NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
15 N.C. J.L. & TECH. ON. 205 (2014)

DO NOT READ THIS ARTICLE AT WORK: THE CFAA'S VAGUENESS PROBLEM AND RECENT LEGISLATIVE ATTEMPTS TO CORRECT IT

Ryan H. Niland*

The Computer Fraud and Abuse Act ("CFAA"), the nation's leading anti-hacking statute, criminalizes unauthorized access to any computer in the world. The CFAA does not specify what types of computer use qualify as unauthorized access, and circuit courts are split over approaches to defining the term. Although some courts have held that violations of private contracts such as employment agreements or website Terms of Service agreements constitute unauthorized access to a computer, others have held that such a broad reading renders the CFAA unconstitutionally vague. In the past year, lawmakers have introduced bills to clarify the conduct prohibited by the CFAA. Although each proposal narrows the scope of the CFAA, only one—Aaron's Law—provides sufficient clarity to correct the CFAA's vagueness problem.

I. INTRODUCTION

Are you reading this sentence on a computer at work? Have you ever exaggerated your best qualities on a dating website, or used a family member's Facebook account? Have you ever used a work computer to check the weather or your personal email, or borrowed a friend's password for a video streaming service such as Hulu or Netflix? If so, you may have violated the Computer Fraud and Abuse Act[1] ("CFAA"), the primary federal anti-hacking

* J.D. Candidate, University of North Carolina School of Law, 2015. The author would like to thank Professor Rob Smith, Katherine Street, Agnieszka Zmuda, and the rest of the NC JOLT editorial staff for their assistance in preparing and proofreading this article. Special thanks to Carley Niland for patiently sitting through countless verbal drafts of this article when she could have been watching reruns of Arrested Development on Netflix.

[1] 18 U.S.C. § 1030 (2012). Hereinafter, the terms "unauthorized access" and "hacking" are used to refer generally to any activity prohibited by the CFAA.

statute, which prohibits unauthorized access to any computer in the world.[2]

Unfortunately, the CFAA does not clearly define what types of activities qualify as unauthorized access to a computer. As a result, the question of whether seemingly innocent activities like those mentioned above should be treated as hacking often depends on the discretion of federal prosecutors and the wording of private contracts, such as an employment agreement or a website's Terms of Service ("TOS"). As a few recent high profile cases have demonstrated, the CFAA affords prosecutors so much discretion that almost anyone who regularly uses the Internet could be charged with a federal computer crime.[3] This has prompted both scholarly and judicial concern that the CFAA, as currently worded, may be unconstitutionally vague.[4]

This Recent Development analyzes three recent legislative proposals designed to correct the CFAA's vagueness problem. Part II provides background on the scope of the CFAA, including the class of computers the statute protects and the scope of activities it prohibits. Part III explains the CFAA's vagueness problem and the three major approaches courts have taken to defining hacking under the statute. Part IV summarizes a few high-profile CFAA prosecutions and examines three bills recently introduced in Congress in response to these controversial cases. Part V analyzes each bill and argues that only one—Aaron's Law—defines unauthorized access with sufficient specificity to correct the CFAA's vagueness problem.

---

[2] *See* United States v. Nosal, 676 F.3d 854, 860–63 (9th Cir. 2012) (en banc) (discussing the range of seemingly innocent activities that could qualify as hacking under a broad reading of the CFAA).

[3] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1582 (2010). This concern is not merely academic; at least one person has been prosecuted under the CFAA for misusing the social networking website MySpace. See discussion of *United States v. Drew*, *infra* Part IV.A.

[4] *See Nosal*, 676 F.3d at 860–63 (discussing the range of seemingly innocent activities that could qualify as hacking under a broad reading of the CFAA); Kerr, *Vagueness Challenges*, *supra* note 3, at 1575–78 (arguing that the void for vagueness doctrine requires courts to adopt a narrow construction of the CFAA).

II. THE SCOPE OF THE CFAA

The CFAA has expanded dramatically over the course of its thirty-year history.[5] Congress has repeatedly amended the CFAA to increase both the class of computers protected by the statute and the scope of conduct it prohibits, such that the CFAA's reach is now "breathtakingly broad."[6] As a result, what began as a relatively narrow statute designed to protect national security secrets and financial records has morphed into "one of the most far-reaching criminal laws in the United States Code."[7]

A. *The Class of Computers Protected by the CFAA*

The CFAA began as three small provisions in the Comprehensive Crime Control Act of 1984.[8] The Act—the first federal computer criminal statute[9]—prohibited "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend."[10] Although this language prohibits a very broad range of conduct, the Act also included additional requirements that effectively limited its reach to three specific contexts: obtaining secret information pertaining to national security, obtaining personal financial information, and hacking computers owned by the federal government.[11]

---

[5] *See generally* Kerr, *Vagueness Challenges*, *supra* note 3, at 1563–71 (providing a detailed history of the amendments to the CFAA).

[6] *Id.* at 1576.

[7] *Id.* at 1561.

[8] *Id.* at 1563–64 (citing the Comprehensive Crime Control Act of 1984 § 2102(a), Pub. L. No. 98-473, 98 Stat. 1976, 2190 [hereinafter *CCCA*]). Two years later, Congress passed the Computer Fraud and Abuse Act of 1986, which, in addition to providing the name for the federal anti-hacking statute, significantly expanded the law's scope. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, 1214 (codified as amended at 18 U.S.C. § 1030 (2012)) [hereinafter *CFAA of 1986*].

[9] Kerr, *Vagueness Challenges*, *supra* note 3, at 1564.

[10] *CCCA* § 2102(a)(1)–(3).

[11] *See id.* § (a)(1) (prohibiting accessing a computer in order to obtain information pertaining to "national defense or foreign relations"); *id.* § (a)(2) (prohibiting unauthorized access to a computer in order to obtain "financial

Congress amended the CFAA five times over the next quarter century, expanding the class of computers protected with each amendment.[12] Today, the CFAA prohibits unauthorized access to any "protected computer,"[13] a term it defines as including any computer "in or affecting interstate commerce or communication."[14] The phrase "in or affecting interstate commerce" signals Congress's intent to regulate an activity as far as the Commerce Clause will allow.[15] The Commerce Clause permits Congress to regulate even purely local activities so long as those activities could potentially affect interstate commerce in the aggregate.[16]

---

record[s] of a financial institution"); *id.* § (a)(3) (prohibiting unauthorized access to a computer in order to modify, destroy, or disclose information "operated for on behalf of the Government of the United States"); *see also* Kerr, *Vagueness Challenges*, *supra* note 3, at 1564 (discussing the CCCA).

[12] *See* Former Vice President Protection Act of 2008, Pub. L. No. 110-326, 122 Stat. 3560 (expanding protection to cover any computer "which is used in or affecting interstate or foreign commerce"); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272 (extending protection to computers located outside the United States); Economic Espionage Act of 1996, Pub. L. 104-294, tit. II, 110 Stat. 3488, 3492 (prohibiting unauthorized access of any kind to any computer when the conduct involves interstate communication); Violent Crime and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (expanding the computer damage provision to apply even when the damage occurred accidentally); *CFAA of 1986*, 100 Stat. at 1214 (adding prohibitions against unauthorized access to computers with intent to defraud, damage information worth more than $1,000, or traffic in computer passwords). *See generally* Kerr, *Vagueness Challenges*, *supra* note 3, at 1563–71 (providing a detailed history of the amendments to the CFAA).

[13] 18 U.S.C. § 1030(a)(2)(C) (2012).

[14] *Id.* § 1030(e)(2)(B).

[15] *See* Kerr, *Vagueness Challenges*, *supra* note 3, at 1567–68 (citing United States v. Chesney, 86 F.3d 564, 571 (6th Cir. 1996)). The Commerce Clause permits Congress to "regulate commerce with foreign nations, and among the several states, and with the Indian tribes." U.S. CONST. art. I., § 8, cl. 3.

[16] *See* Gonzales v. Raich, 545 U.S. 1, 32–33 (2005) (holding that Congress may prohibit the consumption of homegrown marijuana because the aggregate effect of such activity could affect the national marijuana market); Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 261–62 (1964) (holding that Congress may prohibit racial discrimination in hotel chains because such discrimination affects the feasibility of interstate travel and thus interstate commerce); Katzenbach v. McClung, 379 U.S. 294, 304–05 (1964) (holding that

Given the ubiquity of computers as tools of interstate commerce, the term "protected computer" now essentially means "all computers, period."[17] With the exception of handheld calculators and electric typewriters,[18] the CFAA now arguably regulates access to every device in the world that contains a microchip.[19] As a result, the CFAA has become "one of the most far-reaching criminal laws in the United States Code," potentially affecting nearly every aspect of modern life.[20]

B. *Scope of the Types of Conduct Prohibited by the CFAA*

The CFAA contains seven separate—and often overlapping—criminal provisions.[21] For example, Section (a)(1) prohibits unauthorized access to computers containing national security

---

Congress may prohibit racial discrimination in restaurants because such discrimination affects the feasibility of interstate travel and, thus, interstate commerce); Wickard v. Filburn, 317 U.S. 111, 128–29 (1942) (holding that Congress may regulate homegrown wheat because widespread consumption of such wheat could affect national wheat prices).

