Notre Dame Journal of Law, Ethics & Public Policy

Volume 30 | Issue 1 Article 7

2016

Note, The Unconstitutionality of the Computer Fraud and Abuse Act

Michael C. Mikulic

THE UNCONSTITUTIONALITY OF THE COMPUTER FRAUD AND ABUSE ACT

MICHAEL C. MIKULIC*

This Note deals with 18 U.S.C. § 1030, otherwise known as the Computer Fraud and Abuse Act ("CFAA"). The CFAA is the federal computer hacking statute. This Note discusses the statute's history, purpose, and the recent circuit split regarding its interpretation. There are two ways to interpret the statute: one is broad and the other narrow. The broad interpretation, which many, if not a majority of, circuit courts adopt, extends criminal liability to potentially millions of unsuspecting Americans. The approach is wholly unfair and unreasonable. But more than that, this Note argues that the broad interpretation is unconstitutional. There are two reasons why. First, it is void for vagueness in that it fails to provide notice of what conduct is prohibited. Second, it is an impermissible private delegation of lawmaking power, allowing contract drafters the power to delineate criminal sanctions. After arguing that the statute is unconstitutional, this Note proposes one way to limit the statute's wide scope: presidential discretionary non-enforcement.

I. A CAUTIONARY TALE

Andrew Auernheimer (hereinafter "weev")[1] is responsible for Apple's "worst security breach."[2] In 2010, he and another colleague obtained the identity and email addresses of all purchasers of the then newly released iPad 3G.[3] That number exceeded 114,000 people.[4] Weev then gave all the information to a blogger at *Gawker*. Both men exposed "thousands of A-listers in finance, politics, and media, from New York Times Co. CEO Janet Robinson to Diane Sawyer of ABC News

* Candidate for Juris Doctor, Notre Dame Law School, 2016; Master of Arts, Vanderbilt University, 2013; Bachelor of Arts, Vanderbilt University, 2012. I would like to thank my Note advisor, Professor Richard Garnett, for all his invaluable advice and direction on this Note.

1. Weev is a hacker, an Internet troll, and, according to his Twitter account, a "former political prisoner." *See generally* Adam Penenberg, *The Troll's Lawyer*, BACKCHANNEL (Jan. 5, 2014), https://medium.com/backchannel/the-trolls-lawyer-8bf7b2283; @rabite, TWITTER, https://twitter.com/rabite (last visited Jan. 8, 2015).

2. Ryan Tate, *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*, GAWKER (June 9, 2010, 4:50 PM), http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed.

3. According to Tate,

> the specific information exposed in the breach included subscribers' email addresses, coupled with an associated ID used to authenticate the subscriber on AT&T's network, known as the ICC-ID. ICC-ID stands for integrated circuit card identifier and is used to identify the SIM cards that associate a mobile device with a particular subscriber.

Id. Each SIM card has an ICC-ID. *Id.*

4. *Id.*

to film mogul Harvey Weinstein to Mayor Michael Bloomberg. It even appears that [then] White House Chief of Staff Rahm Emanuel's information was compromised."[5] This was no small breach.

Perhaps more surprising than the sheer number of victims was just how easy it was for the two men to obtain the information. All it took was simple arithmetic.[6] When weev logged into the AT&T website to set up an unlimited data plan account, he noticed his email address was already auto-filled in the window. Apparently, AT&T used a number on his SIM card to identify him. Weev realized that the URL on the address bar of the webpage was linked to this number.[7] If he tweaked the numbers of the URL, the website would respond as if a different SIM card was being used. The website would then prepopulate the page with other people's email addresses.[8] Delighted, weev developed an "account slurper," a computer bot that would quickly enter numbers into the address bar to generate more webpages exposing more email addresses.[9] Simple arithmetic.

Federal authorities arrested weev shortly thereafter. He was charged with violating the Computer Fraud and Abuse Act (hereinafter "CFAA").[10] Weev already knew about the CFAA, and his act was a stunt. Now, he would take the case to court, telling his lawyer, "We don't want to get a small sentence here. Because if we get a big sentence, it's going to be better for the press, for the cause, for everything."[11] This was weev's chance to take up the cause, and challenge the CFAA.

The CFAA is a computer hacking statute. It is both a criminal and civil law.[12] Courts interpret the statute in two ways: broadly or narrowly.[13] Under the broad interpretation, the law applies to millions of people both inside and outside of the United States.[14] Two theories justify the broad reading: contract and agency. Under contract theory, the law punishes persons who use a computer in a way that violates a contract or terms of service.[15] Under agency theory, the law punishes any employee who acts contrary to the interests of the employer.[16] Under either approach, the broad reading imposes use restrictions on persons, punishing anyone who uses a computer wrongly.

---

5. *Id.*
6. *See* Penenberg, *supra* note 1.
7. *Id.*
8. *Id.*
9. *Id.*
10. *See generally* 18 U.S.C. § 1030 (2012).
11. *See* Penenberg, *supra* note 1.
12. *Compare* 18 U.S.C. § 1030(c) (providing criminal punishment), *with* 18 U.S.C. § 1030(g) (providing civil remedies to victims).
13. *Compare* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (adopting broad interpretation approach), *with* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (adopting narrow interpretation approach). *See infra* Part IV for a discussion on the circuit court split regarding whether to read the statute broadly or narrowly.
14. *See infra* Part V for why the broad approach makes the CFAA one of the most far-reaching criminal laws.
15. *See infra* Part IV for an in-depth discussion of contract theory.
16. *See infra* Part IV for an in-depth discussion of agency theory.

Weev's case reached the United States Court of Appeals for the Third Circuit.[17] One of the central issues on appeal was whether weev exceeded his authority to use AT&T's website.[18] Weev argued he did not because he accessed AT&T's publically accessible webpage to gather the information.[19] Luckily, the court never decided the CFAA question because it dismissed the case on procedural grounds.[20] But what would have happened had the CFAA count been at stake?[21] Had the court utilized the broad interpretation approach, weev surely would have lost. He would have violated the website's terms of service, which forbade other users from accessing personal information of others. He would then have been criminally liable for accessing information that AT&T negligently provided online to the public. If anything, AT&T, not weev, should have been held responsible for providing confidential information publically online.[22]

Although weev was able to emerge unscathed, the case still illustrates the major problems of the CFAA. It is unduly broad and unfair. Millions of Americans can potentially commit a federal crime like weev every time they access information that was publically available online. Or, they can be criminally liable for using a computer in a way that is contrary to their employer's interest. Under no circumstance should checking Facebook at work amount to a federal crime. Thus, this Note argues for a way to strike down the statute. It argues the statute is unconstitutional for two reasons: it is void for vagueness, and it is an impermissible private delegation of lawmaking power. Each reason is related to an infringement upon on the due process rights of Americans.

This Note proceeds in five Parts. Part II will discuss the CFAA in detail. It first discusses the statute's originally limited purpose and then traces the development of the statute's enormous growth through the last two decades. Part III explains the statute's current statutory framework, detailing the different sections of the law. Part IV introduces the sharp circuit split with regard to the interpretation of the statute. It explains both the broad and narrow interpretations. It will explain why courts decide to adopt one approach over the other. Part V then argues the narrow interpretation is the correct approach. Under a

17. United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2012).

18. *Id.* at 533.

19. For a complete recounting of weev's argument, see his appellate brief. Brief for Petitioner-Appellant, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2012) (No 13-1816), https://www.eff.org/files/filenode/weevs_opening_brief.pdf.

20. *Auernheimer*, 748 F.3d at 541.

21. Interestingly enough, weev might have won. Recently, the Third Circuit decided a case using the narrow interpretation approach. *See* CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116 (3d Cir. 2015). However, the ruling was not precedential. *Id.*

22. What is more, weev did nothing criminal with the email addresses he took from AT&T. He sent the information to *Gawker*, which in turn, published an article giving weev credit for the security breach. All identifiable information was kept confidential the whole time. Weev only wanted credit for the security breach, nothing more. *See* Penenberg, *supra* note 1.

broad reading, the statute is unconstitutional. First, it is void for vagueness because it does not provide fair notice to the people or minimal guidelines to law enforcement, leading to potentially discriminatory enforcement. Second, the statute is an impermissible private delegation of lawmaking power. Congress does not have authority to give its lawmaking power to private parties, especially when it comes to making criminal laws. Part VI concludes the Note.

