American University Law Review

Volume 61 | Issue 5 Article 7

2012

# A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act

Andrew Hernacki

# A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access under the Computer Fraud and Abuse Act

# A VAGUE LAW IN A SMARTPHONE WORLD: LIMITING THE SCOPE OF UNAUTHORIZED ACCESS UNDER THE COMPUTER FRAUD AND ABUSE ACT

ANDREW T. HERNACKI*

*The Computer Fraud and Abuse Act (CFAA) broadly criminalizes unauthorized access to computers and digital information, but how far should these federal prohibitions reach into the mobile data space? As smartphones and mobile applications continually redefine the digital landscape, attempts to apply the decades-old anti-hacking statute in this new territory have created potentially disturbing precedent.*

*Courts and critics have struggled to interpret the arguably vague and ambiguous provisions of the CFAA and have turned to contract law, agency law, and computer science for guidance. This Comment contends that the contract- and agency-based interpretations implicate constitutional vagueness concerns, and the code-based approach does not sufficiently address "insider" misuse of information. In the context of mobile application data privacy, the shortcomings of current interpretations necessitate a narrower view of unauthorized access. By limiting liability to only traditional notions of hacking and serious misuse of information, the CFAA can better serve its original and primary purpose: punishing criminal computer hackers and those who abuse legitimate access rights.*

---

* Junior Staff Member, *American University Law Review*, Volume 61; J.D. Candidate, May 2013, *American University, Washington College of Law*; B.A., Political Science, 2007, *Northwestern University*. I would like to thank Professor Jorge Contreras for his advice and guidance throughout this process. My sincere thanks to Ben Horowitz, Kat Scott, and the rest of the *Law Review* staff for their dedication, patience, and tireless work on this project. To my friends and family, thank you for your continued support and encouragement; and special thanks to Danielle Sunberg and Michael Gropper for helping to keep me sane. Lori, you are my inspiration and I would be nowhere without your love, compassion, and confidence. Dad, this one's for you.

TABLE OF CONTENTS



*"I think there is a world market for maybe five computers."*
–Thomas Watson, Chairman of IBM, 1943

## INTRODUCTION

Cell phones are ubiquitous.[1] As handheld devices become increasingly affordable and network service providers continue to

1. According to the wireless industry trade association, CTIA, the wireless penetration rate, which measures the total active devices over the total U.S. population, reached 102.4% in 2011. *Wireless Quick Facts*, CELLULAR TELECOMMS. INDUS. ASS'N, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited May 5, 2012).

expand cellular and data bandwidth, advanced mobile devices, or smartphones, have become similarly widespread.[2] According to one recent study by the Pew Research Center, eighty-eight percent of Americans own some kind of cell phone, while forty-six percent of Americans own a smartphone.[3] One of the most common and distinctive features of today's smartphones is mobile applications, or "apps." Apple's often-quoted and parodied advertising slogan, "there's an app for that," seemingly encapsulates the current panoply of apps across numerous genres available to smartphone users.[4] With the meteoric rise of smartphones and app usage over the last few years,[5] concerns over data privacy in the mobile space have garnered similar attention from legislators,[6] regulators,[7] and the general public.[8]

Despite increasing legislative and media attention on mobile data privacy, many app developers have not adopted self-regulatory measures to protect user privacy.[9] A recent *Wall Street Journal* investigation of the 101 most popular mobile apps on the market revealed that forty-five did not include privacy policies of any kind.[10]

---

2. *See 2010 Mobile Year in Review Report*, COMSCORE (Feb. 14, 2011), http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Mobile_Year_in_Review (describing consistent growth in percentages of web-enabled phones, unlimited data plans, smartphone ownership, and 3G/4G phone ownership).

3. Aaron Smith, *46% of American Adults Are Smartphone Owners*, PEW RESEARCH CTR. (Mar. 1, 2012), http://pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

4. Perhaps in response to widespread parody, Apple recently obtained a trademark for "there's an app for that." THERE'S AN APP FOR THAT, Registration No. 3,884,408.