[17] Kerr, *Vagueness Challenges*, *supra* note 3, at 1571 (citing 18 U.S.C. § 1030(e)(2)(B)).

[18] The CFAA excludes "automated typewriter[s]," "portable handheld calculator[s]," and "other similar device[s]" from its definition of the term "computer." 18 U.S.C. § 1030(e)(1).

[19] Kerr, *Vagueness Challenges*, *supra* note 3, at 1571. Apart from the exceptions mentioned above, any "high speed data processing device performing logical, arithmetic, or storage functions" qualifies as a computer under the CFAA. 18 U.S.C. § 1030(e)(1). This presumably encompasses not just desktop and laptop computers, but also video game consoles, smartphones, many televisions and Blu Ray Disc players, and any other device that stores or processes digital information. In addition, many commentators have predicted the advent of an "Internet of Things" in which smart refrigerators, thermostats, and other household appliances communicate with each other. Geoff Duncan, *You Can't Avoid the 'Internet of Things' Hype, So You Might As Well Understand It*, DIGITAL TRENDS (Jan. 24, 2014), http://www.digitaltrends.com/home/heck-internet-things-dont-yet/#!zbOYA. If these predictions prove accurate, the CFAA may one day regulate access to every electronic device in many American homes.

[20] Kerr, *Vagueness Challenges*, *supra* note 3, at 1561.

[21] *See* 18. U.S.C. § 1030(a)(1)–(7).

information.[22] Section (a)(4) prohibits accessing a computer to fraudulently obtain items or information of value,[23] essentially the digital equivalent of wire fraud.[24] Section (a)(5) prohibits intentional or reckless computer use that results in damage to a protected computer,[25] and Section (a)(6) prohibits trafficking in passwords or other confidential information.[26] But perhaps the CFAA's most important criminal provision is contained in Section (a)(2)(C).[27]

Section (a)(2)(C) functions as a kind of catchall provision within the CFAA. The section provides that any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby *obtains information* from *any protected computer*" violates the CFAA.[28] This deceptively simple language dramatically increases the scope of conduct that could potentially qualify as hacking. Because any interaction between a human and a computer (or between computers on a common network such as the Internet) involves an exchange of some type of information, Section (a)(2)(C) regulates all forms of computer use, including activities as simple as viewing a login page or visiting a website.[29] In addition, given the immense scope

---

[22] *See id.* § 1030(a)(1) (prohibiting unauthorized access to information that "could be used to the injury of the United States, or to the advantage of any foreign nation").

[23] *See id.* § 1030(a)(4) (prohibiting accessing any protected computer "knowingly and with intent to defraud").

[24] *See* Kerr, *Vagueness Challenges*, *supra* note 3, at 1565.

[25] *See* 18 U.S.C. § 1030(a)(5)(A)–(C) (prohibiting unauthorized access that "intentionally" or "recklessly" results in damage to a computer).

[26] *See id.* § 1030(a)(6) (prohibiting trafficking in "password[s] or similar information through which a computer may be accessed without authorization").

[27] In addition to the provisions already mentioned, the CFAA also prohibits unauthorized access to nonpublic government computers. *See id.* § 1030(a)(3) (prohibiting unauthorized access to any "nonpublic computer of a department or agency of the United States"). Finally, the CFAA also prohibits computer use that facilitates extortion. *See id.* § 1030(a)(7) (prohibiting accessing a computer "with intent to extort from any person any money or other thing of value").

[28] 18 U.S.C. § 1030(a)(2)(C) (emphasis added).

[29] *See* Kerr, *Vagueness Challenges*, *supra* note 3, at 1585–86 ("[B]ecause [visiting a website] uses a computer, it is also technically 'accessing' a protected computer. Each visit, each checking, and each viewing involves entering a

of the term "protected computer,"[30] Section (a)(2)(C) effectively regulates the use of every computer in the world.[31]

Section (a)(2)(C) essentially regulates all forms of computer use, thus, criminal liability under the CFAA depends almost entirely on whether a prosecutor considers a particular activity to be authorized or unauthorized.[32] Every criminal provision in the CFAA prohibits accessing a computer "without authorization,"[33] and three provisions—most notably the catchall Section (a)(2)(C)—prohibit "exceed[ing] authorized access" to a computer.[34] Yet, despite the paramount importance of these terms, the CFAA provides almost no guidance to distinguish between authorized and unauthorized forms of computer use. The statute does not define the term "without authorization," and its definition of the term "exceeds authorized access" is essentially redundant.[35] This failure to provide even basic guidance about the meaning of the CFAA's most important terminology has major implications for the statute's constitutionality.

III. THE CFAA'S VAGUENESS PROBLEM

In the early days of the CFAA, the types of conduct that qualified as unauthorized access to a computer were reasonably

---

command into a computer network and retrieving information from the server.").

[30] The term "protected computer" includes any computer "which is used in or affecting interstate commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). The CFAA arguably covers every type of device that contains a microchip other than handheld calculators and electric typewriters. Kerr, *Vagueness Challenges*, *supra* note 3, at 1571.

[31] See discussion of devices covered by the CFAA, *supra* Part II.A.

[32] David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 927 (2013).

[33] 18 U.S.C. § 1030 (a)(1)–(7).

[34] *Id.* § 1030(a)(1), (a)(2), (a)(4).

[35] *See* 18 U.S.C. § 1030(e)(6) ("[T]he term 'exceeds authorized access' means to access to a computer with authorization and to use such access to obtain or alter information in the computer that the user is not entitled so to obtain or alter.").

clear.[36] Relatively few Americans used computers at all,[37] and even fewer interacted with CFAA-protected computers such as government computers or computers containing national security or financial information.[38] In addition, individuals seeking to access computers in the pre-Internet era either had to be physically present with the machine itself or dial in over a phone line and provide a username and password.[39] As a result, users would likely need to either break into a restricted room or steal login credentials from an authorized user in order to gain unauthorized access to CFAA-protected computers.

In recent years, courts have increasingly struggled to define the boundaries of unauthorized access as both computer technology and the CFAA have changed.[40] Most Americans now carry CFAA-protected devices in their pockets and interact with computers almost constantly throughout the day at school, work, and home.[41] Because many devices now synchronize seamlessly or automatically exchange and update information over the Internet, modern computer users may access dozens or even hundreds of CFAA-protected devices each day without even realizing it.[42]

---

[36] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1640–41 (2003).

[37] According to the U.S. Census Bureau, only 8.2% of U.S. households had a computer at home in 1984, and 59% of those home computer users were still learning how to use them. United States Census Bureau, *Measuring America*, http://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf (last visited Feb. 18, 2014). By 2012, 78.9% of U.S. households had a computer at home. *Id.*

[38] See discussion of devices covered by the CFAA, *supra* Part II.A.

[39] Kerr, *Cybercrime's Scope*, *supra* note 36, at 1640–41.

[40] *See, e.g.*, United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc); LVRC Holdings v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001).

[41] According to the U.S. Census Bureau, 78.9% of U.S. households had a computer at home in 2012, and 94.8% of those households used those devices to connect to the Internet. U.S. Census Bureau, *supra* note 37. In addition, almost half of all American individuals ages twenty-five and over carried smartphones in 2012. *Id*.

[42] Kerr, *Cybercrime's Scope*, *supra* note 36, at 1641.

Although this problem could potentially affect anyone who regularly uses the Internet,[43] the issue is litigated most often in employment cases involving "malicious insiders," such as employees who abuse their permission to access their employers' computers or networks.[44]

A. *The Contract and Agency Approaches to Unauthorized Access*

Early courts confronting the problem of malicious insiders adopted a broad interpretation of unauthorized access, using contract law as a way to hold employees accountable for misusing their employers' proprietary information.[45] In *EF Cultural Travel BV v. Explorica, Inc.*,[46] the First Circuit held a group of former employees liable for damages after they disclosed proprietary information accessed through company computers in violation of a confidentiality agreement with their employer.[47] The court

---

[43] Kerr, *Vagueness Challenges*, *supra* note 3, at 1582; *see also infra* Part III.C.