II. THE HISTORY OF THE CFAA

The birth of the CFAA took place in 1984 with the passing of the Comprehensive Crime Control Act (hereinafter "CCCA").[23] Since that year, the statute has been amended multiple times.[24] With each and every amendment, the statute gradually became broader and broader in scope. Professor Tim Wu of Columbia Law School calls the growth a "nightmare."[25] Professor Orin Kerr of George Washington University Law School details the nightmare. The statute "potentially regulates every use of every computer in the United States and even many millions of computers abroad."[26] According to a United States Census Bureau study, 83.8% of American households have a computer.[27]

Congress originally passed the CCCA to respond to a growing problem: an inability to punish persons who committed computer misuse crimes. The CCCA was a statute primarily aimed at prohibiting one common computer misuse crime called "unauthorized access."[28] The current CFAA has primarily remained an unauthorized access statute.[29]

---

23. Comprehensive Crime Control Act of 1984, Pub L. No. 98-473, 98 Stat. 1837 (1984).

24. Since 1984, the statute has been amended nine times. According to a Department of Justice manual, "As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008." U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 2 (2d ed. 2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

25. Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

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

27. THOM FILE & CAMILLE RYAN, U.S. CENSUS BUREAU, ACS-28, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2013, at 2 (2014), http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf.

28. A United States Department of Justice manual teaching federal prosecutors about the CFAA has this to say about the statute's origins:

> In response, Congress included in the Comprehensive Crime Control Act of 1984 provisions to address the unauthorized access and use of computers and computer networks. The legislative history [of the statute] indicates that Congress intended these provisions to provide "a clearer statement of proscribed activity" to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access." Congress did this by making it a felony to access classified information in a computer without authorization and making it a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer.

U.S. DEP'T OF JUSTICE, *supra* note 24, at 1.

29. For a more in-depth discussion on computer misuse crimes, see *infra* Part III.

With the advent of the computer age, people committed new crimes that did not fit the traditional criminal law mold. Laws like trespass, burglary, and theft proved ill-suited to extend to computer misuse laws.[30] The reason, Professor Kerr explains, is because the statutes "remain[ed] closely tied to the physical world rather than a virtual one . . . . Indeed, it appears that no criminal prosecution has ever used burglary or general trespass statutes to prosecute computer misuse."[31] Congress needed to update the law to the virtual world to protect intangible property interests in a computer.[32]

The CCCA was originally narrow in scope. It established three new federal crimes: (1) hacking into a computer to obtain national security secrets, (2) hacking into a computer to obtain personal financial records, and (3) hacking into a government computer.[33] As such, all three crimes were tailored to the specific government interests of protecting national security, government and private financial records, and government property. Without a doubt, the law was "[c]onsciously narrow in scope and aimed at hackers."[34] However, due to this very reason, Congress updated the law two years later to punish more types of digital crimes.

In 1986, Congress passed a series of amendments to the CCCA that gave the current statute its name—the Computer Fraud and Abuse Act.[35] The amendments established three more federal crimes.[36] Section 1030(a)(4) prohibited unauthorized access with intent to defraud.[37] 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.[38] Section 1030(a)(6) prohibited trafficking in computer passwords.[39] These federal crimes were limited to "Federal interest" computers, which were

30. *See* ORIN S. KERR, COMPUTER CRIME LAW 13–14 (2006).

31. *Id.* at 14.

32. *See id. See also* Kevin Jakopchek, Note, *"Obtaining" the Right Result: A Novel Interpretation of the Computer Fraud and Abuse Act That Provides Liability for Insider Theft Without Overbreadth*, 104 J. CRIM. L. & CRIMINOLOGY 605, 611 (2014) ("As one commenter described it, '[c]omputer-related criminal conduct presents a challenge . . . because it involves electronic impulses that cannot be seen, touched, moved, or copied as those terms have traditionally been defined, and that therefore seem to fall outside the idea of 'property' as defined over centuries of Anglo-American jurisprudence.'" (quoting Joseph Olivenbaum, *<Ctrl><Alt><Del>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 577 (1997))).

33. 18 U.S.C. § 1030(a)(1)–(3) (2012).

34. Samantha Jensen, Note, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 88 (2013).

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

36. 18 U.S.C. § 1030(a)(4)–(6). *See also* Mary Jo Obee & William Plouffe Jr., *Privacy in the Federal Bankruptcy Courts*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1011, 1028 (2000) (explaining the essence of the 1986 CFAA).

37. 18 U.S.C. § 1030(a)(4).

38. 18 U.S.C. § 1030(a)(5).

39. 18 U.S.C. § 1030(a)(6).

"those used either by the U.S. Government or financial institutions, or as part of a multistate computer network."[40]

Congress next expanded the CFAA in 1994 when it passed the Violent Crime Control and Law Enforcement Act.[41] Importantly, the 1994 amendment added a civil provision to the CFAA, allowing victims of computer crimes the ability to recover civil damages against hackers.[42] More amendments ensued. The 1996 amendments introduced dramatic changes. The most notable one had to do with expanding 18 U.S.C. § 1030(a)(2)—the main focus of this Note. The provision was "originally limited to unauthorized access that obtained financial records from financial institutions, card issuers, or consumer reporting agencies."[43] Now, the 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."[44] All interstate hacking was outlawed. On top of this, the new amendments added a seventh crime: computer extortion.[45]

The 1996 amendments greatly expanded the statute by replacing the category of "Federal interest" computers with the new category of "protected computers." The statute described a protected computer as any machine "used" in interstate commerce.[46] Professor Kerr writes, "the change in the definition changed the scope of the statute dramatically."[47] Now, every computer connected to the Internet could be used in interstate commerce. In one fell swoop, adding the term "protected computer" considerably expanded the statute's realm.[48]

The following amendments further broadened that realm. The USA Patriot Act[49] expanded the definition of "protected computer" to include computers located outside the United States.[50] Like Professor Kerr notes, "[t]he amendment effectively extended the CFAA to as many foreign computers as the Commerce Clause allows."[51] The last

40. *See* Kerr, *supra* note 26, at 1565. *See also* 18 U.S.C. § 1030(e)(2).

41. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-122, 108 Stat. 1796 (1994).

42. *See* 18 U.S.C. §1030(g).

43. *See* Kerr, *supra* note 26, at 1567. *See also* 18 U.S.C. § 1030(a)(2).

44. *See* Kerr, *supra* note 26, at 1567.

45. 18 U.S.C. § 1030(a)(7).

46. 18 U.S.C. § 1030(e)(2)(B).

47. *See* Kerr, *supra* note 26, at 1568.

48. Actually, the statute also defines the term "computer," a definition that also expands the reach of the statute:

> The 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, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1).

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

50. 18 U.S.C. § 1030(e)(2)(B).

51. Kerr, *supra* note 26, at 1568 (footnote omitted).

major amendments to the CFAA occurred recently in 2008. These amendments, enacted in the Former Vice President Protection Act,[52] continued the decades-long trend of expanding the CFAA to be as broad as possible. The new amendments expanded 1030(a)(2) by removing the requirement of an interstate communication. 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."[53] The amendments also once again expanded the definition of "protected computers." It included the words "or affecting" in the phrase "which is used in *or affecting* interstate or foreign commerce or communication . . . ."[54] This is a small change, but it makes a big difference. Professor Kerr explains that the phrase "or affecting" is a legal term of art that signals congressional intent to cover as much as the Commerce Clause will allow.[55] Now Congress can regulate any class of activities that, in the aggregate, can impact interstate commerce.[56] Thus, no longer does a computer have to be connected to the Internet in order for Congress to regulate it. A "protected computer" now just means a "computer."

III. THE STATUTORY FRAMEWORK OF THE CFAA

18 U.S.C. § 1030 is a federal statute aimed at prohibiting computer misuse crimes.[57] It is most commonly called the Computer Fraud and Abuse Act. There are generally two types of computer misuse crimes. The first is when a user has unauthorized access—the user exceeds his or her privileges on a computer.[58] The second type of computer misuse crime occurs when a person denies others their privileges to use a computer.[59] The CFAA is a statute aimed mostly at prohibiting the first type of computer misuse crime: unauthorized access to a computer. For this reason, it is deemed an unauthorized access statute.[60]

Section 1030(a) lists seven distinct crimes the statute outlaws. As Professor Kerr notes, "most of [them] are keyed to the basic unauthorized access prohibition."[61] The first of the seven crimes is perhaps the

52. Former Vice President Protection Act, Pub. L. No. 110-326, 122 Stat. 3560 (2008).

53. *See* Kerr, *supra* note 26, at 1569.