5. Press Release, Apple, Inc., Apple's App Store Downloads Top 25 Billion (Mar. 5, 2012), http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html.

6. *See, e.g.*, *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2011) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary) ("The collection, use and storage of location and other sensitive personal information [from mobile devices] has serious implications regarding the privacy rights and personal safety of American consumers.").

7. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (proposing new privacy frameworks for mobile companies).

8. *See, e.g.*, Press Release, Apple, Inc., *supra* note 5 (discussing public comments regarding concerns for better privacy protection).

9. *See* Tanzina Vega, *Industry Tries to Streamline Privacy Policies for Mobile Users*, N.Y. TIMES, Aug. 14, 2011, at B7 (describing one company's effort to solve the problem of non-existent and confusing mobile privacy policies by creating a tool that generates boilerplate privacy policies for app developers).

10. Scott Thurm & Yukari Iwatani Kane, *Your Apps are Watching You*, WALL ST. J., Dec. 18, 2010, at C1. In response to this study, California Attorney General Kamala Harris conducted an investigation and recently reached an agreement with Apple,

Moreover, fifty-six apps transmitted the unique device identification (UDID), a serial-like number that can be linked to other user data,[11] to third-party companies without the users' awareness or consent.[12] Amidst these growing concerns over protecting users' information, both law enforcement and private citizens have looked for new ways to bring their concerns before the judiciary.[13] Some of these novel approaches, however, may push the envelope too far.

App users alleging privacy infringement have recently sought redress under the Computer Fraud and Abuse Act[14] (CFAA), a federal criminal statute originally designed to combat "juvenile computer hacker" attacks against the federal government's computers.[15] Despite the statute's narrow origin, the CFAA now broadly criminalizes and permits private civil actions against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer."[16] Typical criminal and civil cases under the CFAA involve traditional notions of hacking government computers,[17] stealing trade secrets to establish competing businesses,[18] or large-

---

Google, and several other big players in the mobile space to amend the companies' policies regarding privacy policies. Geoffrey A. Fowler, *Tech Giants Agree on Deal on Privacy Policies for Apps*, WALL ST. J., Feb. 23, 2012, at B4. Notably, Attorney General Harris's investigation revealed that twenty-two of the thirty most downloaded apps still lacked privacy policies. *Id.*

11. Modern smartphones are equipped with this identification number that cannot be deleted from the device. Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, WALL ST. J. (Dec. 19, 2010, 9:40 PM), http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained. Although the numbers by themselves do not identify any personal information about the user, the primary concern with these identifiers is that they could potentially be tied to other user metadata, including geo-location data or user-account data, to create a personally-identifiable profile of the user. *Id.*

12. Thurm & Kane, *supra* note 10.

13. *See infra* notes 20–21 and accompanying text (describing pending investigations and class action cases stemming from mobile app data privacy concerns); *see also Cyber Crime: Updating the Computer Fraud and Abuse Act to Protect Cyber Space and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 1 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen.) (proposing further expansion of the CFAA by increasing criminal penalties and making it easier for prosecutors to bring cases against individuals and co-conspirators).

14. 18 U.S.C. § 1030 (2006).

15. Sarah Boyer, Note, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661, 665 (2009).

16. 18 U.S.C. § 1030(a)(2).

17. *See* United States v. Morris, 928 F.2d 504, 505, 511 (2d Cir. 1991) (affirming the criminal conviction of a Cornell student who used a school computer to crash university, governmental, and military servers around the country).

18. *See, e.g.*, United States v. Nosal, No. 10-10038, 2012 WL 1176119, at *1 (9th Cir. Apr. 10, 2012) (en banc) (describing the section of the CFAA that criminalizes theft of confidential documents and trade secrets).

scale data theft via malicious code or "botnets."[19] Law enforcement[20] and classes of app users,[21] however, now argue that app developers and mobile advertisers can be liable under the CFAA when an app merely obtains information from the user's smartphone for targeted advertisements and marketing analytics.[22] The CFAA does not define what it means to access a computer without authorization, and courts continue to struggle to interpret these vague provisions.[23]

This Comment will argue that, in the context of mobile app data privacy cases, broad interpretations of the CFAA's unauthorized access provisions violate the vagueness doctrine and render the statute unconstitutional under the Due Process Clause. As the vagueness doctrine enables courts to adopt narrow interpretations of vague statutes, courts should limit application of the CFAA to

---

19. *See, e.g.*, Indictment at 15–16, 26–27, United States v. Ancheta, No. CR 05-1060 (C.D. Cal. 2005) (charging defendant with CFAA violations for operating and profiting from a botnet—an army of infected computers—used to send malicious spam and conduct distributed denial of service attacks against various websites), *available at* http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf.