[44] *See* Danielle E. Sunberg, Note, *Reining in the Rogue Employee: The Fourth Circuit Limits Employee Liability Under the CFAA*, 62 AM. U. L. REV. 1417, 1424–29 (2013) (discussing the circuit split regarding the appropriate interpretation of "exceeds authorized access" in employment cases). These malicious insiders take a significant toll on commerce. According to one study, 60% of employees who quit or are asked to leave a company steal business data before leaving their jobs. Brian Krebs, *Data Theft Common by Departing Employees*, WASHINGTON POST (Feb. 26, 2009, 12:15 PM), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html. The most frequently stolen types of data included email lists, customer contact lists, employee records, and financial information. *Id.*

[45] *See, e.g.*, United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (holding an employee liable because "Citigroup's official policy, which was reiterated in training programs that John attended, prohibited misuse of the company's internal computer systems and confidential customer information."); *Explorica*, 274 F.3d at 582 ("Congress defined 'exceeds authorized access' as accessing 'a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.' EF is likely to prove such excessive access based on the confidentiality agreement between Gormley and EF.") (internal citations omitted).

[46] 274 F.3d 577 (1st Cir. 2001).

[47] *Id.* at 582–84. In addition to its criminal provisions, the CFAA also provides a civil cause of action that permits victims to recover damages from individuals who violate the statute. 18 U.S.C. § 1030(g).

reasoned that the employees' authorization to use the company's computers derived from their employment agreements, and thus any activity forbidden by those agreements necessarily exceeded their authorization to use the computers.[48] Under this "contract approach," any violation of a private contract governing the use of a particular computer or network, such as an employment agreement or TOS, could classify a user's computer use as unauthorized.[49]

Although the First Circuit adopted the contract approach in a civil case, other courts have used this reasoning to hold employees criminally liable for breaching contracts with their employers. In *United States v. John*,[50] the Fifth Circuit held that a group of Citigroup employees could be held criminally liable for violating their employment agreements by passing confidential customer information to outsiders.[51] The Eleventh Circuit followed a similar approach in *United States v. Rodriguez*,[52] holding a Social Security Administration employee criminally liable for violating his employment agreement by viewing personal information about several different women.[53]

The Seventh Circuit takes an even broader approach to unauthorized access. In *International Airport Centers, LLC v. Citrin*,[54] the court held an employee liable for deleting information from his company-provided computer before quitting to start a competing business.[55] The employee's actions arguably violated his employment agreement,[56] but the court justified its decision to hold the employee liable in terms of agency law rather than contract law.[57] The court reasoned that the employee's permission

---

[48] *Explorica*, 274 F.3d at 582–84.
[49] *See* Sunberg, *supra* note 44, at 1425–26.
[50] 597 F.3d 263 (5th Cir. 2010).
[51] *Id.* at 271–73.
[52] 628 F.3d 1258 (11th Cir. 2010).
[53] *Id.* at 1263–64.
[54] 440 F.3d 418 (7th Cir. 2006).
[55] *Id.* at 419.
[56] *See id.* at 421 (discussing a clause in the employee's contract permitting him to "return or destroy" data on the laptop upon termination of employment).
[57] The court's reliance on agency law may have stemmed from a quirk in the CFAA's wording. Because the employer sued under Section (a)(5) of the CFAA, which prohibits accessing a computer "without authorization" but does

to access his work computer derived from his position as an agent for his employer, and that his authority as an agent terminated as soon as his interests became adverse to those of his employer.[58] Thus, the court concluded that the employee's permission to access his company-issued computer terminated the moment he decided to leave his employer and start a competing company.[59] Under this extremely broad "agency approach," an individual's motivations may transform otherwise permissible forms of computer use into access "without authorization."[60] And because employees are necessarily agents of their employers,[61] any computer activity by an employee that does not further the employer's interests could be construed as criminal hacking under the CFAA.[62]

B. *Vagueness Concerns with the Contract and Agency Approaches*

The contract and agency approaches have received extensive academic criticism.[63] Some commentators have expressed concern that the contract and agency approaches render the CFAA overbroad, criminalizing activities that cause little or no social harm.[64] In addition, leading cybercrime scholar Orin Kerr has

---

not prohibit "exceed[ing] authorized access" to a computer, the court could not simply rely on the contract approach to characterize the defendant's actions as exceeding his authorization. *See id.* at 419.

[58] *Id.* at 420–21.

[59] *Id.* at 418–20.

[60] Sunberg, *supra* note 44, at 1424–25.

[61] *See* RESTATEMENT (THIRD) OF AGENCY § 7.07(3)(a) (2006) ("[A]n employee is an agent whose principal controls or has the right to control the manner and means of the agent's performance of work.").

[62] Katherine Mesenbring Field, *Agency, Code or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 823 (2009). For examples of seemingly innocent activities that could qualify as hacking under the agency approach, see *infra* Part III.C.

[63] *See, e.g.*, Kerr, *Vagueness Challenges*, *supra* note 3, at 1575–85 (arguing that the contract approach renders the CFAA unconstitutionally vague); Kerr, *Cybercrime's Scope*, *supra* note 36, at 1633–40 (criticizing *Explorica* and other contract approach cases).

[64] *See* Thaw, *supra* note 32, at 942 ("[T]erms-of-service based restrictions under current broader CFAA interpretations capture activities surely not intended by Congress to fall under the scope of criminal sanction."); *see also* United States v. Nosal, 676 F.3d 854, 860–63 (9th Cir. 2012) (en banc)

suggested that the contract and agency approaches render the CFAA so broad as to be unconstitutionally void for vagueness.[65]

The void for vagueness doctrine is rooted in the due process clauses of the Fifth and Fourteenth Amendments.[66] The doctrine provides two independent bases for invalidating criminal laws.[67] First, a criminal law is void for vagueness when it is "so vague and standardless that it leaves the public uncertain as to the conduct it prohibits,"[68] such that "men of common intelligence must necessarily guess at [the statute's] meaning."[69] In addition, a criminal law is void for vagueness when it fails to "establish minimal guidelines to govern law enforcement" in order to prevent "arbitrary and discriminatory enforcement."[70] Courts have used the void for vagueness doctrine to invalidate a variety of criminal laws that prohibited activities ranging from loitering[71] to desecrating the American flag.[72]

(discussing the range of seemingly innocent activities that could qualify as hacking under a broad reading of the CFAA).

[65] *See* Kerr, *Vagueness Challenges*, *supra* note 3, at 1576–78. Professor Kerr teaches courses in criminal law and computer crime law at the George Washington University and is among the most cited criminal law scholars in the United States. Professor Kerr has also served as a trial attorney in the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. *Faculty Directory, Orin S. Kerr*, LAW.GWU.EDU, http://www.law.gwu.edu/Faculty/profile.aspx?id=3568 (last visited Mar. 3, 2014).

[66] Kreimer v. Bureau of Police for the Town of Morriston, 958 F.2d 1242, 1246 (3d Cir. 1992) ("[T]he vagueness doctrine, unlike the overbreadth doctrine, additionally seeks to ensure fair and non-discriminatory application of the laws, thus reflecting its roots in the due process clause."); *see also* U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law."); U.S. CONST. amend. XIV, § 1 ("[N]or shall any State deprive any person of life, liberty, or property, without due process of law.").

[67] City of Chicago v. Morales, 527 U.S. 41, 57 (1999).

[68] Giaccio v. Pennsylvania, 382 U.S. 399, 402 (1966); *see also* Connally v. General Construction Co., 269 U.S. 385, 391 (1926) ("[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law.").

[69] Coates v. City of Cincinnati, 402 U.S. 611, 614 (1971) (citation omitted).

[70] Kolender v. Lawson, 461 U.S. 352, 357–58 (1983).

[71] *See, e.g.*, *Morales*, 527 U.S. at 47–48 n.2, 64 (invalidating an ordinance that prohibited "remain[ing] in any one place with no apparent purpose");

Although the void for vagueness doctrine consists of two independent and equal prongs,[73] the Supreme Court appears to be most concerned with the doctrine's second prong: adequate guidance to prevent discriminatory enforcement.[74] The void for vagueness doctrine does not demand "'impossible standards' of clarity" beyond what is necessary or practical to accomplish the law's purpose,[75] but the Court frequently expresses concern over laws it sees as encouraging "arbitrary and erratic arrests and convictions."[76] While the government may use criminal laws to regulate an extremely wide variety of activities, "[i]t cannot constitutionally do so through the enactment and enforcement of an ordinance whose violation may depend upon whether or not a policeman is annoyed."[77] Put another way, a criminal statute may not "set a net large enough to catch all possible offenders, and leave it to the courts to step inside and say who could be rightfully detained, and who should be set at large."[78]

Papachristou v. Jacksonville, 405 U.S. 156, 165–68 (1972) (invalidating an ordinance that prohibited "wandering or strolling around from place to place without any lawful purpose").

