA. First, ACLs acknowledge that there are different types of access that a computer user can have: read-, write-, and execute-access.

Second, ACLs are attached to particular files. A user's rights may be different for different files on the same computer system, and different users may have different rights on the same file. Access granted for one file does not translate into access being granted for all files.

Third, the ACL model of computer security is primarily based on identity. Rights are assigned to particular users or groups.[117] Although

---

113. *Id.*

114. *See id.*

115. *Id.* at 98.

116. *Id.* Column 2 represents the number of links associated with the file, Column 5 represents the size of the file, and Column 6 represents the last modified date and time. None of this information is relevant for the purposes of this Note.

117. It is true that in a UNIX system, some usernames will not correspond to an actual person; the user "root," for example, is not an actual person, but merely a username to whom the system assigns all possible rights. The point here is not to delve into the intrica-

users authenticate their identities using a username and password combination in most implementations of ACLs, the username/password combination is exactly that: a method of authentication for the computer to recognize the user's identity. It is the user's identity, at a general level, that forms the basis of this computer security model.

I propose that courts use these insights into how computer security works in interpreting "access" and "authorization" in the CFAA.

The second and third insights above provide the theoretical bases for the two major ways in which access can be "without authorization." First, the insight that the ACL model is based on identity suggests that one's true identity ought to be a touchstone for determining whether or not access is authorized. Specifically, I propose that one method of construing access "without authorization" is as access that circumvents a mechanism intended to verify a computer user's true identity.

Most commonly, these sorts of mechanisms are the code-based restrictions that are the touchstone of Kerr's theory. A username and password combination used on a credit card's website or on an employer's computer system both verify the user's true identity because the credit card company or the employer required proof of identity from the user before giving him the access-granting combination. The BugMeNot example mentioned previously, however, would not be one of these mechanisms, since the username/password combinations stored on BugMeNot give no clues about the user's true identity. Neither would the defendant in *Drew* be guilty under this theory, as she merely created a new, fake identity instead of circumventing an identity-verification system. Circumventing CAPTCHA mechanisms would also not be a CFAA violation under this test, as they serve only to identify one as a real person, not to verify the person's true identity.[118]

Other forms of identity verification exist. A simple example is a key given to only one person. Bypassing a physical lock that this key opens would also constitute a circumvention of an identity verification mechanism. Thus CFAA protection, under this theory, could extend to

---

cies of UNIX system architecture, but to show how the general design of computer security can inform CFAA construction.

118. *But see* Kim Zelter, *Judge Clears CAPTCHA-Breaking Case for Criminal Trial*, THREAT LEVEL (Oct. 19, 2010, 2:56 PM), http://www.wired.com/threatlevel/2010/10/hacking-captcha/ (describing Judge Hayden's refusal to dismiss a CFAA charge against computer users who circumvented CAPTCHA, a mechanism designed to separate automated computer programs using the websites ("bots") from actual humans). The case also illustrates another difference between this Note's theory and Kerr's, as Judge Hayden, in support of her decision allowing the case to go forward, noted that this case included not only "allegations of breaches of contract but also of code-based restrictions." *Id.* To the extent that the defendants circumvented identity-based barriers as well, the computer security model would also hold them liable.

homeowners whose computers do not have code-based barriers to entry, but are secured behind a locked door.[119] A variety of other methods for verifying one's identity exist, such as employee key cards, Social Security numbers, and credit card numbers. Circumvention of one of these identity-verification mechanisms to gain access to a computer would constitute access without authorization.

