2010

Vagueness Challenges to the Computer Fraud and Abuse Act

Orin S. Kerr

Article

Vagueness Challenges to the Computer Fraud and Abuse Act

Orin S. Kerr†

INTRODUCTION

In 1984, Congress enacted a narrow statute designed to criminalize unauthorized access to computers.[1] That law, generally referred to as the Computer Fraud and Abuse Act (CFAA),[2] has been substantially modified five different times.[3] The statute's reach has been expanded each time, resulting in a remarkable cumulative effect.[4] The statute, originally designed to criminalize only important federal interest computer crimes,[5] potentially regulates every use of every computer in the United States and even many millions of computers abroad. Statutory amendments and the increasing computerization of American society have combined to render the CFAA one of the most far-reaching criminal laws in the United States Code.

This Article argues that the remarkable scope of the CFAA requires courts to adopt narrow interpretations of the statute in light of the void-for-vagueness doctrine. Violations of the

---

† Professor, George Washington University Law School. By way of full disclosure, I provided pro bono representation to Lori Drew, the defendant in one of the cases discussed. All of the viewpoints expressed in this Article represent my personal opinion. Thanks to Eugene Volokh, Paul Ohm, and Chris Slobogin for helpful comments and discussions of these topics.

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

2. Technically speaking, the Computer Fraud and Abuse Act was the 1986 amendment to 18 U.S.C. § 1030. *See* Pub. L. No. 99-474, 100 Stat. 1213 (1986). However, it is common to refer to § 1030 as a whole as the Computer Fraud and Abuse Act. I adopt that convention here.

3. *See infra* Part I.

4. *See infra* Part I.

5. *See* 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985) (criminalizing certain computer misuse relating to national security, financial records, and government property).

CFAA generally require an unauthorized access—either an "access without authorization" or an act that "exceed[s] authorized access."[6] The meaning of unauthorized access is remarkably unclear, however, with courts and commentators disagreeing sharply as to how much conduct counts and what principle of authorization the statute adopts.[7] The void-for-vagueness doctrine requires courts to adopt narrow and clear interpretations of unauthorized access to save the constitutionality of the statute.[8] The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional. Such interpretations would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process of the law.[9]

This Article focuses on two recent criminal prosecutions that have been based on very broad interpretations of unauthorized access. In *United States v. Drew*,[10] the government argued that violations of Terms of Service (TOS) render access to a computer unauthorized.[11] In *United States v. Nosal*,[12] the government argued that an employee who accesses an employer's computer with illicit motives to hurt the employer accesses that computer without authorization.[13] Both theories must be rejected. Because the statute would be unconstitutionally vague under either theory, courts must construe the CFAA narrowly as excluding such theories to avoid invalidating the statute.

More broadly, this Article predicts a new, judicially focused phase of the CFAA's development. Since the statute's initial enactment in 1984, most of the action relating to the CFAA's meaning has come from Congress.[14] Congress has revisited the

---

6. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1616 (2003) (reviewing 18 U.S.C. § 1030 provisions).

7. *See id.* ("The courts that have interpreted 'access' and 'without authorization' have offered a broad range of interpretations that run the gamut from quite narrow to extraordinarily broad.").

8. *See, e.g.*, City of Chicago v. Morales, 527 U.S. 41, 56 (1999) (noting that a criminal statute may be invalidated if it "authorize[s] . . . arbitrary and discriminatory enforcement").

9. *See infra* Part II.A.

10. 259 F.R.D. 449 (C.D. Cal. 2009).

11. *Id.* at 457.

12. No. CR 08-00237 MHP, 2009 WL 981336 (N.D. Cal. Apr. 13, 2009).

13. *Id.* at *4.

14. *See infra* Part I.

statute repeatedly, while courts have generally declined to scrutinize the meaning of the statute's key terms.[15] That will change. The CFAA has become too broad to apply without careful attention to the vagueness doctrine. With Congress having largely abandoned its task of defining what the statute prohibits,[16] the courts are now likely to step in and fill the gap. The meaning of unauthorized access will become a question for the courts rather than Congress.[17]

This Article contains two Parts. Part I explains just how broad the CFAA has become. The short history of the CFAA provides a case study in how readily Congress can expand criminal liability in areas of developing technology. Congress has given the Executive remarkably broad discretion to charge cases that the Executive thinks should be charged. The core legislative question of what conduct should be criminalized has been all but abandoned. Part II argues that Congress's failure to limit the CFAA requires courts to limit the Act using the constitutional vagueness doctrine. The remarkable scope of the CFAA requires courts to adopt a narrow interpretation of the core prohibition of access "without authorization" and "exceeding authorized access."

I. THE EVER-EXPANDING COMPUTER FRAUD AND ABUSE ACT

This Part traces the history of the Computer Fraud and Abuse Act. It focuses on how Congress has repeatedly expanded the CFAA's scope and abolished the statutory limits on its application. It starts with the first version of § 1030 enacted in 1984. It then covers each major amendment through 2008. The history shows a clear and uniform trend of expansion. The law that began as narrow and specific has become breathtakingly broad.

A. COMPREHENSIVE CRIME CONTROL ACT OF 1984

In October 1984, Congress passed a massive omnibus crime bill known as the Comprehensive Crime Control Act

15. *See* Kerr, *supra* note 6, at 1617 ("[S]everal recent decisions point toward remarkably expansive interpretations of unauthorized access.").

16. *See infra* Part II.B.

17. The Supreme Court's recent scrutiny of the "honest services" statute, 18 U.S.C. § 1346, may make such a future much more likely. *See* Mark Sherman, *Court Skeptical of Federal Anti-Fraud Law*, DENV. POST, Dec. 8, 2009, http://www.denverpost.com/business/ci_13949538.

(CCCA).[18] Among the hundreds of provisions in the CCCA was the first federal computer crime statute, found in section 2102(a).[19] The new statute, to be codified at 18 U.S.C. § 1030, established three new federal crimes. All three crimes applied to a person who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend . . . ."[20] Each offense then added requirements that collectively limited the statute to three specific scenarios: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers.[21]

The first offenses protected classified national security secrets. Codified at § 1030(a)(1), it prohibited a person from accessing a computer without authorization to obtain classified national security information with the intent or reason to believe that the information would be used to injure the United States.[22] The second crime protected personal financial information. Codified at § 1030(a)(2), it prohibited a person from accessing a computer without authorization to obtain information contained in a financial record of a financial institution or in a file of a consumer reporting agency.[23] The third offense protected U.S. government computers. Codified at § 1030(a)(3), it prohibited a person from accessing a computer without authorization and then using, modifying, destroying, or disclosing information from a U.S. government computer if so doing affected the computer's operation.[24] All three statutes were tailored to a specific government interest: national security, financial records, and government property.