20. *See* Pandora Media, Inc., Amendment No. 2 to Registration Statement Under the Securities Act of 1933, at 27–28 (Apr. 4, 2011), http://sec.gov/Archives/edgar/data/1230276/000119312511087171/ds1a.htm#toc119636_19 (disclosing that federal prosecutors are investigating the use of app-obtained information as potentially violative of the CFAA); Amir Efrati et al., *Mobile-App Makers Face U.S. Privacy Investigation*, WALL ST. J., Apr. 5, 2011, at B1 (discussing an investigation by federal prosecutors in New Jersey into mobile app data collection and disclosure).

21. *See In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *35–37 (N.D. Cal. Sept. 20, 2011) (alleging CFAA violations against Apple and several mobile advertisers for the unauthorized acquisition of apps, smartphone UDIDs, and geo-location data for marketing and advertising purposes); Hines v. Openfeint, Inc., No. CV113084, 2011 WL 2471471 (N.D. Cal. June 22, 2011) (alleging that a mobile-gaming-network company accessed, without authorization, users' smartphone UDIDs, Facebook/Twitter profiles, and other purportedly personal information for marketing analytics and targeted advertising profiles); *In re* Google Android Consumer Privacy Litig., 802 F. Supp. 2d 1372, 1373 (J.P.M.L. 2011) (consolidating six cases arising out of allegations of Google's "improper business practices"); *see also* Complaint ¶¶ 39–44, Jeffreys v. Google, Inc., No. 9:2011cv80676 (S.D. Fla. June 9, 2011), *available at* http://docs.justia.com/cases/federal/district-courts/florida/flsdce/9:2011cv80676/380889/1 (alleging that Google, through its Android mobile operating system, acquired personal information from users' smartphones without authorization, in violation of the CFAA).

22. *Hines*, 2011 WL 2471471, at *10–12.

23. Some courts have resolved such ambiguities by invalidating overly-broad language and substituting narrower interpretations, applying the "vagueness doctrine." Statutes that are so vague they are indecipherable to the public are especially prime for application of the doctrine. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1619–28 (2003) (comparing "virtual-world" and "physical-world" interpretations of "access" and "authorization"). Professor Kerr also notes that "the few courts to have interpreted access have reached inconsistent conclusions" and "[c]ourts have faced even greater difficulties trying to interpret the meaning of authorization." *Id.* at 1628.

prohibit only traditional notions of hacking and serious misuse of information.

Part I explains the early development of the CFAA as an anti-hacking statute, the current scope of activities triggering liability under the statute, and the three leading interpretations of unauthorized access. Part II argues that broad interpretations of unauthorized access in the context of mobile apps can render the CFAA unconstitutionally void for vagueness. Part III analyzes how courts should limit application of the CFAA to cases of traditional hacking and misuse of information. This Comment concludes that, except for instances of hacking or serious misuse of information, mobile app data privacy cases are improper under the CFAA, especially in light of proposed privacy-specific rules and legislation.

## I. BACKGROUND

### *A. Evolution of the CFAA*

The initial goal of the CFAA was modest: protect information stored on computers owned by the federal government from damage and theft by outside intruders.[24] As the computer industry continues to expand and the threat of hackers pervades virtually every interaction with the digital world, this formerly-little-known anti-hacking statute has grown into a multi-faceted tool with a potentially limitless scope.[25]

#### *1. Initial enactment and early development of the CFAA*

Over the last three decades, the CFAA has evolved considerably from its initial enactment. The CFAA's first iteration was enacted as part of the omnibus Comprehensive Crime Control Act of 1984[26] (CCCA), which included the first federal computer crime statute.[27] The CCCA introduced three new federal computer crimes designed

---

24. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1 (2007) [hereinafter PROSECUTING COMPUTER CRIMES] (citing H.R. REP. NO. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

25. *See id.* at 2–3 (describing the steady expansion of causes of action under the CFAA through numerous amendments over the last twenty-five years).