54. 18 U.S.C. § 1030(e)(2)(B) (emphasis added).

55. *See* Kerr, *supra* note 26, at 1570–71.

56. For parallel scenarios, see, for example, Wickard v. Filburn, 317 U.S. 111 (1942) (holding that Congress's power to regulate interstate commerce extends to local wheat producer's ability to produce wheat above government-imposed limit because, in the aggregate, all local wheat producers ability to grow wheat above that limit would affect the price of wheat in interstate commerce); Gonzalez v. Raich, 545 U.S. 1 (2005) (holding that Congress's power to regulate interstate commerce extends to banning homeowner from producing marijuana because if it did not, all local marijuana producers' products would reach the interstate market—contrary to the interests of the government).

57. A computer misuse crime is an "offense[ ] involving interference with the proper functioning of computers." KERR, *supra* note 30, at 7.

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.* at 28.

most important, but has never been used in practice.[62] It is an extremely narrow section that prohibits accessing a computer without authorization or exceeding authorized access to obtain classified information to injure the United States or aid a foreign power.[63] Section 1030(a)(2) is where all the action lies.[64] It is the most frequently used provision of the CFAA. It prohibits trespassing into a computer to obtain financial information, information from any department or agency of the United States, or information from any protected computer. It is this last proscription that makes the statute too broad.[65] Section 1030(a)(3) is another rarely used provision that prohibits trespassing on a federal government computer.[66] Section 1030(a)(4) is the federal computer fraud provision.[67] It prohibits accessing a computer to defraud and obtain value. Section 1030(a)(5) is the federal computer damage provision prohibiting unauthorized damage and unauthorized access that damages a computer.[68] Section 1030(a)(6) prohibits trafficking in computer passwords.[69] The last section, 1030(a)(7), is an extortion provision prohibiting extorting money or other property by using threats of damage to computers.[70]

The remaining sections of 18 U.S.C. § 1030 supplement the basic crimes that were listed in § 1030(a). Only the most important sections for purposes of this Note will be discussed. Section 1030(b) makes conspiracy to commit these seven crimes a crime in itself.[71] Section 1030(c) is quite detailed.[72] It states that committing any of the seven basic crimes is a misdemeanor. However, in some circumstances, committing such crimes can become a felony. In particular, a person commits a felony when one or more of the following elements are met: (1) the act is "committed for purposes of commercial advantage or private financial gain"[73]; (2) the act is "committed in furtherance of any criminal or tortious act"[74]; or (3) the act committed involves obtaining information that "exceeds 5,000 dollars."[75]

There are two more noteworthy sections. Section 1030(e) contains statutory definitions of all key terms used in the statute.[76] A few are vital to note. The first is the definition of "protected computer." The statute defines it as a computer, "which is used in or affecting interstate or foreign commerce or communication, including a computer located

62. *Id.*
63. *See* 18 U.S.C. § 1030(a)(1) (2012).
64. *See* KERR, *supra* note 30, at 28. *See also* 18 U.S.C. § 1030(a)(2).
65. *See infra* Part V for an in-depth discussion of why 18 U.S.C. § 1030(a)(2)(C) is too broad.
66. 18 U.S.C. § 1030(a)(3).
67. 18 U.S.C. § 1030(a)(4).
68. 18 U.S.C. § 1030(a)(5).
69. 18 U.S.C. § 1030(a)(6).
70. 18 U.S.C. § 1030(a)(7).
71. 18 U.S.C. § 1030(b).
72. 18 U.S.C. § 1030(c).
73. 18 U.S.C. § 1030(c)(2)(B)(i).
74. 18 U.S.C. § 1030(c)(2)(B)(ii).
75. 18 U.S.C. § 1030(c)(2)(B)(iii).
76. 18 U.S.C. § 1030(e).

outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." In a nutshell, a protected computer is any computer inside or outside of the United States that may affect interstate commerce. At a minimum, any computer connected to the Internet is a protected computer because it affects interstate commerce.[77] But, stretched to its limits, the term "protected computer" could mean any computer—regardless of Internet access—due to modern Commerce Clause doctrine.[78]

The second definition of § 1030(e) of note is that of "exceeds authorized access." The CFAA is primarily an unauthorized access statute that seeks to punish those who use a computer "without authorization" or those who "exceed[ ] authorized access." In all the times the statute has been amended, the term "without authorization" has never been defined. But the latter phrase, "exceeds authorized access" has been defined. The term means, "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[79] It is the interpretation of this definition that has led to the current circuit court split.[80] The legislative history and language of the statute reflects the rationale that those who access a computer "without authorization" are hackers from outside of an organization, while those who "exceed[ ] authorized access" are hackers from inside an organization—employees who hack into their corporate computer network.[81]

The last important section is 1030(g),[82] which provides a civil remedy for victims of computer misuse to sue in federal court. As Professor Kerr notes, "most of the published cases interpreting § 1030 arise in the civil context rather than the criminal context."[83] Courts do not treat § 1030 differently in the criminal and civil contexts.[84] However, civil

77. A Department of Justice manual advises all federal prosecutors that the CFAA applies to all computers connected to the Internet. U.S. DEP'T OF JUSTICE, *supra* note 24, at 4. Many courts agree. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("[T]he latter two elements of the section 1030(a)(2)(C) crime [obtaining information from a protected computer] will always be met when an individual using a computer contacts or communicates with an Internet website.").

78. *See* Kerr, *supra* note 26, at 1570–71 (explaining that the phrase "affecting interstate commerce" signals congressional intent to extend the Commerce Clause as wide as possible). *See also* discussion *infra* Part II.

79. 18 U.S.C. § 1030(e)(6).

80. The circuit court split will be discussed in Part IV.

81. "However, some courts have diverged from this general approach and have found that insiders acted 'without authorization' in certain civil cases." U.S. DEP'T OF JUSTICE, *supra* note 24, at 6. *See infra* Part IV for a more meaningful discussion on the contours of "without authorization" and "exceeding authorized access."

82. 18 U.S.C. § 1030(g).

83. KERR, *supra* note 30, at 29.

84. *See* Jakopchek, *supra* note 32, at 612 ("Subsequent criminal cases have not distinguished between statutory CFAA interpretations in criminal and civil contexts." (citing United States v. Nosal, 676 F.3d 854 (9th Cir. 2012))). *Nosal* is a criminal case that cited to a civil CFAA case as authoritative on legal interpretation issue.

plaintiffs cannot bring a claim under § 1030(a)(2)(C).[85] Only federal prosecutors can bring that claim.

IV. THE CIRCUIT SPLIT REGARDING THE CFAA

Although the plain language of the statute appears simple to understand, in reality the CFAA is a vaguely worded statute. There is a deep divide among the circuit courts on how to interpret § 1030(a)(2)(C).[86] The purpose of this section is to detail that divide. The provision creating it reads, "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer . . . shall be punished . . . ."[87] The issue at hand is how to interpret the word "authorization." When does a user lose authority to use a computer? The answer is all-important, for when that authority is lost, or exceeded, a computer user violates the statute and commits a federal crime. Professor Kerr notes, "deciding when an access is 'without authorization' or 'in excess of authorization' often determines the line between an act that is criminal and one that is not."[88]

Courts generally take one of two approaches to interpreting the term. The First, Fifth, Seventh, Eighth, and Eleventh Circuits at one time or another have adopted a broad approach to interpreting the provision.[89] Depending on the circuit, agency or contract theory comprises the underlying rationale for the broad approach. Conversely, the Second, Fourth, Sixth, and Ninth Circuits have adopted a narrow approach to interpreting the provision.[90] The narrow approach is a new way to interpret the statute that has gathered great steam. Code-based theory underlies the approach.

A. *The Broad Interpretation Approach*

Many, if not a majority, of the circuit courts have taken a broad approach to interpreting the statute, reading the word "authorization" to impose use restrictions. A use restriction prohibits the particular way a person uses a computer. If the person has authority to use a com-

85. U.S. DEP'T OF JUSTICE, *supra* note 24, at 40 n.8 ("Civil plaintiffs do not have section 1030(a)(2) available to them.").

86. *See, e.g.*, Audra Dial & John Moye, *The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?*, 64 HASTINGS L.J. 1447 (2013) (providing another detailed account of the circuit split).