B. COMPUTER FRAUD AND ABUSE ACT OF 1986

Congress significantly expanded the statute just two years later when it passed Pub. L. No. 99-474, formally known as the Computer Fraud and Abuse Act, the amendments that gave

18. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976.

19. *See id.* § 2102(a), 98 Stat. at 2190.

20. 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985). For the sake of simplicity, I will refer to this language as simply a prohibition on "access without authorization" or "unauthorized access."

21. *Id.*

22. *Id.* § 1030(a)(1).

23. *Id.* § 1030(a)(2).

24. *Id.* § 1030(a)(3).

§ 1030 its name.[25] The 1986 Act added three new prohibitions codified at § 1030(a)(4)–(6).[26] Section 1030(a)(4) prohibited unauthorized access with intent to defraud; essentially, the traditional crime of wire fraud committed using a computer.[27] Section 1030(a)(5) prohibited accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either $1,000 or more of aggregated loss or impairing a medical diagnosis, treatment, or care of one or more individuals.[28] Section 1030(a)(6) prohibited trafficking in computer passwords.[29]

All three of the new statutes contained new definitions designed to delineate which computers were covered under the new federal prohibitions. Both § 1030(a)(4) and § 1030(a)(5) were limited to "Federal interest" computers. Roughly speaking, federal interest computers were those used either by the U.S. government or financial institutions, or as part of a multistate computer network.[30] The statute defined "Federal interest" computers as follows:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or
>
> (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State[.][31]

Note that the definition in subset (A) largely tracks the coverage of the original 1984 statute, whereas the definition in subset (B) covers new ground. That new ground was quite limited, however, as it effectively required an interstate offense over an interstate network.[32] At a time when use of the Internet remained in its infancy, few crimes would be included in its reach.

---

25. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213.

26. 18 U.S.C. § 1030(a)(4)–(6) (Supp. IV 1987).

27. *Id.* § 1030(a)(4).

28. *Id.* § 1030(a)(5).

29. *Id.* § 1030(a)(6).

30. *Id.* § 1030(e)(2).

31. *Id.*

32. *See* S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482 (detailing the preference of the Senate Judiciary Committee to limit federal jurisdiction over computer crime to instances involving a "compelling federal interest" or where "the crime itself is interstate in nature").

C. VIOLENT CRIME CONTROL AND LAW ENFORCEMENT ACT OF 1994

The next material amendments to § 1030 occurred eight years later with the passage of the Violent Crime Control and Law Enforcement Act of 1994.[33] This law was another omnibus criminal law bill that contained hundreds of sections, passed at the behest of President Bill Clinton, and most famous at the time for the federal assault weapons ban.[34] Section 290001 of the Act provided amendments subtitled the Computer Abuse Amendments Act of 1994.[35] The 1994 amendments expanded § 1030(a)(5), the computer damage statute, to apply to computer damage incurred accidentally and even without any negligence.[36] The statute also added a civil provision to allow victims of § 1030 crimes to recover damages against wrongdoers.[37]

D. ECONOMIC ESPIONAGE ACT OF 1996

The next expansion of § 1030 occurred in 1996 as title II of the Economic Espionage Act, in a subtitle known as the National Information Infrastructure Protection Act of 1996.[38] This law dramatically expanded the statute in three different ways.

The first change vastly expanded the scope of § 1030(a)(2), which was originally limited to unauthorized access that obtained financial records from financial institutions, card issu-

---

33. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796.

34. *See generally* William Jefferson Clinton, *Remarks on Signing the Violent Crime Control and Law Enforcement Act of 1994*, 20 U. DAYTON L. REV. 567 (1995); Bill McCollum, *The Struggle for Effective Anti-Crime Legislation—An Analysis of the Violent Crime Control and Law Enforcement Act of 1994*, 20 U. DAYTON L. REV. 561 (1995).

35. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097.

36. *Id.* § 290001(b), 108 Stat. at 2097–98.

37. *Id.* § 290001(d), 108 Stat. at 2098. At the time, the civil provision stated:

> Any person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

18 U.S.C. § 1030(g) (1994).

38. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

ers, or consumer reporting agencies.[39] The 1996 amendments expanded the prohibition dramatically to prohibit unauthorized access that obtained *any information of any kind* so long as the conduct involved an interstate or foreign communication.[40] Prior legislative history emphasized the tremendous reach of this new amendment by clarifying that obtaining information included simply reading it.[41] Since most forms of unauthorized access will reveal information to read, even if it is only the prompts or graphic interface provided to those with access, the new § 1030(a)(2) effectively criminalized all interstate hacking.

Second, the 1996 amendments added new provisions to the computer damage prohibition, added a new felony enhancement to § 1030(a)(2), and added a computer extortion statute at § 1030(a)(7). The new computer damage section expanded the list of harm that counted as damage: beyond monetary damage (raised to $5,000 from $1,000) and impairing a medical diagnosis or treatment, the law added causing "physical injury to any person" or "threaten[ing] public health or safety" to the list.[42] The felony enhancements to § 1030(a)(2) turned a misdemeanor violation into a felony if the offense was conducted in furtherance of any crime or tortious act, if it was conducted for purposes of financial gain, or if the value of the information obtained exceeded $5,000.[43]

Finally, the 1996 amendments expanded the statute dramatically by replacing the decade-old category of "Federal interest" computers with the new category of "protected computer[s]." As enacted in 1996, a protected computer was defined as a computer:

> (A) exclusively for the use of a financial institution of the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication[.][44]

---

39. *See* 18 U.S.C. § 1030(a)(2) (Supp. II 1996).

40. *See id.* § 1030(a)(2)(C).

41. *See* S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (noting that "obtaining information" in the statute includes "mere observation of the data").

42. 18 U.S.C. § 1030(e)(8)(A)–(D).

43. *Id.* § 1030(c)(2)(B)(i)–(iii).

44. *Id.* § 1030(e)(2).

The critical difference between a "Federal interest" computer and a "protected computer" was that the former required computers in two or more states, while the latter merely required a machine "used" in interstate commerce.[45] Notably, the statute did not specify whether "use" in interstate commerce referred to use in the context of the charged offense or rather use in the general sense. However, the change in the definition changed the scope of the statute dramatically. Because every computer connected to the Internet is used in interstate commerce or communication,[46] it seems that every computer connected to the Internet is a "protected computer" covered by 18 U.S.C. § 1030.