[72] Smith v. Goguen, 415 U.S. 566, 575 (1974) (invalidating a law that prohibited treating an American flag "contemptuously").

[73] *See generally* Michael C. Steel, *Constitutional Law—The Vagueness Doctrine: Two-Part Test, Or Two Conflicting Tests?* City of Chicago v. Morales*, 119 S. Ct. 1849 (1999)*, 35 LAND & WATER L. REV. 255, 257–63 (2000) (arguing that that the traditional understanding of the void for vagueness doctrine misapprehends Supreme Court precedent).

[74] *See Goguen*, 415 U.S. at 574 ("[P]erhaps the most meaningful 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.").

[75] *Kolender*, 461 U.S. at 361 (quoting United States v. Petrillo, 332 U.S. 1, 7–8 (1947)); *see also* Grayned v. City of Rockford, 408 U.S. 104, 110 (1972) ("Condemned to the use of words, we can never expect mathematical certainty from our language.").

[76] *Papachristou*, 405 U.S. at 162.

[77] *See* Coates v. City of Cincinnati, 402 U.S. 611, 614 (1971) (invalidating an ordinance that prohibited conduct on public streets that is "annoying to persons passing by").

[78] *Papachristou*, 405 U.S. at 165.

When interpreted in accordance with the contract and agency approaches, the CFAA appears to fail both prongs of the void for vagueness test.[79] First, the contract and agency approaches provide very little notice to the public regarding the conduct that could qualify as criminal hacking. Although the CFAA is not unique in its reliance on private contracts to define criminal behavior,[80] the employment contracts, TOS, and other contracts governing access to cyberspace differ markedly from contracts governing access to property in the physical world. Unlike contracts governing access to physical property, TOS are generally long, complex, and difficult to understand,[81] and most are presented to users as contracts of adhesion.[82] Service providers typically write these agreements in extremely broad terms in order to limit their own liability.[83] Employment contracts present similar concerns.[84] As a result, seemingly innocent conduct like checking personal email, visiting news sites, or checking the weather may qualify as criminal hacking under the contract and agency approaches,

---

[79] *See* Kerr, *Vagueness Challenges*, *supra* note 3, at 1575–78 (arguing that the void for vagueness doctrine demands that courts adopt "narrow" interpretations of the CFAA).

[80] Congress compared hacking to physical-world trespass as early as 1986. Thaw, *supra* note 32, at 913–14.

[81] *Id.* at 926.

[82] *See id.* at 922–23. A contract of adhesion is a contract "done on terms dictated by one contracting party to another who has no voice in its formulation." CORBIN ON CONTRACTS § 1.4 (1993). Courts sometimes refuse to enforce these "take it or leave it" contracts as unconscionable. *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. a (1981) ("It is to be emphasized that a contract of adhesion is not unconscionable per se, and that all unconscionable contracts are not contracts of adhesion. Nonetheless, the more standardized the agreement and the less a party may bargain meaningfully, the more susceptible the contract or a term will be to a claim of unconscionability.").

[83] Kerr, *Vagueness Challenges*, *supra* note 3, at 1582.

[84] *See id.* at 1585 ("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.").

depending on the wording of particular employment contracts or TOS.[85]

The contract and agency approaches also appear to fail the second prong of the void for vagueness doctrine, providing almost no guidance to prevent arbitrary or discriminatory enforcement of the CFAA. Under the agency approach, for example, prosecutors could charge employees or other agents for any computer-related activity that the prosecutor considers to be against the principal's interests.[86] And although the contract approach appears to be slightly narrower in theory, Professor Kerr argues that the contract approach may be equally broad in practice:

> Violating the TOS is the norm, complying with them the exception . . . 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. As a result, criminalizing TOS violations would for the most part give the government the ability to arrest anyone who regularly uses the Internet.[87]

Thus, in practice, the contract and agency approaches cast a large net over almost all forms of computer activity, leaving the question of which users should be prosecuted and which users should be spared almost entirely to the discretion of courts and local prosecutors.[88]

C. *The Code Approach to Unauthorized Access*

Perhaps in response to this criticism, some circuit courts have rejected the contract and agency approaches in recent years.[89]

---

[85] *See id.*

[86] *See* Field, *supra* note 62, at 823.

[87] Kerr, *Vagueness Challenges*, *supra* note 3, at 1582.

[88] In fact, as one recent case demonstrated, criminal liability may depend, not just on the discretion of local law enforcement, but on the discretion of prosecutors across the country. See discussion of *United States v. Drew*, *infra* Part IV.A.

[89] *See, e.g.*, United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) ("We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead. For our part, we continue to follow the path blazed by *Brekka*."); WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199,

Adopting the so-called "code approach,"[90] these courts hold that access to a computer only qualifies as unauthorized when the user circumvents some type of technological barrier designed to regulate access to a particular computer.[91] In *LVRC Holdings v. Brekka*,[92] the Ninth Circuit held that a disloyal employee did not violate the CFAA when he downloaded company documents and emailed them to his personal computer before leaving the company.[93] Rejecting *Citrin*'s agency approach in favor of what it considered to be the CFAA's plain meaning,[94] the court reasoned, "It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.' "[95] Accordingly, the court concluded that the employee did not exceed his authorization because the employer had not taken away his login credentials.[96]

205–06 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013) ("[W]e reject any interpretation that grounds CFAA liability on a cessation-of agency theory."); LVRC Holdings v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009) (declining to apply *Citrin* and concluding, "Brekka's use of LVRC's computers to email documents to his own personal computer did not violate [the CFAA] because Brekka was authorized to access the LVRC computers during his employment with LVRC.").

[90] Sunberg, *supra* note 44, at 1427–29. *See generally* Kerr, *Cybercrime's Scope*, *supra* note 36, at 1643–60 (arguing that computer misuse statutes should be constructed in terms of "regulation by code" rather than "regulation by contract").

[91] *See* Sunberg, *supra* note 44, at 1427–28.

[92] 581 F.3d 1127 (9th Cir. 2009).

[93] *Id.* at 1137.

[94] *See id.* at 1133 ("[Plain language analysis] leads to a sensible interpretation of §§ 1030(a)(2) and (4), which gives effect to both the phrase 'without authorization' and the phrase 'exceeds authorized access': a person who 'intentionally accesses a computer without authorization' accesses a computer without any permission at all, while a person who 'exceeds authorized access' has permission to access the computer, but accesses information on the computer that the person is not entitled to access.") (internal citations omitted).

[95] *Id.* at 1135.

[96] *Id.* at 1333–35. The court noted, however, that the employee's permission to access the computer would terminate as soon as he left the company. *Id.* at 1136 ("There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would

Subsequent decisions by the Ninth and Fourth Circuits followed *Brekka* in adopting the code approach and also expressed concerns that the contract and agency approaches may render the CFAA unconstitutionally vague.[97] In *United States v. Nosal*,[98] the Ninth Circuit rejected criminal liability for an employee who used confidential information from his employer's computers to start a competing company.[99] The court noted that the contract and agency approaches could potentially criminalize an extremely wide range of behaviors, from checking sports scores on a work computer to exaggerating one's attractiveness on a dating website.[100] Arguing that modern computer use "is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands,"[101] the court concluded that the contract and agency approaches do not provide sufficient notice to computer users as to what conduct the CFAA prohibits.[102]

In addition to lack of notice, the *Nosal* court expressed concern that the contract and agency approaches leave too much discretion in the hands of law enforcement. The court noted that the agency

---

have accessed a protected computer 'without authorization' for purposes of the CFAA.").

[97] *See* United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) ("We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead. For our part, we continue to follow the path blazed by *Brekka*."); WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 205–06 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013) ("[W]e reject any interpretation that grounds CFAA liability on a cessation-of agency theory.").

[98] 676 F.3d 854 (9th Cir. 2012) (en banc).

[99] *Id.* at 864.

[100] *Id.* at 860–61 ("Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars . . . Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit.").

[101] *Id.* at 861.