The insight that ACLs grant file-specific access highlights the second way that access can be "without authorization." Because authorization in the ACL model is file-specific, if read, write, or execute privileges are given to a computer user on one file, and the given privileges are exploited so as to assert read, write, or execute privileges on a different file for which the user lacks any authorization, this latter access would be "without authorization." For example, in a buffer overflow attack, a user is given privileges to write to a finite piece of memory, but inputs more characters than that memory can hold.[120] This causes the extra characters to alter a different file that was not part of the original privilege grant. Such access would be without authorization, since the ACL provided the user with authorization to access the original file, but provided no authorization to access the file altered by the attack. Prohibiting this kind of access covers some of the core of computer misuse activities, such as computer hacking and computer worms and viruses.[121]

This Note also proposes that courts recognize the different types of "access" that the ACL model recognizes to give effect to the phrase "exceeds authorized access." Accordingly, a person has "exceeded authorized access" when he possesses one access right (e.g., the right of read-access) on a file, but asserts a different right on that file that he knows or should know he does not possess (e.g., altering a file, which requires write-access).[122] To make this part of the test effective in addressing insider computer crime, however, it is important to recognize an additional "access right": insiders may have a "nominal" access right to a file or set of files on a computer system. That is, there may be files on the system on which the insider could technically exercise read- or write-access privileges by virtue of his identity, but on

---

119. This addresses Winn's concerns about the "intuitive" case missed by Kerr's theory. *See* Winn, *supra* note 11, at 1420. This assumes, of course, that the potential CFAA offender actually targets information on the computer in question.

120. For more on buffer overflow attacks, see generally JAMES C. FOSTER, ET AL., BUFFER OVERFLOW ATTACKS: DETECT, EXPLOIT, PREVENT (2005). *See also* Kerr, *supra* note 12, at 1645.

121. *Cf.* Kerr, supra note 12, at 1603–04 ("Common examples [of computer misuse] include computer hacking, distribution of computer worms and viruses, and denial-of-service attacks.").

122. There may be times when a CFAA offender both "exceeds authorized access" and accesses "without authorization." For example, if the person has read privileges on a file, such as a system configuration file, but alters the file to give himself greater privileges, he has exceeded his authorized access for that file. If he then uses those privileges to access files for which he originally had no access privileges, such access is without authorization.

which the insider knows or reasonably should know that he should exercise neither. The insider's knowledge of his lack of meaningful access privileges could be imputed from a variety of sources (contract, code, or custom, for example) but must be limited to knowledge about whether he possesses access privileges. For example, a janitor's ID card could gain him access to a corporation's server room. In that room, he could exercise read- or write-access privileges on files on the servers. But it is obvious in this situation that the janitor's access to the server room does not imply access to the server files, and therefore to do so would be to exceed his authorized access.

The analogue of "nominal access" in the ACL model of computer security is a UNIX user who has read-privileges on a directory. This user can see that files exist in the directory, but unless affirmatively granted read-, write, or execute-access privileges on the individual files in the directory, he cannot do more. This sort of user is akin to one who can wander about a library and see that books line the shelves, but cannot open any of the books.

With that additional form of "access" added to the ACL model, application of the "exceeds authorized access" test becomes a bit more administrable than trying to wade through the "paper thin" distinctions courts currently have to draw between "exceeds authorized access" and "without authorization."[123] First, the court determines what type of access the insider's identity gave him to the files at issue: nominal, read, write, and/or execute access. Second, the court determines what type of access the insider exercised on the files at issue. Finally, the court determines whether that access falls within one of the categories identified in the first step.

In this respect, the ACL-based theory differs from the code-based theory because it allows a measure of CFAA regulation that could conceivably flow from contract, while cabining such regulation to the realm of actual computer misuse. Under the "exceeds authorized access" prong of the statute, an employer or website owner cannot regulate all aspects of its employees' or users' conduct simply because such conduct relates to the use of a computer. Rather, CFAA protection extends only to the employer's or website owner's limits concerning what types of access a computer user has. His restrictions on a user's ability to obtain or alter information will be enforced under the CFAA, but not those restrictions that concern what the user does if he already has the access rights to obtain or alter that information.