E. USA PATRIOT ACT OF 2001

The USA Patriot Act, passed soon after the terrorist attacks of September 11, 2001, also contained provisions expanding the scope of 18 U.S.C. § 1030.[47] The amendment appears in section 814 of the Act, labeled "Deterrence and Prevention of Cyberterrorism."[48] The most significant amendment to the scope of § 1030 in the Patriot Act was the expanded definition of "protected computer" to include computers located outside the United States.[49] Specifically, the amendment added those computers "located outside the United States that [are] used in a manner that affects interstate or foreign commerce or communication of the United States."[50] As we will see shortly, the terms "affects interstate commerce" is a term of art in Federal Commerce Clause law.[51] The amendment effectively extended the CFAA to as many foreign computers as the Commerce Clause allows.[52]

---

45. *Compare* 18 U.S.C. § 1030(e)(2)(B) (Supp. IV 1987) (defining a "Federal interest" computer as one "which is one of two or more computers used in committing the offense, not all of which are located in the same State"), *with* 18 U.S.C. § 1030(e)(2)(B) (Supp. II 1996) (defining a "protected computer" as one "which is used in interstate or foreign commerce or communication").

46. *See infra* notes 65–73 and accompanying text.

47. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

48. *Id.* § 814, 115 Stat. at 382.

49. *See* 18 U.S.C. § 1030(e)(2)(B) (Supp. II 2004).

50. *Id.*

51. *See infra* notes 60–64 and accompanying text.

52. *See infra* notes 60–65 and accompanying text.

Second, the Patriot Act added new triggers for the felony violations of § 1030(a)(5). The Act added damage to any computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security" to the list of harms that, if caused, trigger the felony computer damage provisions of § 1030(a)(5).[53]

F. IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT OF 2008

The most recent expansions to 18 U.S.C. § 1030 were enacted in September 2008 as title II of the Former Vice President Protection Act,[54] subtitled the Identity Theft Enforcement and Restitution Act. This amendment once again expanded the scope of the CFAA, and it did so in subtle ways that have a surprisingly large impact.

Three changes are most notable. First, the statute once again expanded the scope of § 1030(a)(2) by removing the requirement of an interstate communication.[55] Under the new § 1030(a)(2)(C), *any* unauthorized access to *any* protected computer that retrieves *any* information of *any* kind, interstate or intrastate, is punishable by the statute.[56] The statute also once again expanded the reach of § 1030(a)(5), creating misdemeanor liability for harms under $5,000 and adding once again to the list of felony triggers—this time, harming ten or more computers, designed to cover cases of botnets.[57]

The third significant expansion is the most subtle but the most far-reaching. The 2008 amendments once again expanded the definition of "protected computer."[58] Therefore, the present definition includes any computer that is:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United

53. 18 U.S.C. § 1030(a)(5)(B)(v); *see* § 814(a)(4), 115 Stat. at 382.

54. Former Vice President Protection Act of 2008, Pub. L. No. 110-326, 122 Stat. 3560.

55. *See id.* § 203, 122 Stat. at 3561.

56. *See id.*

57. *See id.* § 204, 122 Stat. at 3561–62.

58. 18 U.S.C.A. § 1030(e)(2) (West 2000 & Supp. 2009).

> States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.][59]

It is easy to miss the change. Congress added "or affecting" in the first phrase of § 1030(e)(2)(B), replacing the definition that included computers "used in interstate or foreign commerce or communication" with computers "used in *or affecting* interstate or foreign commerce or communication."[60]

But sometimes two words make a big difference. The phrase "affecting interstate commerce" is a term of art that signals congressional intent to cover as far as the Commerce Clause will allow.[61] Modern Commerce Clause doctrine gives the federal government the power to "regulate purely local activities that are part of an economic 'class of activities' that have a substantial effect on interstate commerce."[62] In application, that allows Congress to regulate any class of economic activities that when aggregated can impact interstate commerce.[63] In *Gonzales v. Raich*, for example, the Supreme Court allowed Congress to regulate entirely local activities like growing marijuana for home use on the theory that the aggregate effect of homegrown marijuana could have an impact on the supply and demand for marijuana in the national economy.[64] No matter how local the marijuana growing, Congress could still regulate it.

This excursion into Commerce Clause doctrine explains just how broad the current version of "protected computer"[65] has become, and by extension, just how far the CFAA reaches. Because the definition now applies to both computers in the United States and abroad that are used in or affecting interstate commerce or communication, every computer around the world that can be regulated under the Commerce Clause is a "protected computer" covered by 18 U.S.C. § 1030.[66] This does not merely cover computers connected to the Internet that are actually "used" in interstate commerce.[67] Instead, it applies to

---

59. *Id.*

60. *Compare* 18 U.S.C. § 1030(e)(2)(B) (2006), *with* 18 U.S.C.A. § 1030(e)(2) (West 2000 & Supp. 2009) (emphasis added).

61. *See* United States v. Chesney, 86 F.3d 564, 571 (6th Cir. 1996).

62. Gonzales v. Raich, 545 U.S. 1, 17 (2005) (quoting Perez v. United States, 402 U.S. 146, 152 (1971)).

63. *See id.*

64. *See id.* at 18–19.

65. 18 U.S.C.A. § 1030(e)(2) (West 2000 & Supp. 2009).

66. *See id.*

67. *See id.*

all computers, period, so long as the federal government has the power to regulate them.[68]

The 2008 amendments of the CFAA and the nearly limitless scope of modern Commerce Clause doctrine mean it may be no exaggeration to say that a "protected computer" now just means a "computer."[69] Computers are ubiquitous as tools of modern commerce, and intrastate use of computers often has interstate effects. Computer data created and used in one state is easily moved across state lines, and breaches of computer security among intrastate computers can have an effect on computer use generally.[70] It would be premature to rule out Commerce Clause challenges to intrastate use of computers in *all* cases. If limits exist, however, they likely are very narrow ones.[71] Perhaps the only identifiable exclusion from the scope of protected computers is a "portable hand held calculator, or other similar device,"[72] exempted from the definition of "computer." Everything else with a microchip or that permits digital storage is, arguably, covered.[73]

II. THE VOID-FOR-VAGUENESS DOCTRINE AND UNAUTHORIZED ACCESS STATUTES

The vast scope of the current version of 18 U.S.C. § 1030 places tremendous pressure on the particular meaning of "access without authorization" and "exceeds authorized access," the two closely related prohibitions at the heart of the CFAA.[74] As I have written elsewhere, the meaning of these terms remains surprisingly uncertain.[75] These terms may only prohibit

68. *See id.*

69. 18 U.S.C.A. § 1030(e)(1) defines a "computer" as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]

70. *See, e.g.*, Press Release, U.S. Attorney's Office, Dist. of Mass., Former Inmate Sentenced for Hacking Prison Computer (Dec. 22, 2009), *available at* http://www.cybercrime.govt/janoskosent.pdf (illustrating how a person hacking one prison computer can have a significant effect on the lives of hundreds of government officials outside prison walls).