87. 18 U.S.C. § 1030(a)(2)(C).

88. KERR, *supra* note 30, at 43.

89. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Teague, 646 F.3d 1119 (8th Cir. 2011); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

90. *See, e.g.*, United States v. Valle, 807 F.3d 508 (2d Cir. 2015), WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295 (6th Cir. 2011); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). The Third Circuit recently utilized the narrow approach in a non-precedential opinion. *See* CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116 (3d Cir. 2015).

puter in a certain way, but then uses the computer in another way, that person has violated the statute.

Two theories underlie the use restriction approach: contract theory and agency theory.[91] Contract theory "finds its roots in contract law, focusing on the contractual relationship between the parties."[92] It declares a contract between an employer and employee, and sets the grounds for how the user will use the computer. If the user violates those grounds, they violate the contract, in turn violating the statute.[93] It is easy for prosecutors to prove a defendant violated the statute under the contract-based approach. All they have to do is show the defendant violated a restriction memorialized in writing, such as through "terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."[94] Thus, an employee who uses a computer to access Facebook when the employment contract prohibits accessing the website violates the law.[95] Meanwhile, agency theory is grounded in the traditional principles of agency.[96] In an agency relationship, an employee owes a special duty of loyalty to the employer. That duty is to act primarily for the benefit of the employer.[97] As soon

91. There is actually a third theory supporting the broad-based approach: norms-based theory. Professor Kerr explains that norms-based theory will hold the user of a computer accountable under the statute if he uses the computer "beyond the pale of accepted social practices" in the workplace. Orin Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, VOLOKH CONSPIRACY (Jan. 14, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/. However, the theory has little support, as professor Kerr admits, "Courts have mostly rejected this theory . . . ." *Id.* Still, the Fifth Circuit essentially utilized norms-based theory to find a defendant liable. *See* United States v. Phillips, 477 F.3d 215 (5th Cir. 2007). There, the Fifth Circuit adopted an "intended-use analysis," finding the defendant violated the CFAA because he used the computer contrary to the "expected norms of intended use or the nature of the relationship established between the computer owner and the user." *Id.* at 219. For a more in-depth look at norms-based theory, see KERR, *supra* note 30, at 45.

92. *See* Jensen, *supra* note 34, at 106 (citing Garrett Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1388 (2011)).

93. *Id.* ("Liability under the CFAA may attach if a court finds that an employee accessed a protected computer in a way that was prohibited or in excess of limitations set by a contract or a clearly communicated employer policy." (citing Urban, *supra* note 92, at 1372)).

94. U.S. DEP'T OF JUSTICE, *supra* note 24, at 9.

95. See *Nosal*, 676 F.3d 854 for Judge Kozinski's criticism of the contract-based approach to interpreting the CFAA. He posits this same Facebook scenario to highlight how unduly harsh and broad the CFAA can potentially be under the theory. *Id.* at 860. He also cites to a real case where an employer countersued a former employee under the CFAA for using Facebook at work. *See* Lee v. PMSI, Inc., No. 8:10-CV-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011). However, the *Lee* court ultimately dismissed the counterclaim. *Id.*

96. Agency is the "fiduciary relation which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." RESTATEMENT (SECOND) OF AGENCY § 1 (AM. LAW INST. 1958). *See also* RESTATEMENT (THIRD) OF AGENCY § 1.01 (AM. LAW INST. 2006).

97. RESTATEMENT (SECOND) OF AGENCY § 13 cmt. a (AM. LAW INST. 1958) ("The agreement to act on behalf of the principal causes the agent to be a fiduciary, that is, a person having a duty, created by his undertaking, to act primarily for the benefit of another in matters connected with his undertaking.").

as the employee acts adversely to the employer's interest, the employee severs the agency relationship. As such, a computer user violates § 1030(a)(2)(C) whenever the user uses the computer for purposes that do not further his or her employer's interest. Once the computer user acts adversely to his or her employer's interest, the agency relationship is terminated and the user loses authorization on the computer.[98]

The flagship case representing the contract-based approach is *EF Cultural Travel BV v. Explorica, Inc.*[99] The case stands for the proposition that "using a computer in violation of a contractual agreement with the computer's owner [or website's creator] constitutes exceeding authorized access to that computer."[100] In that case, the defendant created a "scraper" computer software program that systematically gleaned prices on EF Cultural Travel's website.[101] This would help his new company, Explorica, undercut his old company's prices. The court focused much of its attention on the contract agreement the defendant had previously signed with EF Cultural Travel. The defendant promised "to maintain in strict confidence and not to disclose to any third party . . . any Confidential or Proprietary Information . . . for Employee's own benefit or for the benefit of any other person or business entity other than EF."[102] The defendant breached the contract when he used the scraper to analyze tour prices and thus obtain proprietary information. As such, the court concluded the defendant exceeded his authority on EF Cultural Travel's website and violated the CFAA.[103]

The Seventh Circuit in *International Airport Centers, L.L.C. v. Citrin*[104] adopted an agency approach of the broad interpretation. In that case, the court held the defendant lost the authority to use his company's laptop when he decided to act adversely to his employer's interests.[105] By deleting valuable data that was stored on the company laptop, the defendant breached his agency relationship and no longer had authority to use the laptop. The court explains, "his authorization to access the laptop terminated when . . . he 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 on an employee."[106] The court directly cited to agency law in finding the employee exceeded his authorization on the computer.

98. *See also* Jensen, *supra* note 34, at 103–04 ("An employee has 'authorization' under the CFAA as long as his work furthers the interest of his employer. . . . Authorization is implicitly revoked whenever an employee accesses a computer for purposes that do not further his employer's interest." (citing Katharine Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 891, 823 (2009) (footnotes omitted))).

99. 274 F.3d 577 (1st Cir. 2001).

100. KERR, *supra* note 30, at 58.

101. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

102. *Id.* at 582.

103. *Id.* at 583–84.

104. 440 F.3d 418 (7th Cir. 2006).

105. *Id.* at 421.

106. *Id.* at 420. The court further explained, "Citrin's breach of his duty of loyalty [deleting valuable data on company computer] terminated his agency relationship . . . and with it his authority to access the laptop . . . ." *Id.* at 420–21.

B. *The Narrow Interpretation Approach*

Circuit courts have recently begun adopting a narrow approach to interpreting the CFAA. The narrow approach is a much different reading of the CFAA. In it, courts impose access restrictions on users of computers, not use restrictions. Under an access restriction, a user only violates the CFAA when he or she did not have initial authority to access a computer. The access restriction approach is different than the use restriction approach because it does not matter how the employee uses the computer—all that matters is whether he or she had authority to use the computer in the first place. As such, an employee under an access restriction could conceivably commit acts of terrorism on the computer and still not violate the CFAA, because he or she was given authority to initially use the computer.[107] However, under the use restriction approach, using the computer in such a way would almost certainly result in a breach of the law under the contract or agency theories of liability.

Professor Kerr's code-based theory is synonymous with the narrow interpretation approach.[108] Under the theory, the user of a computer does not have authority to use a computer if he or she must circumvent the computer's code-based restrictions in order to access the computer.[109] As Professor Kerr explains, "when an owner regulates privileges by code, the owner or her agent designs and programs the computer's hardware and software so that the code limits each user's privileges . . . . For a user to exceed privileges imposed by code, the user must somehow 'trick' the computer into giving the user greater privileges."[110] In other words, if the owner requires a computer have a password, and the user does not know the password because he or she does not have authority to know it, but somehow guesses it, that user violates the CFAA.

The Ninth Circuit was the first circuit to utilize the narrow-based approach.[111] The court in *United States v. Nosal* best illustrates it.[112] In *Nosal*, the court held that the phrase "exceeds authorized access" in the CFAA embraces individuals who have only limited access to files or data

107. *See also* U.S. DEP'T OF JUSTICE, *supra* note 24, at 11 ("However, a number of recent civil cases have rejected the idea that users can exceed authorized access within the meaning of section 1030(e)(6) when they access information that they are authorized to access, even if their access is motivated by an implicitly improper purpose.").

108. KERR, *supra* note 30, at 44–45.

109. *Id.* at 44.

110. *Id.* at 44–45.

111. The Ninth Circuit first officially adopted the narrow interpretation approach in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009). Since then, the Fourth Circuit adopted the approach in WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012). The Sixth Circuit likely has too. *See* Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304–05 (6th Cir. 2011) ("Commonly understood, then, a defendant who accesses a computer 'without authorization' does so without sanction or permission." (citing *Brekka*, 581 F.3d at 1132–33)).