[102] *See id.* (arguing that, under the contract and agency approaches, "behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever").

and contract approaches could allow employers and prosecutors to use the CFAA as a pretense for discrimination against unpopular individuals.[103] The court also rejected the argument that courts should ignore theoretical vagueness concerns because prosecutors are unlikely to pursue criminal charges for minor violations in practice:

> The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor. And it's not clear we *can* trust the government when a tempting target comes along . . . . The difference between puffery and prosecution may depend on whether you happen to be someone [a federal prosecutor] has reason to go after.[104]

Arguing that "[u]biquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement,"[105] the court concluded that the contract and agency approaches render the CFAA unconstitutionally vague.[106]

As articulated in *Brekka* and *Nosal*, the code approach appears to limit CFAA liability to users who gain access to particular computers or information by circumventing a system's privileges or passwords.[107] Under the code approach, a user who "tricks" a restricted computer by using stolen login credentials to hide his identity could be liable as a hacker, but an employee who uses his own login credentials to download confidential information from a work computer would be subject only to civil liability for breach of contract and misuse of trade secrets.[108] Similarly, an employee who violates company policy by using a work computer to log into her

---

[103] *Id.* at 860 ("While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you could be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit.").

[104] *Id.* at 862 (internal citations omitted). In support of its concerns, the court cited *United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009). For a discussion of *Drew*, see *infra* Part IV.A.

[105] *Id.* at 860.

[106] *See id.* at 866 (Sullivan, J., dissenting) (characterizing the majority decision as implying that the agency approach renders the CFAA unconstitutionally vague).

[107] *See* Sunberg, *supra* note 44, at 1427.

[108] *See* Kerr, *Cybercrime's Scope*, *supra* note 36, at 1664–65.

own Facebook account would not be liable under the CFAA,[109] but an employee who hacks into her boss's Facebook account would be liable.

Although some commentators have expressed concern that the code approach may be difficult or unworkable in practice,[110] the approach appears to be gaining popularity in circuit courts. *Nosal* and *Brekka* remain good law in the Ninth Circuit, and the Fourth Circuit recently adopted the code approach out of concerns for the vagueness in the contract and agency approaches to the CFAA.[111] As a result, the circuit courts are now divided over the proper interpretation of the CFAA, with the First, Fifth, and Eleventh Circuits following the contract approach,[112] the Fourth and Ninth Circuits following the code approach,[113] and the Seventh Circuit following the agency approach.[114]

IV. LEGISLATIVE RESPONSES TO THE CFAA'S VAGUENESS PROBLEM

Despite the judicial and academic debate surrounding the CFAA, the Supreme Court appears to be uninterested in resolving the widening circuit split over unauthorized access.[115] Congress similarly failed to clarify the CFAA's definition of hacking

---

[109] *See id.* at 1665.

[110] *See, e.g.*, Thaw, *supra* note 32, at 928–34 (detailing various "practical, theoretical, and normative problems" with the code approach); Sunberg, *supra* note 44, at 1432 ("As the CFAA becomes a less viable option, employers will need to find alternative theories to hold employees accountable (e.g., contractual, tort, and state statutory remedies). The CFAA may only protect employers against circumvention of technological barriers to proprietary information, requiring additional provisions to protect against the misuse of such information.").

[111] *See* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204–06 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013).

[112] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

[113] *See Miller*, 687 F.3d at 204–06; United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).

[114] *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[115] The Court recently dismissed certiorari in *Miller*. *Miller*, 133 S. Ct. at 831.

throughout the 2000s.[116] A few recent high-profile prosecutions, however, have brought public attention to the law's ambiguities, rekindling legislative interest in reforming the CFAA.

A. *Recent High Profile CFAA Cases*

The CFAA's vagueness problem first received national attention in 2008 in response to the prosecution of Lori Drew.[117] Drew created a fake MySpace account to harass her daughter's thirteen-year old classmate, ultimately prompting the girl to commit suicide.[118] State and federal prosecutors in Missouri concluded that Drew had not committed a crime,[119] but federal prosecutors in MySpace's home state of California decided to pursue the case in order to send an "overwhelming message" to Internet users everywhere.[120] Prosecutors charged Drew with misdemeanor hacking for violating MySpace's TOS, which required that all information on profile pages be "truthful and accurate."[121] A jury convicted Drew, but the trial court ultimately vacated the conviction in response to the vagueness concerns expressed in *Brekka*.[122]

Perhaps the highest-profile CFAA case to date involved Internet activist Aaron Swartz. Swartz posed as a guest on the Massachusetts Institute of Technology's ("MIT") campus network

---

[116] Kerr, *Vagueness Challenges*, *supra* note 3, at 1583.

[117] *See id.* at 1579; *see also* Jennifer Steinhauer, *Woman Indicted in MySpace Suicide Case*, N.Y. TIMES (May 16, 2008), http://www.nytimes.com/2008/05/16/ us/16myspace.html?fta=y (reporting on the *Drew* indictment).

[118] United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009); *see also* Steinhauer, *supra* note 117 (claiming that the girl "committed suicide in response to [Lori Drew's] cyberbaiting").

[119] Kerr, *Vagueness Challenges*, *supra* note 3, at 1582–83.

[120] Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES (Nov. 26, 2008), http://www.nytimes.com/2008/11/27/us/27myspace.html. U.S. Attorney Thomas P. O'Brien later clarified that message, saying, "If you are going to attempt to annoy or go after a little girl, and you're going to use the Internet to do so, this office and others across the country will hold you responsible." *Id.*

[121] *Drew*, 259 F.R.D. at 454. Had they been so inclined, prosecutors could also have targeted MySpace cofounder Tom Anderson, who has also been accused of violating the TOS by lying about his age on his MySpace page. *See* Kerr, *Vagueness Challenge*, *supra* note 3, at 1582.

[122] *Drew*, 259 F.R.D. at 467–68.

in order to download a substantial portion of the articles in the academic research database JSTOR, a violation of JSTOR's TOS.[123] Although Swartz's motive remains unclear, it appears that he intended to make the articles available free of charge online.[124] Swartz avoided detection by using fictitious names and altering his computer's IP address,[125] eventually entering a restricted wiring closet on MIT's campus to plug his laptop directly into the network.[126] Prosecutors indicted Swartz on eleven felony counts under the CFAA, charges that potentially carried a thirty-five year prison sentence.[127] Swartz committed suicide shortly before his trial was to begin, prompting extensive public outcry.[128] In the wake of this controversy, lawmakers began to consider new legislative proposals to correct the CFAA's vagueness problem by clarifying the scope of unauthorized access.[129]

B. *Recent Legislative Proposals to Reform the CFAA*

On April 10, 2013—three months after Aaron's Swartz's death—Representative Marsha Blackburn[130] introduced the SECURE

---

[123] Superseding Indictment at ¶ 12–31, United States v. Swartz, 945 F. Supp. 2d 216 (D. Mass. 2012) (No. 11-CR-10260-NMG), 2012_WL_4341933 [hereinafter *Indictment*].

[124] *See id.* ¶ 31.

[125] *Id.* ¶ 12–22.

[126] *Id.* ¶ 25–31.

[127] *See id*, ¶ 36–43; Stephanie Francis Ward, *Hacker's Hell: After Broad Prosecutions—And One Suicide—Many Want to Narrow the Computer Fraud and Abuse Act*, 99-MAY A.B.A. J. 15, 15–16 (2013). Swartz was charged with five counts of computer fraud, five counts of unlawfully obtaining information from a protected computer, and one count of recklessly damaging a protected computer. *Indictment*, *supra* note 123, ¶ 36–43.

[128] Ward, *supra* note 127, at 16.

[129] *See* Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform to the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/.

[130] Representative Blackburn, a Republican, represents Tennessee's 7th District. *Congresswoman Marsha Blackburn: Biography*, HOUSE.GOV, http://blackburn.house.gov/biography/ (last visited Mar. 12, 2014).

IT Act of 2013.[131] The bill, which covers a wide variety of cyber and data security programs,[132] has been referred to the House Subcommittee on Research and Technology.[133] The SECURE IT Act would modify the CFAA by increasing the length of criminal sentences for hacking,[134] increasing punishments for unsuccessful attempts at hacking,[135] and creating the new offense of "aggravated" hacking for cases involving industries of public significance.[136]

The SECURE IT Act's most important modification to the CFAA relates to the definition of hacking itself. The Act attempts to ease concerns about overbroad CFAA prosecutions by explicitly limiting the scope of activities that qualify as unauthorized access to a computer. Specifically, the bill redefines the phrase "exceeds authorized access" to exclude:

> [A]ccess in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.[137]

This language appears to reject the contract approach to unauthorized access, at least in cases involving individuals other

---

[131] Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013, H.R. 1468, 113th Cong. [hereinafter *SECURE IT Act*].