71. *Cf.* United States v. Jeronimo-Bautista, 425 F.3d 1266, 1273–74 (10th Cir. 2005).

72. *See* 18 U.S.C.A. § 1030(e)(1).

73. *Cf.* United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005).

74. *See* 18 U.S.C.A. § 1030(a)(2).

75. *See* Kerr, *supra* note 6, at 1597.

accessing a computer in a way that circumvents code-based restrictions such as password gates.[76] Alternatively, they may prohibit accessing a computer in a way that violates a contract or widely shared norms of computer use.[77] Exactly what is an "access," and what makes an "access" unauthorized, is presently unclear.

This Part shows how courts should apply the constitutional void-for-vagueness doctrine to require narrow interpretations of unauthorized access in the CFAA. The void-for-vagueness doctrine requires legislatures to say what is prohibited.[78] It prohibits legislatures from essentially delegating the decision as to what is criminal to the executive branch.[79] The remarkable growth of the CFAA has made the void-for-vagueness doctrine a critical weapon for challenging overbroad interpretations of the Act. As the statute grows in scope, the constitutional void-for-vagueness doctrine places increasing pressure on courts to adopt narrow interpretations of access and authorization. Only a narrow construction of the statute can save its constitutionality.[80]

This Article focuses on two specific applications featured in recent criminal prosecutions. The first is whether an Internet user violates the CFAA when she violates Internet Terms of Service (TOS), a question raised by *United States v. Drew*.[81] The second application is whether an employee violates the CFAA when he accesses his employer's network for personal reasons contrary to the employer's interest, a question discussed by the court in *United States v. Nosal*.[82] In both cases, the void-for-vagueness doctrine should force the conclusion that neither conduct is prohibited by the CFAA. The acts of violating TOS and acting contrary to an employer's interest, without more, should not constitute either an access without authorization or exceeding an authorized access. In my view, *Drew* and *Nosal* are easy cases. At the same time, they are illustrative easy cases. The arguments in *Drew* and *Nosal* should be re-

76. *See id.* at 1619–21.
77. *See id.* at 1622–24.
78. *See* discussion *infra* Part II.A.
79. *See* discussion *infra* Part II.A.
80. *See* discussion *infra* Part II.B.
81. 259 F.R.D. 449, 451 (C.D. Cal. 2009).
82. No. CR 08-00237 MHP, 2009 WL 981336, at *4 (N.D. Cal. Apr. 13, 2009).

peated in other settings to pressure the courts to adopt narrow interpretations of the CFAA.

A. INTRODUCTION TO THE VOID-FOR-VAGUENESS DOCTRINE

The void-for-vagueness doctrine is rooted in the Due Process Clause.[83] It includes two distinct and largely independent tests: fair notice and discriminatory enforcement.[84] The fair notice test asks whether the law is "so vague and standardless that it leaves the public uncertain as to the conduct it prohibits."[85] If a law is so vague that a person cannot tell what is prohibited, "it leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case."[86]

Importantly, the fair notice standard assumes that the public knows the legal precedents construing the statute's terms. For example, if a criminal statute uses a term of art, or employs language that has been construed narrowly by the courts, that legally recognized meaning applies and can save the statute from being vague.[87] As a result, the fair notice inquiry focuses on what a lawyer, judge, or legally informed juror might think the law means rather than a member of the public.[88] This focus may seem odd, as most people aren't lawyers and don't hire them to analyze vague criminal laws. The focus serves an important purpose, however: it permits courts to address vagueness concerns by interpreting a vague law in a clear way.[89] The clear interpretation becomes the new meaning.[90] As a result, courts confronted with a vague law can either invalidate the law or construe it narrowly to cure the vagueness.[91]

---

83. United States v. Williams, 128 S. Ct. 1830, 1845 (2008).

84. *See* City of Chicago v. Morales, 527 U.S. 41, 56 (1999).

85. Giaccio v. Pennsylvania, 382 U.S. 399, 402 (1966).

86. *Id.* at 402–03.

87. *See* Wainwright v. Stone, 414 U.S. 21, 22–23 (1973) ("For the purpose of determining whether a state statute is too vague and indefinite to constitute valid legislation 'we must take the statute as though it read precisely as the highest court of the State has interpreted it.'").

88. *See id.*

89. *See id.*

90. *See id.*

91. *See, e.g.*, City of Chicago v. Morales, 527 U.S. 41, 64, 92, 112 (1999) (invalidating a Chicago ordinance under a broad reading while the dissent would have upheld the statute under a narrow reading).

Coates v. City of Cincinnati illustrates a law that failed the fair notice test.[92] A Cincinnati, Ohio ordinance made it a criminal offense for "three or more persons to assemble" on sidewalks and to "there conduct themselves in a manner annoying to persons passing by."[93] The Supreme Court of Ohio had not adopted a narrow construction of the word "annoying." The Ohio court had written that "the word 'annoying' is a widely used and well understood word; it is not necessary to guess its meaning."[94] The U.S. Supreme Court held that the statute, so construed, was unconstitutionally vague:

> Conduct that annoys some people does not annoy others. Thus, the ordinance is vague, not in the sense that it requires a person to conform his conduct to an imprecise but comprehensible normative standard, but rather in the sense that no standard of conduct is specified at all. As a result, 'men of common intelligence must necessarily guess at its meaning.'[95]

The ordinance failed to say in what way, and by what standard, the conduct was annoying. As construed by the Ohio Supreme Court, the ordinance had effectively failed to say what was prohibited.[96]

The second void-for-vagueness test addresses discriminatory enforcement.[97] Under this test, a statute is unconstitutionally vague if it does not "establish minimal guidelines to govern law enforcement,"[98] so that the law "encourage[s] arbitrary and discriminatory enforcement."[99] The constitutional flaw in this setting is not what the law means to a potential violator, but rather how the law is or would be enforced by the police in practice.[100] The inquiry focuses on how much discretion the law gives the police.[101] If the law leaves its enforcement to the "whim of any police officer,"[102] it is unconstitutionally vague for its failure to provide minimum guidelines.[103] This can be re-

92. Coates v. City of Cincinnati, 402 U.S. 611, 616 (1971).

93. *See id.* at 611 (quoting CINCINNATI, OHIO, CODE § 901-L6 (1956)).

94. *Id.* at 612 (quoting City of Cincinnati v. Coates, 255 N.E.2d 247, 249 (Ohio 1970)).

95. *Id.* at 614 (quoting Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926)).

96. *See id.*

97. *See, e.g.*, Kolender v. Lawson, 461 U.S. 352, 357 (1983).

98. *Id.* at 358.