112. 676 F.3d 854 (9th Cir. 2012). For an excellent recounting of the decision, see Recent Case, *Statutory Interpretation—Computer Fraud and Abuse Act—Ninth Circuit Holds That Employees' Unauthorized Use of Accessible Information Did Not Violate the CFAA.*—United States v. Nosal, *676 F.3d 854 (9th Cir. 2012) (en banc).*, 126 HARV. L. REV. 1454 (2013).

and who exceed restrictions on that access [access restriction], not those who have unrestricted physical access to a computer but use the stored information for unauthorized purposes [use restriction].[113] The facts of the case were clear. The defendant and other employees used their login credentials in order to download valuable information from their company. They later transferred this information to a competitor company for their own personal gain.[114] Although the court believed the behavior culpable, it was not so under the CFAA. There were various reasons why.[115] In the end, the court adopted an access restriction approach, and went so far as to urge its sister circuits to renounce the broad interpretation approach.[116]

V. THE UNCONSTITUTIONALITY OF THE CFAA

Why did the Ninth Circuit in *Nosal* suddenly decide to break with so many of its sister circuits and reject the popular broad interpretation approach? The reason was simple—the broad interpretation approach is unfair to the American people.[117] The problem of the CFAA lies in § 1030(a)(2)(C). Under its broad reading, millions of Americans commit at least a misdemeanor any time they break a use restriction. Under the contract theory of a use restriction, if a person uses a computer in a way that breaches a contract, either her employer's or a website's terms of service, she is instantly liable. Under an agency theory, if a person uses a computer contrary to his employer's interests, such as to peruse Facebook, he is also instantly liable.

What actually makes the CFAA so expansive under the broad reading? A number of things. First and foremost, § 1030(a)(2)(C) imposes a use restriction instead of an access restriction. Contract theory and agency theory underlie the contours of a use restriction.[118] Second, the provision requires no scienter requirement under contract theory (however, agency theory does impose a scienter requirement).[119]

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

114. *Id.*

115. The major reasons will be detailed in Part V.

116. The court was explicit: "We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead. . . . [We] recognize that the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *Nosal*, 676 F.3d at 863 (quoting Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)).

117. The court in *Nosal* sheds light:

> Were we to adopt the government's proposed interpretation [the broad interpretation approach], millions of unsuspecting individuals would find that they are engaging in criminal conduct. . . . Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents—and their parents and teachers into delinquency contributors.

Id. at 859–61.

118. *See infra* Part IV.A (detailing both contract theory and agency theory).

119. It is extremely odd that 18 U.S.C. § 1030(a)(2)(C) does not really impose a scienter requirement under the broad interpretation approach. Other provisions in the CFAA impose such a requirement. For instance, § 1030(a)(4) imposes a scienter requirement of "knowingly and with intent to defraud." 18. U.S.C. § 1030(a)(4) (2012). To be clear, § 1030(a)(2)(C) does state the scienter requirement of "intentionally"—but only in

Third, the provision requires the use of a "protected computer"[120]—which is basically any computer in existence today. The reason is because almost every computer is connected to the Internet, which automatically means the computer is used in interstate commerce. But, the other reason is the phrase "or affecting" in the statute. As Professor Kerr noted, this language means Congress meant to use the Commerce Clause to its widest possible reach. Even a computer used solely for a local activity can affect interstate commerce—if one imagines that millions of local computers "affect" interstate commerce. Finally, the provision defines "computer" much too broadly.[121]

Due to the CFAA's alarming reach under the broad interpretation, the statute must be construed differently. The broad interpretation approach is the most popular reading of the CFAA, used in at least five circuits. Something must be done to stop this reading. One way is to argue the CFAA is unconstitutional on its face. There are two reasons why, both grounded in the Due Process Clause of the Fifth Amendment. First, the statute is void for vagueness. It does not provide fair notice, and it leads to discriminatory enforcement. Second, the statute violates the private nondelegation principle. Aside from constitutional considerations, there are a plethora of reasons for why a court can refuse the broad interpretation approach.[122] However, this Note will only focus on the unconstitutionality of the broad reading.

A. *The Void for Vagueness Doctrine*

According to the Supreme Court, the void for "vagueness doctrine is an outgrowth . . . of the Due Process Clause of the Fifth Amendment."[123] The Due Process Clause requires that persons "be informed as to what the State commands or forbids."[124] The vagueness doctrine states a statute violates due process if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[125] Thus, there are two separate tests a court undergoes to determine if a statute is unconstitutionally void. A statute violates the

---

the sense that the user must intend to access the computer. 18 U.S.C. § 1030(a)(2)(C). That is it. There is no scienter requirement that the user must intend to *purposefully use a computer to commit a computer misuse crime.* That is the difference. Perhaps one way for Congress to fix the CFAA and impose a narrow interpretation is to add a more robust scienter requirement.

120. *See infra* Part III (discussing the definition in more detail).

121. *See infra* Part III (detailing the broad definition of a computer).

122. *See, e.g.*, Jensen, *supra* note 34 (explaining other reasons why the broad interpretation approach is incorrect, including the rule of lenity, the overbreadth doctrine, the plain language rule, the canon of consistency, the no "mere surplusage" rule, and the legislative history of the statute). *See also* David Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed Without Permission*, 47 CREIGHTON L. REV. 423 (2014); Stephanie Greene & Christine O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281 (stating more or less the same reasons for why the broad approach is flawed).

123. United States v. Williams, 553 U.S. 285, 304 (2008).

124. Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939).

125. *Williams*, 553 U.S. at 305 (citations omitted).

doctrine if (a) it does not provide fair notice of what action violates the law, or (b) it leads to discriminatory police enforcement of the law.

The Court in *Coates v. City of Cincinnati*[126] elaborated on the first test of fair notice. There, the Court struck down an Ohio ordinance that made it a crime for three or more persons to assemble on sidewalks and be "annoying."[127] The Court explained why: "Conduct that annoys some people does not annoy others. Thus, the ordinance is vague . . . 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.'"[128] The ordinance was vague because it did not give people of common intelligence notice of what behavior was "annoying" in public. In another case, the Court described the rationale for fair notice: "The underlying principle is that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed."[129] It makes no sense under any theory of punishment to chastise a person who violates a statute that gives no fair explanation of what behavior is criminal.

The Court in *Kolender v. Lawson*[130] elaborated a second way a statute can be void for vagueness. In that case, the Court struck down a California ordinance that required persons to provide "credible and reliable" identification when stopped by a cop with reasonable suspicion.[131] The statute defined such identification as, "carrying reasonable assurance that the identification is authentic and providing means for later getting in touch with the person who has identified himself."[132] The Court held this definition was vague because it "contain[ed] no standard for determining what a suspect has to do in order to satisfy the requirement to provide a 'credible and reliable' identification."[133] The Court explained that as a result of this uncertainty, "the statute vests 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."[134] The Court assumed giving complete discretion to the police

126. 402 U.S. 611 (1971). The Supreme Court has repeatedly elaborated on the fair notice standard. *See, e.g.*, Kolender v. Lawson, 461 U.S. 352, 357 (1983) (explaining that the statute satisfies fair notice when it defines the criminal offense "with sufficient definiteness that ordinary people can understand what conduct is prohibited"); Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) ("This ordinance is void for vagueness . . . in the sense that it 'fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute'" (quoting United States v. Harriss, 347 U.S. 612, 617 (1954))); *Williams*, 553 U.S. at 307 ("What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is.").

127. *Coates*, 402 U.S. at 615.

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

129. *Harriss*, 347 U.S. at 617 (footnote omitted).

130. 461 U.S. 352 (1983).

131. *Id.* at 361.

132. *Id.* at 357.

133. *Id.* at 358.

134. *Id.*

would lead to arbitrary enforcement: "An individual, whom police may think is suspicious . . . , is entitled to continue to walk the public streets 'only at the whim of any police officer' . . . ."[135]

The Court also explicitly noted that this second test—the statutory requirement of minimal guidelines that will stave off discriminatory enforcement—is more paramount than the first test of fair notice. The Court wrote,

> Although the doctrine focuses both on actual notice to citizens and arbitrary enforcement, we have recognized recently that the more important aspect of the vagueness doctrine "is not actual notice, but the other principal element of the doctrine—the requirement that a legislature establish minimal guidelines to govern law enforcement."[136]

The Court was clear on why this second test was more important than the first: "Where the legislature fails to provide such minimal guidelines, a criminal statute may permit 'a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections.'"[137] In other words, the fear of discriminatory enforcement is greater than the fear that the law will happen to punish someone who did not know they were violating the law.