Finally, the insight that ACLs are file-specific counsels in favor of a fine-grained analysis of "access" in the computer context. Individual files can be password-protected, and different users can have different rights to a given file. When performing an analysis of a po-

123. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

tential CFAA violator's conduct, analyzing access to individual files is most appropriate under the computer security model.

C. Justifications for the Computer Security Model

The most important justification for the computer security model is that it better tracks the statutory language than does the code-based theory. It does so while achieving many of the policy advantages the code-based theory has over the agency- and contract-based theories. In addition, it avoids some of the miscues that the code-based theory has with respect to computer security.

In particular, the computer security model's interpretations of "access" and "authorization" acknowledge "that statutory interpretation turns on 'the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.'"[124] Acknowledging that the CFAA is a statute primarily concerned with computer security, it utilizes definitions of access and authorization prevalent in a common, traditional computer-security model.

The computer security model of CFAA interpretation also provides a concrete distinction between "unauthorized access" and "exceeds authorized access," something the code-based interpretation fails to do.[125] This interpretation of the statute enables Congress's deliberate choice of language to reflect a real distinction in judicial interpretation, giving effect to all of Congress' language.[126]

In addition, the computer security model achieves many of the policy benefits for which Kerr's theory is lauded. By limiting "unauthorized access" CFAA violations to cases in which a person has bypassed a mechanism to verify his real identity, the computer security model of interpretation avoids the widespread criminalization associated with the contract-based theory of CFAA interpretation. For example, Kerr's example of a researcher who violates a hypothetical Ku Klux Klan's Terms of Service by entering the Klan site despite not being a white supremacist would not constitute a violation under this theory.[127] The researcher has not bypassed any barrier intended to verify who he actually is or any mechanism intended to allow him to represent an identity online credibly. Neither would the user of a pro-life website who expresses pro-choice viewpoints in contravention of the website's terms of service violate the CFAA under the computer

124. *See* Nken v. Holder, 129 S.Ct. 1749, 1756 (2009) (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997)).

125. *See supra* note 94 and accompanying text.

126. *See supra* notes 95–96 and accompanying text.

127. See Kerr, *supra* note 12, at 1622–23 for a discussion of the Ku Klax Klan example.

security model.[128] He, too, has not bypassed a mechanism meant to verify his identity or to allow him to represent a true identity online.

At the same time, tying CFAA violations to barriers based not on code but rather those connected with identity avoids some of the problems associated with Kerr's theory. By adopting an interpretation based on identity, for example, the computer security model avoids the issue of "artificially restrict[ing] the set of norms to which courts are permitted to look . . . — what we might call a system of 'norms by nerds.'"[129] This interpretation also allows data owners some flexibility in the approaches they use to protect their data; it merely requires the data owner to try to verify, in some way, who is accessing the data.

The recent case involving a CFAA prosecution for circumventing CAPTCHA also raises a potential problem with a code-based interpretation.[130] CAPTCHA requires computer users to read and retype distorted images of letters and numbers; its purpose is to prevent automated computer programs from using the website in question.[131] CAPTCHA, however, is really just a code-based barrier implementing a contract-based restriction — namely, one prohibiting the use of "bots" on a website. A code-based interpretation of the CFAA curtails some of the most criticized uses of the CFAA, but only as long as technology remains unable to serve as a proxy for contract-based restrictions. Kerr, for example, illustrates the breadth of using contract-based CFAA interpretation with a website's terms of services restricting access to those eighteen or older.[132] But it is not inconceivable that a code-based test could try to distinguish people of a certain age and thereby serve as a proxy for this contract restriction.[133]

Furthermore, flexibility along these lines acknowledges that many forms of outsider attack on computer systems happen not at the code level, but at the human level.[134] Hackers often find that because people are inevitably in the computer security chain, it is easier to use an unwitting accomplice to gain unauthorized access to a computer system than it is to attempt to subvert the computer's cryptography.[135] Such "social engineering" attacks merely trick a help-line operator or some other agent of the data owner into thinking that the person with

---

128. See *id.* at 1658–59 for a discussion of this example.

129. Winn, *supra* note 11, at 1419.

130. See *Men Plead Guilty in Ticket Conspiracy*, N.Y. TIMES, Nov. 19, 2010, at B8 for a description of the case.

131. *See id.*

132. *See* Kerr, *supra* note 12, at 1646.