99. *Id.* at 357.

100. *See id.* at 358.

101. *See* Shuttlesworth v. City of Birmingham, 382 U.S. 87, 90 (1965).

102. *Id.*

103. *See id.*

lated to the fair notice vagueness test, in that a law that is unclear on its face may also give the police too much power to enforce it as officers wish.[104] But it focuses on a different question: how the police would enforce the law rather than whether the law is unclear.[105]

Kolender v. Lawson provides an example of a law that did not establish minimal guidelines to govern law enforcement.[106] A California statute required persons stopped by the police to give the officer "credible and reliable" identification and to account for his presence.[107] The Supreme Court struck down the statute on the ground that the standard gave the police too much power to pick and choose whom to arrest.[108] According to the Court, the law gave "no standard for determining what a suspect has to do in order to satisfy the requirement to provide a 'credible and reliable' identification."[109] As a result, the law vested "virtually complete discretion in the hands of the police to determine whether the suspect has satisfied the statute and must be permitted to go on his way in the absence of probable cause to arrest."[110]

B. VOID FOR VAGUENESS AND THE CFAA

This section argues that the void-for-vagueness doctrine requires courts to adopt a narrow interpretation of unauthorized access. The basic argument has two stages. First, courts must adopt a clear theory of what makes access unauthorized to provide sufficient notice as to what is prohibited. The interpretation must make clear to potential wrongdoers what is prohibited so they can do more than merely guess at the meaning of the statute.[111] Second, courts must adopt a narrow theory to avoid encouraging discriminatory enforcement.[112] The remarkable breadth of this statute requires courts to adopt a clear and narrow interpretation of unauthorized access to provide fair warning to individuals and to limit government discretion.

---

104. *Compare Kolender*, 461 U.S. at 358, *with Shuttlesworth*, 382 U.S. at 90.
105. *Compare Kolender*, 461 U.S. at 358, *with Shuttlesworth*, 382 U.S. at 90.
106. *Kolender*, 461 U.S. at 358.
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*
111. *See* Giaccio v. Pennsylvania, 382 U.S. 399, 402–03 (1966).
112. *See Kolender*, 461 U.S. at 358.

The core difficulty is that access and authorization have a wide range of possible meanings. In particular, the definition of authorization is notoriously uncertain.[113] What makes access to a computer unauthorized—either "without authorization" or "in excess of authorization?"[114] Is it unauthorized if the computer owner tells the person not to access the computer? Is it unauthorized if the access is against the interests of the computer owner? Is it unauthorized if the access violates a contract on access?[115] Presently the answer is remarkably unclear.[116] To be sure, there are some obvious cases. If *A* guesses *B*'s password, and logs into *B*'s e-mail account to read *B*'s e-mail, *A*'s access to the computer is clearly unauthorized: *A* has hacked into *B*'s account. If hacking is not unauthorized access, nothing is. But the courts have not yet settled on the broader question of what exactly makes access without authorization or in excess of authorization.[117] The statute simply does not define what makes access "without authorization." As a result, there are a surprising number of instances in which citizens cannot know whether their conduct amounts to an unauthorized access.[118] The statutes simply do not say what the terms mean, and no precedents have provided clear answers.[119]

The requirement that a statute must "establish minimal guidelines to govern law enforcement"[120] requires courts to reject the broader possible theories of authorization. The CFAA is breathtakingly broad.[121] The statute essentially makes it a fed-

113. *See* United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009) (noting "there is a considerable amount of controversy" as to the meaning of "without authorization"); *see* Kerr, *supra* note 6, at 1622–24 (discussing ambiguities in the concept of authorization to access computers).

114. *See* Kerr, *supra* note 6, at 1630 ("Although courts have struggled to distinguish between these two phrases, prohibitions against exceeding authorization appear to reflect concerns that users with some rights to access a computer network could otherwise use those limited rights as an absolute defense to further computer misuse.").

115. *See id.* at 1637–40 (describing cases in which two parties are "bound by a contract that implicitly or explicitly regulates access to a computer, and one side uses the computer in a way that arguably breaches the contract").

116. *See id.* at 1640–42 (discussing the courts' difficulties with interpreting "unauthorized access").

117. *Id.*

118. *See* Kerr, *supra* note 6, at 1598–99.

119. *See generally id.* at 1624–32 (discussing the conflicting definitions of "access" and "authorization" in case law).

120. Smith v. Goguen, 415 U.S. 566, 574 (1974).

121. *See* A. HUGH SCOTT & KATHLEEN BURDETTE SHIELDS, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 4-3 (Supp. 2006)

eral crime to access without authorization or exceed authorized access to any computer at all anywhere in the world.[122] As a result, the meaning of unauthorized access determines the scope of the statute.[123] Courts must adopt a meaning of unauthorized access that does not let the police arrest whomever they like. This means that courts must reject interpretations of unauthorized access that criminalize routine Internet use or that punish common use of computers. An interpretation that criminalizes routine computer use would give the government the power to arrest any typical computer user. Courts must adopt a narrower view to limit the discretion of law enforcement authorities to bring charges at their whim.

The scope of the CFAA is the heart of the problem. When the CFAA was a narrow statute, it was constitutionally permissible to adopt a broad construction of access and lack of authorization.[124] Computers were relatively rare at the time, and only certain types of computers used in particular ways were covered by the statute.[125] That is not true today. Today, computers are everywhere. Nearly every computer is a "protected computer" under the statute.[126] Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of "computer."[127] That category can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm

("Congress has steadily increased the breadth of the coverage of the CFAA . . . . Thus, invasion of or damage to any computer connected to the Internet, or to the information on those computers . . . is now a federal crime under 18 U.S.C. § 1030.").

122. *See id.* at 4-25 to -26.

123. *See id.* at 4-16 ("[T]he notion of 'accessing' a computer is central to the CFAA . . . .").

124. *See id.* at 4-3 ("The original 1984 version of the statute was limited to protecting federal government computers, defense or foreign relations information of the United States, and information of a financial institution or credit reporting agency.").

125. *See* Kerr, *supra* note 6, at 1641 (describing the development of computer technology since the 1970s).

126. *See* 18 U.S.C.A. § 1030(e)(2)(B) (West 2000 & Supp. 2009) ("[T]he term 'protected computer' means a computer . . . which is used in or affecting interstate or foreign commerce or communication . . . .").