B. *The Private Nondelegation Principle*

There is another way for the CFAA to be unconstitutional: it can violate the private nondelegation principle. On the one hand, the public nondelegation principle generally prohibits one government branch from authorizing another branch to carry out its constitutionally granted powers and functions.[138] It is not rooted in the Due Process Clause.[139] On the other hand, the private nondelegation principle states that no branch may give its powers and functions to a private entity.[140] Just like the void for vagueness doctrine, this principle is

---

135. *Id.* (citing Shuttlesworth v. City of Birmingham, 382 U.S. 87, 90 (1965)).

136. *Id.* at 357–58 (quoting Smith v. Goguen, 415 U.S. 566, 574 (1974)).

137. *Id.* at 358 (quoting *Goguen*, 415 U.S. at 575).

138. Touby v. United States, 500 U.S. 160, 165 (1991) ("Congress may not constitutionally delegate its legislative power to another branch of Government.").

139. Unlike the private nondelegation doctrine, the public nondelegation doctrine does not find its roots in the Due Process Clause of the Fifth Amendment. Instead, it finds them in two sources of law: (1) Article I, section 1 of the Constitution, and (2) the general notion of separation of powers. This difference is consequential—it means states cannot violate the private nondelegation principle if that principle finds its foundations in the Due Process Clause. Indeed, many states recognize they cannot. *See, e.g.*, Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 150 (2000) (stating that the private nondelegation doctrine "flourishes . . . in the state courts"). To see the different sources of law underlying the private and public nondelegation principles, *compare* Carter v. Carter Coal Co., 298 U.S. 238 (1936), *with* Mistretta v. United States, 488 U.S. 361, 371–72 (1989).

140. However, this is only true for the most fundamental powers and functions of a branch. Generally, "Congress cannot let private actors make law unless they do so through a process that internalizes the wishes of affected parties or is subject to meaningful state oversight." Michael Horton, *Arbitration as Delegation*, 86 N.Y.U. L. REV. 437, 441

mainly, but not always,[141] rooted in the Due Process Clause.[142] Both principles are chiefly concerned with Congress giving away its lawmaking power. Of the two, private delegations "raise . . . more troubling constitutional issues . . . ."[143] One of the major reasons is transparency. The great fear of public delegations is that Congress will be able to transfer its lawmaking power to an unelected agency that will make hard policy choices, rendering Congress free from having to make the choice and be held accountable. In private delegations, Congress has an even greater accountability problem because potentially no one is supervising the private party. At least in public delegations, the agency is subject to presidential oversight. Private nondelegation is also more troubling than public because of abuse of power concerns. Public officials are supposed to serve the public. Private persons, however, are apt to be more selfish. As Professor Horton notes, "[t]hey inevitably 'select regulation that provides them with maximum benefits without considering the effect on the other regulated parties or the public.'"[144]

Due to these two concerns, the private nondelegation principle requires a more robust test than the public one, making it a "more muscular version of the [public] nondelegation doctrine."[145] The public nondelegation principle relies on the toothless "intelligible principle" test.[146] The private nondelegation principle requires a fact sensitive, three-part examination of whether a statute allows private parties to make law without the safeguards that will "inhibit[ ] arbitrary or self-motivated action."[147] The first factor focuses on the nature of the delegation: whether it authorizes private actors to make law in a neutral, transparent way.[148] The second inquiry asks whether affected par-

(2011) (citing *Carter Coal Co.*, 298 U.S. at 311); Gillian Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1437–40 (2003).

141. *See, e.g.*, Crain v. First Nat'l Bank of Oregon, 324 F.2d 532, 537 (9th Cir. 1963) ("Congress cannot [under Article I, section 1] delegate to private corporations or anyone else the power to enact laws . . . .").

142. *Carter Coal Co.*, 298 U.S. at 311 ("The delegation is so clearly arbitrary, and so clearly a denial of rights safeguarded by the due process clause of the Fifth Amendment, that it is unnecessary to do more than refer to decisions of this court which foreclose the question."). However, the constitutional foundation for the private nondelegation doctrine has never been clear. Professor Michael Horton explains, "Courts and commentators have alternatively opined that private delegations violate Article I, section 1, the Due Process Clause of the Fifth Amendment, or both." Horton, *supra* note 140, at 473–74 (footnotes omitted).

143. Horton, *supra* note 140, at 472 (quoting Tex. Boll Weevil Eradication Found., Inc. v. Lewellen, 952 S.W.2d 454, 469 (Tex. 1997)). *See also* United Chiropractors of Wash., Inc. v. State, 578 P.2d 38, 40 (Wash. 1978) ("Delegation to a private organization raises concerns not present in the ordinary delegation of authority to a governmental administrative agency.").

144. Horton, *supra* note 140, at 473 (quoting Lisa Bressman, Schechter Poultry *at the Millennium: A Delegation Doctrine for the Administrative State*, 109 YALE L.J. 1399, 1428 (2000)).

145. *Id.* at 472.

146. J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928).

147. Horton, *supra* note 140, at 474 (quoting Santaniello v. N.J. Dep't of Health & Senior Servs., 5 A.3d 804, 810 (N.J. Super. Ct. App. Div. 2010)).

148. One way to determine if the lawmaking power is neutral is to look at the nature of the lawmaking power conferred. If it seems substantial, then it is more likely

ties are adequately represented in the private lawmaking process. Courts should look for the existence of a "representative process—a decision-making structure that includes all affected constituencies."[149] Finally, the third inquiry asks whether the state retains control over the private party.[150] This factor is probably the most important of the three.[151] The Court has generally found the presence of government oversight will shield private delegation from constitutional attacks.[152] By controlling the private party, the government makes its presence known to the public and thereby becomes accountable. Moreover, the government stops the party from wielding power in a non-neutral, self-serving fashion.[153]

The only Supreme Court case to utilize the private nondelegation principle to strike down a statute was *Carter v. Carter Coal Co.*[154] In that case, the Court held a provision of Bituminous Coal Conservation Act unconstitutional for delegating power to a private party to fix the maximum hours of labor and minimum wages for all coal producers and miners in its region.[155] Before even getting to the three-part inquiry, the Court outright stated that it viewed private delegation of lawmaking power suspiciously: "This is legislative delegation in its most obnoxious form; for it is not even delegation to an official or an official body . . . ."[156] The Court then partially utilized the three-part inquiry. First, it found the lawmaking power conferred to the private party was not

---

that the private party will wage that power in a non-neutral, self-serving way. Some circuit courts "have understood the Supreme Court's private nondelegation decisions to mean 'that Congress may employ private entities for *ministerial* or *advisory* roles, but it may not give these entities governmental power over others.'" Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 765 (2013) [hereinafter *Vagaries of Vagueness*] (quoting Pittston Co. v. United States, 368 F.3d 385, 395 (4th Cir. 2004)). *See also* United States v. Frame, 885 F.2d 1119, 1129 (3d Cir. 1989).

149. Horton, *supra* note 140, at 477 (citing Tex. Boll Weevil Eradication Found., Inc. v. Lewellen, 952 S.W.2d 454, 472 (Tex. 1997)); David M. Lawrence, *Private Exercise of Governmental Power*, 61 IND. L.J. 647, 689 (1986) (noting that private delegations are not troubling if they are "to groups that arguably contain all those importantly affected by the set of rules made by the group").

150. *See Vagaries of Vagueness*, *supra* note 148, at 765 ("[T]he most important [of the three factors] appears to be the presence of government supervision." (citing Donna M. Nagy, *Playing Peekaboo with Constitutional Law: The PCAOB and Its Public/Private Status*, 80 NOTRE DAME L. REV. 975, 1059, 1059 n.459 (2005))).

151. *Id.* at 765 ("Though judicial opinions seldom identify the factors clearly, the most important appears to be the presence of government supervision." (citing Nagy, *supra* note 150, at 1059)).