[132] Among other things, the bill would require greater coordination and communication between public and private entities regarding threats to cybersecurity. *See id.* § 102. The bill would also amend the High-Performance Computing Act of 1991. *See id.* § 405.

[133] CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/house-bill/1468/actions?q=%7B%22search%22%3A%5B%22hr1468%22%5D%7D (last visited Mar. 23, 2014).

[134] *See SECURE IT Act* § 301 (tripling and doubling the maximum prison sentences for first time and repeat offenders, respectively).

[135] *See id.* § 303 (providing that attempted computer crimes shall be punishable to the same extent as completed crimes).

[136] *See id.* § 305 (creating a new offense for hacking that affects, among other things, the oil and gas industries, telecommunications, water supply systems, and emergency services).

[137] *Id.* § 306.

than government employees.[138] Under this approach, for example, the Citigroup employees in *John* could not have been prosecuted solely for violating their employment agreements.[139] Perhaps more importantly, prosecutors could not have targeted Lori Drew or Aaron Swartz solely for violating TOS agreements with MySpace or JSTOR.[140]

Republicans sponsored the SECURE IT Act, but Democrats have also expressed support for similar modifications to the CFAA. On January 8, 2014, Senator Patrick Leahy[141] introduced the Personal Data Privacy and Security Act of 2014[142] ("PDPSA"). Although the PDPSA has primarily received attention for its

---

[138] *See* Sunberg, *supra* note 44, at 1433–35 (discussing an earlier version of the SECURE IT Act and concluding that the bill would adopt the code approach).

[139] *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (holding an employee liable because "Citigroup's official policy, which was reiterated in training programs that John attended, prohibited misuse of the company's internal computer systems and confidential customer information"). Although the SECURE IT Act would have prevented most of the contract cases discussed above, the bill would not have prevented the prosecution in *Rodriguez* because the defendant in that case violated an employment agreement with the Social Security Administration, a government employer. *See* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

[140] Of course, it is not clear that Swartz's CFAA prosecutions were based *solely* on his violations of JSTOR's TOS. *See Indictment*, *supra* note 120, ¶¶ 11–31 (alleging that Swartz committed several arguably criminal acts, including installing mass-download software on MIT's network and entering a restricted wiring closet without permission). For a full discussion of the SECURE IT Act's implications, including its hypothetical impact on the Swartz prosecution, see *infra* Part III.C.

[141] Senator Leahy, a Democrat, represents the State of Vermont. *Senator Patrick Leahy: Biography*, SENATE.GOV, http://www.leahy.senate.gov/biography/ (last visited Mar. 12, 2014).

[142] Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. [hereinafter *PDPSA*]. The current bill is the fifth such proposal submitted by Senator Leahy since 2005. Brian Fung, *Prosecutors Used This Cybercrime Law Against Aaron Swartz. Now a Senator Wants to Strengthen It*, WASHINGTON POST (Jan. 9, 2014 10:19 AM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/prosecutors-used-this-cybercrime-law-against-aaron-swartz-now-a-senator-wants-to-strengthen-it/.

provisions requiring reporting of consumer data breaches,[143] the bill, which has been referred to the Senate Judiciary Committee,[144] also contains several sections devoted to reforming the CFAA. Like the SECURE IT Act, the PDPSA would create a new offense for "aggravated" hacking and would generally increase penalties for all forms of hacking and attempted hacking.[145]

The PDPSA also explicitly narrows the scope of the term "exceeds authorized access."[146] In fact, the PDPSA and SECURE IT Act contain identical provisions redefining the term, and both specifically excluding contract violations.[147]

The PDPSA also goes a step further, explicitly removing violations of private contracts from the CFAA's civil cause of action as well.[148] Thus, not only would the PDPSA prevent the criminal prosecutions based on facts similar to those of *Drew* and *John*, the bill would likely preclude civil claims on facts similar to those of *Explorica* as well.[149]

---

[143] *See* Brian Fung, *The Bright Side to the Target Hack? It's Getting Congress Moving*, WASHINGTON POST (Jan. 10, 2014, 3:36 PM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/10/the-bright-side-to-the-target-hack-its-getting-congress-moving/; *see also PDPSA* § 211 (requiring all businesses engaged in interstate commerce to notify consumers of security breaches affecting "sensitive personally identifiable information").

[144] CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/senate-bill/1897/actions?q=%7B%22search%22%3A%5B%22S1897%22%5D%7D (last visited Mar. 23, 2014).

[145] *See PDPSA* § 109 (creating an offense for aggravated hacking); *PDPSA* § 103 (increasing the length of punishments for computer fraud); *PDPSA* § 105 (providing that attempted computer crimes shall be punishable to the same extent as completed crimes).

[146] *PDPSA* § 110.

[147] *Compare id.*, *with SECURE IT Act* § 306.

[148] *PDPSA* § 107. This provision may be unnecessary, as the CFAA's civil cause of action is based entirely on violations of the Act's criminal provisions. *See* 18 U.S.C. § 1030(g) (2012) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[149] *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (holding an employee criminally liable for violating an employment contract); United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (discussing a criminal prosecution

The most notable attempt to harness the public outcry over Swartz's death is known as Aaron's Law.[150] Sponsored by Representative Zoe Lofgren[151] and Senator Ron Wyden,[152] identical versions of the bill have been referred to the House and Senate Judiciary Committees.[153] Unlike the SECURE IT Act and PDPSA, Aaron's Law does not seek to clarify the meaning of access that exceeds authorization. Instead, Aaron's Law removes that phrase from the CFAA entirely, leaving only the general prohibition against accessing a computer "without authorization."[154] The bill then clarifies the scope of the phrase "without authorization," defining the term as "knowingly circumvent[ing] one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals" from accessing particular information.[155] Thus, Aaron's Law essentially adopts the code approach to unauthorized access as articulated by the Ninth Circuit in *Brekka* and endorsed by the Fourth Circuit in *Miller*.[156]

---

based on the fact that the defendant's conduct "violated MySpace's terms of service"); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (holding a group of former employees civilly liable for violating their former employer's confidentiality agreement). Although the PDPSA would have prevented most of the contract cases discussed above, the bill would not have prevented the prosecution in *Rodriguez* because the defendant in that case violated an employment agreement with the Social Security Administration, a government employer. *See* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

[150] Aaron's Law Act of 2013, H.R. 2454, S. 1196, 113th Cong. [hereinafter *Aaron's Law*].

[151] Congresswoman Lofgren, a Democrat, represents California's 19th District. *Congresswoman Zoe Lofgren: Biography*, HOUSE.GOV, http://lofgren.house.gov/biography/ (last visited Mar. 10, 2014).

[152] Senator Wyden, a Democrat, represents the State of Oregon. *Ron Wyden: Senator for Oregon: Biography*, SENATE.GOV, http://www.wyden.senate.gov/ (last visited Mar. 10, 2014).

[153] *Actions, H.R. 2454*, CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/house-bill/2454/all-actions/?q=%7B%22search%22%3A%5B%22hr2454%22%5D%7D (last visited Mar. 23, 2014); *Actions, S. 1196*, CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/senate-bill/1196/actions?q=%7B%22search%22%3A%5B%22s1196%22%5D%7D (last visited Mar. 23, 2014).

[154] *Aaron's Law* § 2(a)–(b).

[155] *Id.* § 2(a)(2).

[156] Thaw, *supra* note 32, at 945.

Ironically, it is unlikely that Aaron's Law would have prevented its namesake's prosecution. Aaron Swartz arguably circumvented several technological and physical measures designed to restrict his access to JSTOR and, later, MIT's entire network. Among other things, Swartz allegedly altered his computer's client name and MAC address in order to mask the source of his download requests;[157] hard wired his computer directly into MIT's guest network in order to override the network's IP address system;[158] used a computer program called "keepgrabbing.py" to confuse JSTOR's code-based safeguards against mass downloads;[159] entered a restricted wiring closet on MIT's campus;[160] and used a bicycle helmet to hide his face from security cameras.[161] Regardless of Swartz's motivations, he clearly used his technological savvy to avoid MIT's and JSTOR's attempts to expel him from their networks. If proven, these accusations would amount to hacking under almost any reasonable definition of the term.