127. *Id.* § 1030(e)(1) ("[T]he term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . .").

clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers.[128] Plus, the definition of "computer" arguably extends to flash drives, CDs, DVDs, and other electronic storage devices, as the definition "includes any data storage facility . . . directly related to or operating in conjunction with" an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions."[129]

Under the current version of 18 U.S.C. § 1030, any action that accesses such a device or exceeds authorized access, perhaps even anywhere in the world, will trigger liability under the statute so long as *some* information—*any* information—is obtained.[130] There is no requirement of an interstate network, an interstate communication, or an interstate computer.[131] Regardless of what interpretation Congress may have intended for access and authorization in the 1980s, and regardless of what early cases have held, the current version of 18 U.S.C. § 1030 requires a narrow and clear interpretation of unauthorized access to avoid constitutional vagueness.

C. *UNITED STATES V. DREW* AND TERMS OF SERVICE

The role of vagueness doctrine in the proper interpretation of the CFAA is particularly clear in the case of Internet Terms of Service violations. This issue arose in the recent prosecution of Lori Drew, a case in which I served as co-counsel for Drew and raised these arguments myself in the District Court.[132]

---

128. *Id.* ("[T]he term 'computer' . . . does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device . . . ."). Perhaps future courts will construe "other similar device" broadly to exempt common items that have been computerized, but as of now we have no sign that courts will take that approach. *See, e.g.*, United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (adopting a broad interpretation of § 1030(e)(1), limited only by its explicit exceptions).

129. 18 U.S.C.A. § 1030(e)(1).

130. *Id.* § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . . .").

131. SCOTT & SHIELDS, *supra* note 121, at 4-25 (explaining that the broad definition of protected computer combined with a global Internet means that home computers with online access fall within the CFAA's reach).

132. *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

The Lori Drew case has been widely reported in the national media,[133] and I suspect many readers will be familiar with it. Drew helped create a false profile on the MySpace.com social networking site in order to contact a neighbor of the Drew family, thirteen-year-old Megan Meier.[134] The profile falsely claimed to belong to an attractive sixteen-year-old boy named Josh Evans.[135] The apparent purpose of creating the fake profile was to have "Evans" communicate with Meier and to learn what Meier was saying about Drew's daughter.[136] "Evans" communicated with Meier for a few weeks until "he" told Meier that he was moving away.[137] On October 16, 2006, less than a month after the "Josh Evans" account was created, Meier received an instant message from "Evans" saying that he no longer liked her and that "the world would be a better place without her in it."[138] Later that same day, Meier committed suicide.[139]

The government's theory in the *Drew* case was that the creation of the "Josh Evans" profile had violated the TOS of MySpace.com, and that the TOS violation rendered the access to MySpace's computers either without authorization or in excess of authorization.[140] The TOS stated that its provisions governed access rights to MySpace:

> This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the Services. By using the Services, you agree to be bound by this Agreement . . . . You are only authorized to use the Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the Website and discontinue use of the Services immediately.[141]

---

133. *See, e.g.*, Times Topics: Lori Drew, http://topics.nytimes.com/top/reference/timestopics/people/d/lori_drew/index.html?scp=1-spot&sq=Lori%20Drew&st=cse (last visited Apr. 12, 2010).

134. *Drew*, 259 F.R.D. at 452.

135. *Id.*

136. Christopher Maag, *A Hoax Turned Fatal Draws Anger But No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23 ("In a report filed with the Sheriff's Department, Lori Drew said she created the MySpace profile of 'Josh Evans' to win Megan's trust and learn how Megan felt about her daughter.").

137. *Drew*, 259 F.R.D. at 452.

138. *Id.*

139. *Id.*

140. Indictment at 6, *Drew*, 259 F.R.D. 449 (No. 08-00582), 2008 WL 2078622.

141. *Drew*, 259 F.R.D. at 454.

The TOS then offered a series of restrictions that were relevant to the creation of the Evans profile. It required that "all registration information you submit is truthful and accurate," that the user will not solicit "personal information from anyone under 18" and that the user cannot include "a photograph of another person that you have posted without that person's consent."[142] The government argued that the group that had created and used the Josh Evans profile had violated these terms—they were not really a teenage boy named Josh Evans, they solicited information from Meier, and they included a picture of a boy alleged to be Josh Evans without the boy's permission.[143] The government argued that these TOS violations rendered the access to MySpace's computers either without authorization or in excess of authorization.[144]

The defense argued two main points.[145] First, as a matter of statutory construction, the TOS did not govern authorization.[146] Regardless of what the TOS said, MySpace had in fact given authorization to access its computers by creating the Josh Evans account and allowing the group to send and receive messages using it.[147] Second, as a matter of constitutional law, an interpretation of unauthorized access that included violating website TOS would render the statute void for vagueness.[148] As a result, the statute had to be interpreted more narrowly to exclude mere TOS violations.[149]

Judge Wu agreed with the defense and granted the motion to dismiss.[150] On one hand, Judge Wu reasoned that he saw no reason as a matter of statutory interpretation to construe the

142. *Id.*

143. Indictment, *supra* note 140, at 6–7.

144. *Id.* at 9.

145. *See* Notice of Motion; Motion to Dismiss Indictment for Vagueness, *Drew*, 259 F.R.D. 449 (No. 08-00582), 2008 WL 2848959.

146. *Id.*

147. *See* Supplement to Rule 29 Motion at 4, *Drew*, 259 F.R.D. 449 (No. 08-00582), 2008 WL 5381025 ("If a person or business actually *grants* permission for the act, conditioned on some understanding that turns out to be false, then the act is *still authorized* for the purposes of criminal law.").

148. *Drew*, 259 F.R.D. at 464 ("[I]f a website's terms of service controls what is 'authorized' and what is 'exceeding authorization' . . . section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will."); *see* Reply to Government Response to Defense Rule 29 at 5–6, *Drew*, 259 F.R.D. 449 (No. 08-00582), 2009 WL 54313 (outlining the defense's arguments regarding the fair warning canons).

149. *Drew*, 259 F.R.D. at 464–65.

150. *Id.* at 468.

statute narrowly.[151] Because the language of the TOS specifically denied rights to access the computer in ways that violated the TOS, it ordinarily should govern authorization.[152] On the other hand, Judge Wu recognized that this reading could not be adopted under the void-for-vagueness doctrine.[153] If any violation of any TOS rendered access unauthorized, then the statute would encourage discriminatory enforcement.[154] It "would result in transforming § 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals."[155] According to Judge Wu:

> It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publicly available for access and use. However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered from the more serious (*e.g.* posting child pornography) to the more trivial (*e.g.* posting a picture of friends without their permission). All can be prosecuted. Given the "standardless sweep" that results, federal law enforcement entities would be improperly free "to pursue their personal predilections."[156]

On the other hand, a ruling that some TOS-governed authorization but others did not would render the statute void for vagueness for its failure to provide sufficient notice as to what was prohibited.[157]

Judge Wu's holding that an interpretation of unauthorized access that includes all TOS violations would render the statute unconstitutionally vague is clearly correct. TOS are written extremely broadly to give providers a right to cancel ac-

---

151. *See id.* at 459–60.