152. *See, e.g.*, Sunshine Anthracite Coal Co. v. Adkins, 310 U.S. 381, 389–99 (1940). The court held that the Bituminous Coal Act was a valid private delegation of lawmaking power. The act gave private coal boards the ability to propose minimum prices of coal that were subject to substantial government oversight by the National Bituminous Coal Commission. The Commission would accept, deny, or modify the private coal boards' recommendations. The Court wrote, "Nor has Congress delegated its legislative authority to the industry. The members of the code [private coal boards] function subordinately to the Commission. It, not the code authorities, determines the prices. And it has authority and surveillance over the activities of these authorities." *Id.* at 399.

153. Horton, *supra* note 140, at 479.

154. Carter v. Carter Coal Co., 298 U.S. 238, 311 (1936).

155. *Id.*

156. *Id.*

neutral. Congress allowed a private party the ability to regulate the businesses of its competitors. As such, "[t]he power conferred upon the majority is, in effect, the power to regulate the affairs of an unwilling minority."[157] Next, the Court found the affected parties had no representation in the process. This was an infraction of the Due Process Clause: "a statute which attempts to confer such power undertakes an intolerable and unconstitutional interference with personal liberty and private property. The delegation is so clearly arbitrary, and so clearly a denial of rights safeguarded by the due process clause of the Fifth Amendment . . . ."[158] Lastly, there was no government oversight of the private parties that fixed the hours and wages. For the first and only time, the Court utilized the private nondelegation principle to strike down a law.

C. *Applying the Void for Vagueness Doctrine to the CFAA*

Above all else, the CFAA is void for vagueness. It raises serious due process concerns because it fails both separate tests of the doctrine.[159] It fails to provide a person of ordinary intelligence fair notice of what conduct is prohibited under the statute. The question remains: does the statute impose a use restriction or an access restriction? The CFAA is also so standardless that it leads to discriminatory law enforcement. It provides no minimal guidelines to law enforcement of what behavior is criminal.

Under the first test, the CFAA does not give fair notice of what "without authorization" or "exceeds authorized access" mean in § 1030(a)(2)(C). The statute fails to provide fair notice because ordinary "men of common intelligence must necessarily guess" at the phrases' meanings.[160] In fact, it is not just ordinary men or women—but various judges in sister circuits who have vigorously disagreed on which interpretative approach to use. There are many reasons why such impermissible guessing is required. First, the plain language of the statute is vague. Just like the word "annoying" in *Coates*, both phrases here are so vague that their meaning is open to rigorous

157. *Id.* The Court also mentioned the power conferred was "to private persons whose interests may be and often are adverse to the interests of others in the same business." *Id.*

158. *Id.* (citing Schechter Poultry v. United States, 295 U.S. 495, 537 (1935)).

159. *See* United States v. Drew, 259 F.R.D. 449, 464–466 (C.D. Cal. 2009). The court found that 18 U.S.C. § 1030(a)(2)(C) was void for vagueness because it failed both prongs of the void for vagueness test. The court wrote, "This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies." In the case, a user violated MySpace's terms of service. *Id.* at 452. The court concluded the statute did not provide sufficient notice to the defendant that violating the terms of service would be a federal crime. *Id.* at 465. It also concluded the statute did not provide law enforcement with minimal guidelines on how to enforce the statute. *Id.* at 466. *See also* Terence Lau, *Towards Zero Net Presence*, 25 NOTRE DAME J.L. ETHICS & PUB. POL'Y 237, 258 (2011) (explaining the district court overturned the user's conviction because the CFAA was unconstitutionally vague).

160. *Drew*, 259 F.R.D. at 463. The court in *Drew* agrees "the question is whether individuals of 'common intelligence' are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not." *See id.* at 464.

debate. The only difference with the statute in *Coates* and the CFAA is that the latter has two vague phrases, not one. The phrases can either refer to an access restriction or a use restriction. Second, and closely related to the first reason, the CFAA does not explicitly inform ordinary men or women that a violation of a contract will result in criminal penalties.[161] It does not even specify *which* contract provisions will result in criminal liability.[162] Will de minimis breaches result in a misdemeanor? What if the contract provisions themselves are vague?[163] The contract theory approach is fatally flawed. If anything, ordinary men and women presume a contract breach does not result in criminal prosecution.[164] Third, the CFAA never explicitly specifies that acting contrary to an employer's interests will result in criminal penalties. Fourth, when the statute actually does provide a definition of the phrase "exceeds authorized access," the definition fixes nothing. The question still remains over what kind of restriction it implements: access or use. What is more, the legislative history of the statute is ambiguous.[165] Ultimately, just like the Court in *United States v. Harriss* explained, it makes no sense to hold a man or woman responsible for violating a statute that is not clear on its face as to what behavior is prohibited. No principle of punishment can justify such a vague act.

Under the second test, the CFAA is void for vagueness because it leads to discriminatory enforcement of the law—just like in weev's case, as presented in the introduction of this Note. The statute here glaringly fails to provide *any* guidelines to law enforcement for what behavior to punish—not just the "minimal guidelines" required by the vagueness doctrine.[166] First, it leads to discriminatory enforcement

161. *See id.* ("Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has 'criminalized breaches of contract' in the context of website terms of service.").

162. *Id.* Indeed, will de minimis breaches of contract result in criminal prosecution? The court in *Drew* took notice: "[the CFAA] 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." *Id.*

163. *Id.* at 465 ("This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers.").

164. *Id.* at 464 ("Normally, breaches of contract are not the subject of criminal prosecution. Thus, while 'ordinary people' might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties." (citations omitted) (footnote omitted)).

165. *Compare* United States v. Nosal, 676 F.3d 854, 859 n.5 (9th Cir. 2012) ("Were there any need to rely on legislative history, it would seem to support Nosal's [narrow interpretation] rather than the government's [broad interpretation]."), *with* United States v. Phillips, 477 F. 3d 215, 219 (5th Cir. 2007) ("In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between insiders, who are authorized to access a computer, and 'outside hackers who break into a computer.'" (quotations omitted)). In other words, the court in *Nosal* read the legislative history to support the narrow interpretation, while the court in *Phillips* read the history to allow for use restrictions against employees, thereby ultimately adopting the broad interpretation.

166. The court in *Drew* agrees: "Section 1030(a)(2)(C) does not set forth clear guidelines or objective criteria as to the prohibited conduct in the Internet/website or similar contexts." *Drew*, 259 F.R.D. at 466 (quotations omitted).

because it is vague. The CFAA is similar to the California ordinance struck down in *Kolender*. There, the Court held the definition for the phrase "credible and reliable" was vague: "carrying reasonable assurance that the identification is authentic and providing means for later getting in touch with the person who has identified himself."[167] The Court could not figure out what exactly authentic identification meant. Here, the phrases "without authorization" and "exceeds authorized access" are also vague. Do they impose a use or access restriction?[168] Second, the CFAA leads to discriminatory enforcement because it does not require an employer who suffered a broken promise to call the police. No complaining is necessary.[169] The police can just go after someone on a "whim."[170] Third, there is no requirement that there be actual loss or damage suffered by the employer.[171] Fourth, there is really no scienter requirement. The only one provided is that the person must "intentionally" access a computer "without authorization" or must intentionally "exceed[ ] authorized access" on it.[172] What does this really mean though? As the court in *United States v. Drew* wrote, "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."[173] Ultimately, the CFAA permits a "standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections."[174]

D. *Applying the Private Nondelegation Principle to the CFAA*

Under the broad interpretation, the CFAA raises a legitimate private delegation problem in violation of the Due Process Clause. Here, Congress gave the power to delineate a criminal sanction to private parties. The delineation occurs in agency or contract theory jurisdictions. In the agency setting, it happens when the employee and employer have an agency relationship. In the contractual setting, it occurs when two parties agree to the terms of a contract. Without a doubt, "[a] statute that criminalizes violating these agreements—often adhesion contracts, seldom read, drafted to benefit only the party who controls access, and subject to modification—essentially abdicates the legislative role to self-interested private parties."[175] Congress has no right to

167. Kolender v. Lawson, 461 U.S. 352, 356 (1983).

168. What is more, an argument can be made that the definition for "credible and reliable" was less vague than the definition here for "exceeds authorized access." At least in that definition, the word "reasonable" was used. Here, there is no reasonable requirement courts must utilize to determine when a user surpasses their authority on a computer.

169. *Drew*, 259 F.R.D. at 466 ("[S]ection 1030(a)(2)(C) is not limited to instances where the website owner contacts law enforcement to complain about an individual's unauthorized access or exceeding permitted access on the site." (footnote omitted)).