133. The "Mosquito," for example, emits a high-pitched noise audible to teenagers, but not most adults. *See* Melissa Block, *Teens Turn 'Repeller' into Adult-Proof Ringtone*, NPR, May 26, 2006, http://www.npr.org/templates/story/story.php?storyId=5434687.

134. *See, e.g.*, BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 266–69 (2000).

135. *See id.* at 267 (recounting one hacker's testimony before Congress that he "was so successful in [the social engineering] line of attack that [he] rarely had to resort to a technical attack").

whom the agent is talking is someone authorized to access the computer in question.[136] Although a code-based approach might fail to criminalize attacks on computer systems aimed at the human weak link, the computer security model's identity-based approach retains the ability to criminalize such offenses.

The computer security model's treatment of insider access retains the substantive definition of "exceeds authorized access" as when a user has one access privilege on a computer system, but exercises another that he knows or should know that he does not have. By focusing on the access privileges the potential CFAA offender reasonably should know that he does not possess, this test acknowledges that it may be impractical or perhaps even impossible to erect identity-based barriers at every point at which an insider could commit a CFAA violation.[137] It therefore imputes criminal liability not based on an organization's ability to erect identity- or code-based barriers against its own insiders, but based on the knowledge of the offender that he is engaged in a type of access for which he does not possess the requisite type of privilege.

The computer security model's definition of "exceeds authorized access" also tracks the statutory definition of that phrase. To "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"[138] corresponds to the traditional UNIX privileges of read-access (obtaining information) and write-access (altering information). The computer security model, therefore, also has the benefit of tracking the statutory definition of "exceeds authorized access" by reading it as prohibiting a user who has one privilege (e.g., "obtain" or "alter") from exercising one he does not possess.

It is true that this definition of insider computer crime may miss some of the cases that courts have held to be CFAA violations under the agency theory. The trade secret theft in *Shurgard*, for example, may fall outside of the scope of the CFAA under a computer security model interpretation.[139] These areas, however, merely constitute the use of a computer for impermissible purposes, and, as noted above, have been the subject of considerable policy debate.[140] Interpreters of the CFAA are well-advised to leave these policy judgments undisturbed.

The computer security model returns the focus of the CFAA to the original purpose for which it was meant: computer misuse. By

---

136. *Cf. id.* at 266.

137. *See id.* at 48 ("Most computer security measures . . . try to deal with the external attacker, but are pretty much powerless against insiders. . . . An insider knows how the systems work and where the weak points are.").

138. 18 U.S.C.A. § 1030(e)(6) (West 2006 & Supp. II 2008).

139. *See supra* Part II.C.

140. *See supra* Part II.E.

limiting insider violations to situations in which an insider asserts an access privilege which he knows he does not have, the computer security model appropriately ignores situations covered by other law and criminalizes only situations in which the computer access itself — as opposed to the use of the data — was beyond authorization.

V. CONCLUSION

Both courts and commentators have struggled to find a consistent interpretation of the CFAA. Some judicial interpretations have given rise to an extraordinarily broad CFAA and given private actors remarkable discretion to define what is criminal. The prominent code-based academic theory, on the other hand, attempts to rein in the broad judicial interpretations of the CFAA, but does so at the price of reading out the importance of some of Congress's language.

By exploring the common computer security model of access control lists, this Note has sought to put forth a theory that retains many of the code-based theory's policy benefits while still tracking the statutory language of the CFAA. Doing so provides sufficient flexibility to criminalize the computer misuse that intuitively ought to be considered criminal while also excluding those areas of computer use already covered by other areas of the law.