152. *Id.* at 462 ("[T]he vast majority of the courts (that have considered the issue) have held that a website's terms of service/use cannot define what is (and/or is not) authorized access vis-a-vis that website.").

153. *Id.* at 465 ("[B]y utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner—in essence—the party who ultimately defines the criminal conduct. This will lead to further vagueness problems.").

154. *See id.* at 463–65 (noting the ability of website owners to "unilaterally amend . . . the terms with minimal notice to users" and stating that statutes that do not define the criminal offense with sufficient definiteness encourage discriminatory enforcement).

155. *Id.* at 466.

156. *Id.* at 467 (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)) (citation omitted).

157. *Id.* at 463.

counts and not face any liability.[158] Because they are written so broadly, most Internet users violate them regularly. Violating the TOS is the norm, complying with them the exception. Indeed, Meier had violated the TOS as well.[159] Meier had created her account in violation of the TOS stating that no one under the age of fourteen could use MySpace.[160] Even the cofounder of MySpace, Tom Anderson, violated the TOS in creating his profile.[161] In late 2007, it was revealed that Anderson's profile misrepresented his age in an apparent effort to seem younger.[162]

The key point is that no one actually treats TOS as if they govern access rights. Few people bother to read them, much less follow them. Internet users routinely click through such agreements on the assumption that they are legal mumbo jumbo that don't impact what users are allowed to do.[163] As a result, criminalizing TOS violations would for the most part give the government the ability to arrest anyone who regularly uses the Internet. Agents could set up a webpage, dontvisithere.gov, announce that no one could visit the webpage, and then swoop in and arrest anyone who did.

In my view, *Drew* was an easy case. The government's theory was an enormous stretch. It is no surprise that both state and federal prosecutors where both Drew and Meier were

158. *See generally* Jessica R. Friedman & Gerry A. Fifer, *Website Development and Hosting Agreements for Terms of Service, in* REPRESENTING THE NEW MEDIA COMPANY 2000, at 467, 476–81 (2000) (PLI Patents, Copyrights, Trademarks, & Literary Property, Course Handbook Series No. 587, 2000) (providing website owners with an overview of points to consider in drafting a Terms of Service agreement).

159. *See Drew*, 259 F.R.D. at 466.

160. *Id.*

161. The Terms of Service require that "all registration information you submit is truthful and accurate." *Id.* at 454.

162. Jessica Bennett, *Is Age Just a Number?*, NEWSWEEK, Nov. 5, 2007, http://www.newsweek.com/id/62330 ("According to public documents obtained by NEWSWEEK—including professional license information, voter registration and utility and telephone service applications—Anderson is five years older than he claims.").

163. *See* Jacob Rogers, *A Passive Approach to Regulation of Virtual Worlds*, 76 GEO. WASH. L. REV. 405, 420 (2008) ("The typical consumer does not read a terms-of-service contract because the costs of doing so (primarily the time spent reading) outweigh the benefits, which are most often essentially zero."). The forewoman of the Lori Drew jury appears to be a rare exception. When she spoke to the press after the trial, she expressed the view that she "always" read Terms of Service and that a person "absolutely" should be held liable if they are "lazy" and do not read the entire agreement. *See* Kim Zetter, *Jurors Wanted To Convict Lori Drew of Felonies, but Lacked Evidence*, WIRED, Dec. 1, 2008, http://www.wired.com/threatlevel/2008/12/jurors-wanted-t/.

located declined prosecution on the ground that no crime was committed.[164] At the same time, the basic strategy in *Drew* can be repeated in other cases that are less clear. Congress has largely given up defining what the CFAA covers and placing limits on its scope. That task now falls to the courts. The courts now must use vagueness arguments to chisel away at the edifice of the CFAA until the resulting scope of the statute is both relatively clear and relatively narrow.

D. *UNITED STATES V. NOSAL* AND DISLOYAL EMPLOYEES

The second important theory of the CFAA that implicates the void-for-vagueness doctrine is its use in the employment setting. In the last five years, cases applying the CFAA to allegedly disloyal employees have become by far the most common type of CFAA case. Most of these cases are on the civil side of the docket, and they have sharply divided the lower courts.[165] But the CFAA's role in regulating employee use of an employer's computer network also arose in a recent criminal prosecution, *United States v. Nosal*.[166]

David Nosal was a high-level executive at a large company, Korn/Ferry International (KFI), which provides executive recruitment services.[167] In October 2004, Nosal left KFI and signed a noncompete agreement.[168] According to the government, however, Nosal secretly made a deal with KFI employee Becky Christian and Nosal's former assistant, known in the case only by the initials "J.F."[169] Under the deal, Christian and J.F. would use their KFI accounts to obtain trade secrets and other confidential information from KFI and would provide them to Nosal.[170] Nosal could then use the information to start a competitor business.[171] Nosal and Christian were charged with a range of crimes, among them violations of 18 U.S.C.

---

164. *See* Ashley Surdin, *Woman Guilty of Minor Charges for MySpace Hoax*, WASH. POST, Nov. 27, 2008, at A10.

165. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964–65 (D. Ariz. 2008) (detailing the split among courts over the meaning of the word "authorization" in the CFAA).

166. No. CR 08-00237 MHP, 2009 WL 981336, at *3 (N.D. Cal. Apr. 13, 2009).

167. *Id.* at *1.

168. *Id.*

169. *Id.*

170. *Id.*

171. Superseding Indictment at 2–3, *Nosal*, 2009 WL 981336 (No. CR 08-00237 MHP).

§ 1030(a)(4).[172] Section 1030(a)(4) is the computer fraud provision of the CFAA.[173] It prohibits unauthorized access to a computer to further a scheme to defraud.[174]

The *Nosal* case is the first criminal prosecution that tests whether an employee violates the CFAA by accessing his employer's computer for personal reasons. In the civil setting, some courts have taken the view that an employee's authorization is implicitly bounded by whether he is acting as the employer's agent.[175] By acting contrary to the employer's interest and accessing the employer's computer in a way designed to hurt the employer, the thinking goes, that access is unauthorized.[176] In contrast, other courts have rejected the agency theory of the CFAA.[177] Those courts have reasoned that an employee who is authorized to access an employer's computer is, well, authorized to use the employer's computer.[178] The eventual or attempted misappropriation of the employer's data does not render the access unauthorized.[179]

---

172. *Nosal*, 2009 WL 981336, at *2.

173. 18 U.S.C.A. § 1030(a)(4) (West 2000 & Supp. 2009).

174. *Id.* ("Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . shall be punished . . . .").

175. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (distinguishing this case in what appears to be dicta by finding that "Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship"); *see also* Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 823–24 (2009) (outlining the agency-based interpretation of authorization and the Seventh Circuit's adoption of it in *Citrin*).

176. *See* Kerr, *supra* note 6, at 1632–37 (describing several cases in which employees exceeded authorized use by using "their employers' computers in ways that exceeded the scope of their employment").

177. *See Nosal*, 2009 WL 981336, at *5.

178. *See id.*

179. The *Nosal* court cited a line of cases in which the courts "generally reasoned that the CFAA is intended to punish computer hackers, electronic trespassers and other 'outsiders' but not employees who abuse computer access privileges to misuse information derived from their employment." *Id.* at *5. *See, e.g.*, Bridal Expo, Inc. v. van Florestein, No. 4:08-cv-03777, 2009 WL 255862, at *10 (S.D. Tex. Feb. 3, 2009); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933–34 (W.D. Tenn. 2008); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1341–43 (N.D. Ga. 2007); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *2–4 (E.D. Pa. July 13, 2007); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL

The defense in *Nosal* argued that the court should adopt the narrower construction as a matter of statutory interpretation and therefore dismiss the indictment.[180] Judge Patel recognized the division in the case law, but she opted for the broader interpretation.[181] That choice didn't last for very long. A few weeks after the district court decision in *United States v. Nosal*,[182] the Ninth Circuit rejected the broader interpretation in a civil case, *LVRC Holdings v. Brekka*,[183] which therefore has controlling effect on further proceedings in the *Nosal* prosecution. But the more interesting question is how the void-for-vagueness arguments could have been used by *Nosal* to argue in favor of the narrower interpretation.

Does the void-for-vagueness doctrine require courts to reject the broader agency view of authorization in the CFAA? I believe it does. To see why, we need to recognize that many employees routinely use protected computers in the course of their day for a tremendously wide range of functions. Employee use of computers tracks employee attention spans. Attention wanders, and our computer use wanders with it. We think, therefore we Google. As a result, it is rare, if not inconceivable, for every keystroke to be clearly and strictly in the course of furthering an employment relationship. The best employee in a larger company might spend thirty minutes writing up a report, and then spend one minute checking personal e-mail and twenty seconds to check the weather to see if the baseball game after work might be rained out. He might then spend ten more minutes working on the report followed by two minutes to check the online news. Over the course of the day, he might use the computer for primarily personal reasons dozens or even hundreds of times.

The checking of personal e-mail, viewing a weather report, or loading up a new site is the modern equivalent of getting up to stretch, or to talk briefly with a coworker. It is downtime, time spent recharging mental batteries. And yet because it uses a computer, it is also technically "accessing" a protected computer.[184] Each visit, each checking, and each viewing involves

---

2683058, at *5 (M.D. Fla. Aug. 1, 2006); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

180. *Nosal*, 2009 WL 981336, at *4.

181. *Id.* at *5–6.

182. *Id.*

183. 581 F.3d 1127, 1132–35 (9th Cir. 2009).

184. *See* 18 U.S.C.A. § 1030(e)(2) (West 2000 & Supp. 2009) (defining "protected computer").

entering a command into a computer network and retrieving information from a server. Assuming that using a computer to retrieve information "accesses" that computer,[185] the interpretation that courts give to lack of authorization ends up determining whether these keystrokes amount to federal crimes.

The interpretation of unauthorized access must give employees sufficient notice of what is criminal and also provide sufficient guidelines to law enforcement to avoid discriminatory enforcement. Interpreting the CFAA to prohibit employee access of an employer's computer for reasons outside the employment context runs afoul of that command. First, the theory gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited. The key consideration seems to be motive, but the employee has no way to determine what motives are illicit—and in the case of mixed motives, what proportion are illicit. Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line? If use of an employer's computer directly contrary to the employer's interest is required, how contrary is directly contrary? Is mere waste of the employee's time enough? The cases generally deal with the dramatic facts of an employee who accessed a sensitive and valuable database to gather data that could be used to establish a competing company. But how sensitive does the database need to be? How valuable does the data need to be? The agency theory of liability under the CFAA does not appear to answer these questions. It does not answer what kind of employee conduct is actually prohibited, and it therefore does not provide sufficient notice to employees as to what is prohibited to satisfy the void-for-vagueness doctrine.

To the extent the agency theory prohibits *any* access to an employer's computer that does not further the employer's interests, and is therefore outside the scope of employment, the law does not "establish minimal guidelines to govern law enforcement" and therefore "encourage[s] arbitrary and discriminatory enforcement."[186] Employees routinely use their employers' computers for personal reasons. The question is not *whether* employees use employers' computers for personal reasons; it is how *often* and for how *long*. But under the agency theory of au-

185. *See supra* note 123 and accompanying text.

186. Kolender v. Lawson, 461 U.S. 352, 357–58 (1983) (citing Smith v. Goguen, 415 U.S. 566, 574 (1974)).

thorization, the question of how often and how long is irrelevant. A single unauthorized use, even if just for an instant, amounts to either an access without authorization or exceeding authorized access. As a result, a broad agency theory of authorization would turn millions of employees into criminals. It would give the government the power to arrest almost anyone who had a computer at work, much like the government's theory in the Lori Drew case would give the government the power to arrest almost anyone who used MySpace.com.

CONCLUSION

The CFAA is a remarkably broad statute, and the recent prosecutions in *Drew* and *Nosal* show that federal prosecutors eventually will try to exploit the breadth and ambiguity of the statute to bring prosecutions based on aggressive readings of the statute. Vagueness doctrine should be a major tool to fight those aggressive readings. The doctrine prohibits overly unclear or overbroad interpretations of the statute, and it should push courts to adopt reasonably clear and reasonably narrow interpretations of unauthorized access.

Faced with the uncertainty of the new world of computer crimes, Congress has opted for very broad and unclear prohibitions. The pressure to interpret the CFAA to avoid vagueness concerns may lead to a new court-created jurisprudence of the meaning of unauthorized access. The void-for-vagueness doctrine will force courts to answer the questions that Congress has failed to answer. The pressure to interpret the CFAA in a constitutional way will force courts to say what unauthorized access means for employees, for Internet service users, and for other computer users in the many different settings in which the CFAA might apply.

Exactly what approaches the courts will allow and which they will reject is unclear. *Drew* and *Nosal* are easy cases. More difficult cases remain. But it seems fair to predict that we are entering into a new phase of the development of the CFAA. Congress has largely given up, and the courts are now likely to step in. In coming years, the meaning of unauthorized access—and with it, the meaning of § 1030—is likely to be seen as a constitutional question for the courts rather than a statutory question for Congress.