170. Shuttlesworth v. City of Birmingham, 382 U.S. 87, 90 (1965).

171. *Drew*, 259 F.R.D. at 467.

172. *Id.*

173. *Id.*

174. Smith v. Goguen, 415 U.S. 566, 575 (1974).

175. *Vagaries of Vagueness*, *supra* note 148, at 768.

"delegate federal criminal lawmaking to self-interested, unsupervised, and democratically unaccountable private parties."[176] The CFAA fails the three-prong inquiry and is an impermissible private delegation of lawmaking power.

Starting with the most important prong, the CFAA fails to provide any means of government involvement. This case is opposite the *Sunshine Anthracite Coal Co. v. Adkins* case. There, the Court held the private delegation was valid because the private coal boards' recommendations for coal prices were subject to government oversight. Each coal board's recommendations had to be approved, disapproved, or modified by the National Bituminous Coal Commission. Here, no government agency approves, disapproves, or modifies the terms of the contract between employer and employee. They set the terms of the contract, and that is it.[177] Ultimately, this case is analogous to *Carter Coal Co.*, where the Court held the statute unconstitutional partly because there was no government oversight.

The remaining two prongs may or may not suggest the CFAA is invalid. The first prong asks whether the delegation authorizes private actors to make law in a neutral, transparent way. This is difficult to determine in the contract setting. In the CFAA context, the court will have to look to the facts of the case at hand to see if the contract agreed to is neutral, or fair, to both parties. Do employees have a voice when negotiating a contract? Do users have one when accepting a website's terms of service agreement? The answer to both questions is that they most certainly do. But courts should look to the realities of the situation. Often times, employees accepting a contract or those accepting a website's terms of service do not read the lengthy text.[178] Even if they did, many of these agreements are subject to unilateral modification without a notice requirement.[179] Courts also should look to the disparities in negotiating power between employer and employee to determine if it is neutral. As for transparency issues under the first prong, they perennially exist in the CFAA context—the government is leaving it to the private parties to set the terms of the contract. The government has no involvement in the process.

As for the last prong, the courts look to whether affected parties are adequately represented in the private lawmaking process. Again, courts can look to the nature of the contract and the power imbalance between the negotiating parties to find the answer. They should also

176. *Id.* at 761.

177. Well, not completely it. The agreement must "compl[y] with the strictures of the relevant jurisdiction's contract laws." *Id.* at 769 (footnote omitted).

178. Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), http://www.wired.com/2013/06/aarons-law-is-finally-here/ ("Millions of Americans . . . routinely submit to legal terms and agreements every day when they use the Internet. Few have the time or the ability to read and completely understand the lengthy legal agreements.").

179. *Vagaries of Vagueness*, *supra* note 148, at 771 ("[A]greements criminally enforceable under the CFAA are 'lengthy, opaque, subject to change and seldom read,' not to mention extremely broad and subject to unilateral modification" (quoting United States v. Nosal, 676 F.3d 854, 860, 862 (9th Cir. 2012))).

look for the existence of a "representative process." In the CFAA setting, it seems there is one: the negotiation phase of the contract. However, the question remains whether employees and users of a website's terms of service are actually reading the text at hand.

VI. Conclusion and Immediate Proposal

The broad reading of the CFAA must end. The statute places millions of unsuspecting Americans in harm's way every single day they access a computer at work or an Internet website in which they agree to a terms of service. To begin, the history of the CFAA is unsettling. It indicates Congress has repeatedly expanded the scope of liability of the CFAA. Congress originally passed the then-CCCA to target outside hackers. Yet, through amendments, the CFAA has come to punish inside hackers, or employees who misuse their computers. Just like the history of the CFAA, its statutory framework is also unsettling. The CFAA fails to define the phrase "without authorization" and poorly defines the phrase "exceeds authorized access," leaving the statute vulnerable to a broad interpretation. Then, the statute defines "protected computer" broadly. A protected computer is any computer that "affects" interstate commerce, which presumably includes computers that are not even connected to the Internet but that in the aggregate affect interstate commerce. What is more, the statute does not really impose a scienter requirement. It only punishes persons who intend to use a computer, not persons who intend to use a computer in such a way as to lose authorization. This is such a poor requirement that the statute might as well impose strict liability.

This Note proposes that one way to defeat the CFAA, or at least to stop its broad reading, is to argue that it is unconstitutional. The first reason is the statute is void for vagueness. It fails to provide a person of ordinary intelligence notice of what behavior is culpable. The fact that there is a circuit split on how to read the statute indicates that it fails to provide such notice. Furthermore, the statute leads to discriminatory enforcement. It provides no minimal guidelines to police. Should police wish, they can go after someone like weev in *United States v. Auernheimer*, who obtained publically available information online, or someone like the defendant in *Lee v. PMSI, Inc.*, who violated his employment contract by accessing Facebook at work, or even someone like the defendant in *United States v. Drew*, who violated MySpace's terms of service. The second reason the statute is unconstitutional is because it is an impermissible private delegation of lawmaking power. Congress has empowered the writers of a contract or terms of service with the ability to define when a crime occurs. Every provision the employee breaks in the contract makes that employee liable in theory for a federal crime. This is alarming, considering that most employees and users do not read the lengthy text of the contracts or terms of service agreements they sign.

The Supreme Court has thus far denied certiorari concerning the reading of the CFAA. Even if proponents can argue the CFAA is uncon-

stitutional, it does not matter if the Court refuses the issue. Perhaps, proponents can look to the executive branch. It is true that President Obama has entertained expanding the reach of the CFAA.[180] Although his changes would impose liability for breaching a written contract—lending credence to the broad approach—it would only occur in three situations: (1) when a user violates a written contract in conjunction with a government computer, (2) when a user takes information worth $5,000 or more from a computer, or (3) when a user breaches a written contract in furtherance of committing a state or federal crime.[181] Still, even the President's proposals will take time to implement since they must pass through Congress. Thus, in the immediate future, the President can choose the route of discretionary nonenforcement. He can choose to not enforce the broad interpretation—except for in the three circumstances of his proposal. There is both case precedent and legal authority supporting the notion that the President does not have to enforce unconstitutional laws.[182] The CFAA, this Note contends, is an unconstitutional law.

---

180. *See, e.g.*, Kerr, *supra* note 91 ("[The CFAA] could expand liability in some undesirable ways."); Orin Kerr, *Obama to Propose Expanding the Computer Crime Laws (Again)*, VOLOKH CONSPIRACY (Jan. 13, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/13/obama-to-propose-expanding-the-computer-crime-laws-again/; Dave Smith, *Computer Fraud and Abuse Act 2013: New CFAA Draft Aims to Expand, Not Reform, the 'Worst Law in Technology'*, INT'L BUS. TIMES (Mar. 28, 2013, 12:06 PM), http://www.ibtimes.com/computer-fraud-abuse-act-2013-new-cfaa-draft-aims-expand-not-reform-worst-law-technology-1158515; Jim Garland, *President Obama Seeks to Strengthen and Clarify Cybercrime Law Enforcement*, INSIDEPRIVACY (Jan. 16, 2015), http://www.insideprivacy.com/uncategorized/president-obama-seeks-to-strengthen-and-clarify-cybercrime-law-enforcement/; Julie Hirschfeld Davis, *Obama Calls for New Laws to Bolster Cybersecurity*, N. Y. TIMES (Jan. 13, 2015), http://www.nytimes.com/2015/01/14/us/obama-to-announce-new-cyberattack-protections.html?_r=0. For the text of President Obama's new proposal to the CFAA, see *Updated Administration Proposal: Law Enforcement Provisions*, WHITE HOUSE (Jan. 13, 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf [hereinafter *Updated Administration Proposal*].

181. *See* Kerr, *supra* note 91 (explaining the three situations); *Updated Administration Proposal*, *supra* note 180 (showing the language of the proposed changes).

182. For excellent sources analyzing presidential discretionary nonenforcement, see Zachary S. Price, *Enforcement Discretion and Executive Duty*, 67 VAND. L REV. 671 (2014); Kate Andrias, *The President's Enforcement Power*, 88 N.Y.U. L. REV. 1031 (2013); Robert J. Delahunty & John C. Yoo, *Dream On: The Obama Administration's Nonenforcement of Immigration Laws, the DREAM Act, and the Take Care Clause*, 91 TEX. L. REV. 781 (2013).