V. DO THE CURRENT PROPOSALS CORRECT THE CFAA'S VAGUENESS PROBLEM?

Although the SECURE IT Act, PDPSA, and Aaron's Law all narrow the scope of conduct that qualifies as hacking, these bills take very different approaches to solving the CFAA's vagueness problem. The SECURE IT Act and PDPSA both employ a negative approach, specifying one type of conduct that *does not* qualify as unauthorized access.[162] Aaron's Law, by contrast, takes a positive approach, specifying the type of conduct that *does* qualify

[157] *Indictment*, *supra* note 123, ¶¶ 14, 17.
[158] *Id.* ¶ 24.
[159] *Id.* ¶ 28.
[160] *Id.* ¶¶ 24, 26.
[161] *Id.* ¶ 26.
[162] *See SECURE IT Act* § 306 (providing that the phrase "exceeds authorized access" does not include "access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized"); *PDPSA* § 110 (providing the same).

as unauthorized access.[163] The difference between these approaches has significant consequences for the CFAA's vagueness problem.

A. *The SECURE IT Act and PDPSA*

The SECURE IT Act and PDPSA take a negative approach to restricting the scope of the CFAA. Both bills narrow the scope of the phrase "exceeds authorized access," providing that "violation[s] of a contractual obligation or agreement" cannot be the "*sole basis* for determining that access to a protected computer is unauthorized."[164] As Senator Leahy explained, this language is designed to "make clear that Congress does not intend for the Justice Department to pursue criminal prosecutions under the CFAA for conduct solely involving a violation of a terms of service agreement or contractual agreement."[165]

Although SECURE IT Act and PDPSA narrow the scope of the CFAA somewhat, these bills fail to fully correct the CFAA's vagueness problem. As an initial matter, both bills explicitly exempt government employment contracts from their clarification of unauthorized access.[166] This exemption may reflect legitimate concerns: government agencies often have access to highly sensitive information and it may not be feasible for these agencies to set up technological safeguards against all forms of improper computer use. But these concerns are equally applicable to many

---

[163] *See Aaron's Law* § 2(a)(2)(C) (providing that computer use is unauthorized when the user circumvents a technological or physical barrier to access).

[164] *SECURE IT Act* § 306 (emphasis added); *PDPSA* § 110 (emphasis added).

[165] Fung, *supra* note 142.

[166] *See SECURE IT Act* § 306 (providing that violations of contracts with "non-government employer[s]" shall not be the sole basis for determining that access to a protected computer is unauthorized); *PDPSA* § 110 (providing the same). Thus, although the SECURE IT Act and PDPSA might prevent CFAA prosecutions based on violations of private employment contracts, such as the bank employees' confidentiality agreement in the *John* case, these bills would not preclude prosecutions based on violations of government employment contracts, such as the Social Security Administration confidentiality agreement in the *Rodriguez* case. *See* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

private employers,[167] and it makes little sense to treat a DMV employee who visits Facebook at work as a hacker when the same activity would not be illegal if performed by a bank employee. Regardless, the exemption for government employees indicates that the SECURE IT Act and PDPSA would not preclude the contract approach; instead, these bills would merely restrict the class of individuals against whom the contract approach may be used.[168] At least among the class of government employees, the SECURE IT Act and PDPSA do nothing to curtail the unguided discretion prosecutors currently enjoy under the contract and agency approaches. For government employees, the SECURE IT Act and PDPSA fail to correct the CFAA's vagueness problem.

It is also not clear that the SECURE IT Act and PDPSA would preclude the contract approach for private citizens. Both bills provide that violations of private contracts shall not be the "sole basis" for determining that a particular form of computer use exceeds authorization.[169] This language leaves open the possibility that a contractual violation could be used as a factor for determining that a particular form of access exceeds authorization, so long as some other "plus factor" also weighs in favor of treating the computer use as hacking.[170] Neither bill provides any guidance

---

[167] *See* Thaw, *supra* note 32, at 928 (arguing that many employers lack the practical and technological resources necessary to implement code-based restrictions on all types of computer behavior they consider inappropriate). For example, consumer reporting agencies have access to highly sensitive personal information, to the point that Congress specifically regulates their use of such information. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681(a)(4) (2012) ("There is a need to insure [sic] that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").

[168] *See SECURE IT Act* § 306 (providing that violations of contracts with "non-government employer[s]" shall not be the sole basis for determining that access to a protected computer is unauthorized); *PDPSA* § 110 (providing the same).

[169] *SECURE IT Act* § 306; *PDPSA* § 110.

[170] This appears to be the most natural reading of the SECURE IT Act and PDPSA, notwithstanding Senator Leahy's protestations to the contrary. *See* Fung, *supra* note 142 (quoting Senator Leahy as explaining that the PDPSA is designed to "make clear that Congress does not intend for the Justice Department to pursue criminal prosecutions under the CFAA for conduct solely

as to what types of plus factors might be relevant to this inquiry, leaving this question to the discretion of prosecutors. And because the CFAA itself treats several very broad factors as potentially relevant to the issue of criminal punishment—including whether the offense was committed in furtherance of "any criminal or tortious act"[171] and whether the offender has previously been convicted of a CFAA offense[172]—the SECURE IT Act and PDPSA may actually do little to curtail the ambitions of particularly creative prosecutors.

In theory, the SECURE IT Act and PDPSA's "contract plus" approach might not preclude even the most arbitrary or discriminatory contract-based CFAA prosecutions. For example, Lori Drew arguably committed several torts when she set up a fake MySpace account to harass her daughter's classmate, including negligence[173] and intentional infliction of emotional distress.[174]

---

involving a violation of a terms of service agreement or contractual agreement"). Congress clearly knows how to distinguish between providing that a factor may not be "the basis" for a decision (i.e., that it may not be considered at all in reaching the decision) and providing that it may not be the "sole basis" for a decision (i.e., that it may be considered among other factors in reaching the decision). *See* 8 U.S.C. 1154(h) (2012) (distinguishing between the dissolution of a marriage, which "may not be the sole basis for revocation" of a particular immigration petition, and remarriage, which "shall not be the basis" for revocation of the same type of petition).

[171] *See* 18 U.S.C. § 1030(c)(2)(B)(ii) (2012) (providing that a violations of the catchall Section (a)(2) that would otherwise be treated as a misdemeanors shall be treated as a felony if "the offense was committed in furtherance of *any criminal or tortious act* in violation of the Constitution or laws of the United States *or of any State*") (emphasis added).

[172] *See id.* § 1030(c) (providing greater punishments for an offense "which occurs after a conviction for another offense under this section").

[173] *See* RESTATEMENT (SECOND) OF TORTS § 282 (1965) (defining negligence as "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm"). Drew arguably fell below the legal standard of care when she bullied a young girl online. *See* Steinhauer, *supra* note 117 (claiming that the girl "committed suicide in response to [Drew's] cyberbaiting").

[174] *See* RESTATEMENT (SECOND) OF TORTS § 46 ("One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily to the other results from it, for such bodily harm."). Assuming that Drew's cyber

Under a contract plus approach, prosecutors could claim that their case against Lori Drew did not depend *solely* on Drew's violating MySpace's TOS. Rather, prosecutors could argue that Drew's behavior amounted to hacking because it both breached the MySpace TOS and facilitated the commission a tort. [175] Alternatively, motivated prosecutors could cite a particular employee's criminal record as a plus factor to render his checking personal email at work a federal crime, even when the same activity by other employees would not constitute hacking. This is precisely the type of arbitrary and discriminatory enforcement the void for vagueness doctrine is designed to preclude.[176]

Finally, regardless of any effect the bills may have on the contract approach, the SECURE IT Act and PDPSA would not preclude the much broader agency approach to unauthorized access. The agency approach does not depend on "violation[s] of a contractual obligation or agreement," [177] but rather on general principles of agency law. Under the agency approach, *any* use of a computer by an agent (such as an employee) that does not further the principal's interests constitutes unauthorized access, regardless of any contract between the parties.[178] Thus, although the SECURE

---

bullying qualifies as extreme and outrageous conduct, she almost certainly could be held liable for contributing to a young girl's suicide. *See* Steinhauer, *supra* note 117 (claiming that the girl "committed suicide in response to [Drew's] cyberbaiting").

[175] In fact, prosecutors raised this very argument in the Drew case. *See* Government's Trial Memorandum at 10–14, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (No. 08-582-GW), *available at* http://www.scribd.com/doc/23406419/Governments-Trial-Memo (arguing that intentional infliction of emotional distress could trigger liability in a CFAA prosecution).

[176] Careful prosecutors might also take note of the perverse double-edged sword this argument presents. If, for example, a prosecutor were to bring a weak case based on evidence gathered through a fake Facebook account (created in violation of that site's TOS), the prosecutor himself could arguably be subject to CFAA liability based on the combination of the contractual violation and the tort of malicious prosecution.

[177] *SECURE IT Act* § 306; *PDPSA* § 110.

[178] *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006). It is also worth noting that, although the SECURE IT Act and PDPSA would modify the CFAA's definition of "exceeds authorized access," the *Citrin* decision makes clear that the agency approach considers any computer use by a

IT Act and PDPSA may restrict the class of individuals against whom the CFAA is likely to be enforced, it does nothing to restrict the scope of conduct that could potentially qualify as hacking. That issue remains, as before, a question for the unguided discretion of prosecutors.

B. *Aaron's Law*

In contrast with the SECURE IT Act and PDPSA, Aaron's Law takes a positive approach to limiting the scope of the CFAA. Rather than specifying one particular category of conduct that does not constitute hacking, Aaron's Law limits the conduct that qualifies as hacking to a single, relatively specific category.[179] Aaron's Law provides that computer use only qualifies as hacking when the user circumvents some type of physical or technological barrier designed to restrict access to that computer or information.[180] Thus, unlike the SECURE IT Act and PDPSA, Aaron's Law explicitly addresses the type of *conduct* prohibited by the CFAA, rather than any contractual or agency *relationship* that may exist between the computer's owner and the user.

Although Aaron's Law would significantly clarify the CFAA's definition of hacking, the bill would not remove all ambiguity from the statute. In particular, the bill does not provide any guidance as to what constitutes a "technological or physical measure[]"[181] designed to regulate access to a computer or information. Some types of technological barriers may be obvious; a user who bypasses a login screen by stealing another user's password has clearly circumvented a technological barrier to access.[182] But other types of barriers to access may be more difficult to identify. For

---

disloyal computer to be completely "without authorization," rather than merely exceeding the user's authorization. *Id.* at 419.

[179] *See Aaron's Law* § 2(a)(2) (providing that a user must "knowingly circumvent one or more technological or physical measures" in order to access a computer without authorization).

[180] *Id.* § 2(a)(2)(C).

[181] *Id*.

[182] *See* Kerr, *Cybercrime's Scope*, *supra* note 36, at 1664 (explaining that a user who correctly guesses another user's password would violate a code-based computer crime statute).

example, some websites require users to attest that they are over a certain age before granting access, but do not attempt to independently verify information entered by users.[183] Do such websites present users a true barrier to access? This problem is even more acute when physical barriers to access are considered. Must a user break into a locked room in order to violate the CFAA, or could a user "circumvent" a physical barrier simply by opening the door to a room labeled "restricted area?"[184]

Notwithstanding these ambiguities, Aaron's Law appears to clarify the CFAA's definition of hacking with enough specificity to satisfy the void for vagueness doctrine. First, the bill would define hacking in a way most computer users can understand. Unlike the terms of many private contracts, login pages and other similar technological barriers clearly and unambiguously signal to users that certain types of conduct are prohibited. More importantly, Aaron's Law would eliminate much of the discretion prosecutors currently enjoy under the contract and agency approaches. Borderline technological and physical barriers like the ones discussed above are relatively rare today; most modern computers, websites, and smartphones either require a password, or present no barrier to access whatsoever. As a result, Aaron's

---

[183] *See, e.g.*, Maker's Mark Distillery, Inc., *Official Website of Maker's Mark*, https://www.makersmark.com/ (last visited Feb. 17, 2014) (requiring users to enter a date of birth before entering a website for a brand of whiskey). Users who visit this website are asked to enter their date of birth. If the user enters a birthdate reflecting an age over twenty-one, the user may proceed to the full site. If the user enters a date of birth reflecting an age under twenty-one, the user is redirected to a separate website sponsored by the distillery industry where, among other things, former basketball star Shaquille O'Neal will urge them not to engage in underage or binge drinking. *See* The Century Council, *Why Am I Here*, CENTURYCOUNCIL.ORG, http://www.centurycouncil.org/landing-page/why-am-i-here (last visited Feb. 17, 2014).

[184] The Swartz case itself highlights this issue. The government accused Swartz of entering a "restricted network interface closet" on the MIT campus. *Indictment*, supra note 123, ¶ 24. Swartz's supporters, by contrast, characterize the room as "an unlocked maintenance closet." Joshua Kopstein, *Aaron Swartz's Family Releases Statement, Blames Overreaching Prosecutors For His Untimely Death*, THE VERGE, (Jan. 12, 2013, 8:42 PM), http://www.theverge.com/2013/1/12/3870500/aaron-swartz-family-statement-blames-reddit-suicide-on-government.

Law would draw a relatively clear line between hacking and permissible types of computer use. Prosecutors would, of course, retain discretion over which hackers to prosecute,[185] but they would lack discretion to determine which forms of computer use qualify as hacking.

VI. CONCLUSION

Bipartisan support for the SECURE IT Act and PDPSA indicate that, after two decades of steady expansion, Congress may soon act to restrict the reach of the CFAA for the first time in the statute's history. Although any measure that narrows the CFAA's immense scope would be a welcome improvement, the SECURE IT Act and PDPSA do not fully preclude the contract and agency approaches to unauthorized access. Under these bills, the difference between harmless computer use and criminal hacking would continue to depend, at least in part, on "whether you happen to be someone [a prosecutor] has reason to go after."[186] Thus, although the SECURE IT Act and PDPSA might ease popular concerns about the CFAA, these bills fail to provide sufficient checks on prosecutorial discretion to correct the CFAA's problem.

Although Aaron's Law would largely correct the CFAA's vagueness problem, the bill's code approach also presents certain theoretical and practical problems.[187] As a theoretical matter, the code approach appears to misplace the burden of differentiating between authorized and unauthorized forms of computer use on computer owners rather than computer users. Aaron's Law essentially treats *all* forms of computer use as authorized by default: if a computer owner wants to control access to his own device or data, he must erect some kind of technological or

---

[185] For example, a prosecutor might choose to pursue charges against an individual who used forged the login credentials to access a stranger's online banking account but not against another individual who used forged login credentials to access a friend's Netflix account.

[186] United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) (internal citations omitted).

[187] Thaw, *supra* note 32, at 928–29 (arguing that the code approach overlooks various "practical, theoretical, and normative problems").

physical barrier.[188] In addition, in practice it may be difficult or impossible for some computer owners to design and implement technological restrictions on all types of activities they wish to restrict.[189]

Aaron's Law is not perfect, but the bill's code approach to unauthorized access may be the only workable way to balance the constitutional demands of the void for vagueness doctrine with the need for flexible criminal laws that can adapt in the face of rapidly advancing digital technology. The void for vagueness doctrine does not demand more specificity from a criminal statute than is possible or practical.[190] As the Supreme Court has noted, "[c]ondemned to the use of words, we can never expect mathematical certainty from our language."[191] This is particularly true in an age when that language attempts to regulate the activities of devices whose computing power—and, consequently, potential uses—doubles approximately every eighteen months.[192] By essentially defining unauthorized access as the digital equivalent of

---

[188] *See Aaron's Law* § 2(a)(2)(C) (providing that computer use is unauthorized when the user circumvents a technological or physical barrier to access). This is the opposite approach from that taken by most laws governing access to physical property. For example, trespassing laws protect all real property from unreasonable intrusions, regardless of whether the owner erects a fence around the property or hangs a "No Trespassing" sign.

[189] Thaw, *supra* note 32, at 928.

[190] Kolender v. Lawson, 461 U.S. 352, 361 (1983).

[191] Grayned v. City of Rockford, 408 U.S. 104, 110 (1972).

[192] In 1965, engineer Gordon Moore predicted that the number of transistors capable of being placed on silicon microchips would double each year for the next decade. Over the next half-century, advances in microchip technology largely followed Moore's prediction, albeit at eighteen month intervals. Moore's prediction was so prescient that many computer scientists eventually came to treat it as a technological principle, commonly known as Moore's Law. Encyclopedia Britannica, *Moore's Law*, BRITTANICA.COM, http://www.britannica.com/EBchecked/topic/705881/Moores-law (last updated Sept. 23, 2013). Although some have expressed skepticism that computing power can continue to advance at this rate indefinitely, ongoing technological advances suggest that the general principle of increased computing power will continue for at least the near future. *See* Ryan Whitwam, *Graphene Nanoribbons Could Be the Savior of Moore's Law*, EXTREME TECH (Feb. 17, 2014, 11:01 AM), http://www.extremetech.com/extreme/176676-graphene-nanoribbons-could-be-the-savior-of-moores-law.

trespassing, Aaron's Law returns the CFAA to the popular understanding of the term "hacking" and corrects the CFAA's vagueness problem.