26. Pub. L. NO. 98-473, 98 Stat. 1837 (codified as amended at 18 U.S.C. § 1030 (2006)).

27. *See* H.R. REP. NO. 98-894, at 6, *reprinted in* 1984 U.S.C.C.A.N. at 3692 (recognizing the absence of federal computer crime legislation and acknowledging how, prior to this enactment, law enforcement relied primarily on wire- and mail-fraud statutes to attempt to combat computer crimes committed with computers); *see also* PROSECUTING COMPUTER CRIMES, *supra* note 24, at 1 (discussing same).

to protect the burgeoning universe of federal systems controlled by and stored on computers.[28] While all of the new offenses applied to a person who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend,"[29] each provision criminalized conduct affecting a distinct federal interest.

The first offense created under the CCCA prohibited accessing a computer to obtain national security information that could be used to injure the United States.[30] The second portion of the CCCA criminalized accessing a computer to obtain sensitive information from a financial institution or consumer-reporting agency.[31] Finally, the CCCA criminalized accessing a computer if such conduct would affect the government's use of that computer or government operations.[32] These new provisions sought to protect national defense, financial information, and the use of government property.[33]

Congress's first attempt at creating a unified computer crime statute, however, was limited to only harm resulting from unauthorized access. Accordingly, the statute left two significant regulatory gaps: (1) the statute did not cover individuals who caused harm with authorized access; and (2) it failed to address access by proxy or a co-conspirator.[34] To remedy these loopholes, Congress amended § 1030 in 1986 to create the Computer Fraud and Abuse Act but limited it to only those crimes implicating a compelling federal interest.[35] The 1986 act attempted to remedy the misuse-of-legitimate-access problem by adding the phrase "exceeds authorized access," thereby criminalizing any access, including unknowing access, which even minimally steps over the line of authorized

---

28. *See* Boyer, *supra* note 15, at 665–66 (noting that the CCCA was intended to "protect only the most vital federal interests" and not to broadly criminalize computer fraud affecting interstate commerce).

29. 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985) (current version at 18 U.S.C. § 1030 (2006)).

30. *See* Boyer, *supra* note 15, at 665 (discussing 18 U.S.C. § 1030(a)(1)).

31. *See id.* at 665–66 (discussing 18 U.S.C. § 1030(a)(2)).

32. *See id.* at 666 (discussing 18 U.S.C. § 1030(a)(3)).

33. H.R. REP. NO. 98-894, at 6–7, 21–22 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692, 3707. *See generally* Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453 (1990) (discussing scope and structure of the 1984 Act and summarizing policy considerations behind both the 1984 act and the subsequent 1986 amendments).

34. Branden Darden, Note, *Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene?*, 13 SMU TECH. L. REV. 329, 331 (2009).

35. 18 U.S.C. § 1030 (1988) (current version at 18 U.S.C. § 1030 (2006)); *see also* Darden, *supra* note 34, at 331–32.

access.[36] This small phrase would later prove to have widespread interpretive problems.[37]

In 1994, Congress amended the CFAA to expand the statute beyond the criminal sector and add a private right of action.[38] This civil analogue permits not only injunctive relief, but also equitable relief for violations of the statute that result in damage or loss.[39] This change, in conjunction with additional amendments to § 1030(a)(5),[40] shifted the focus of the statute from the technical ideas of computer access to an individual's intent and the scope of the harm caused.[41]

The Economic Espionage Act of 1996[42] (EEA) continued the expansion of the CFAA. While prior versions of the statute were purposefully limited to unauthorized access of only federal-interest information, such as financial records or national security data,[43] the EEA expanded the scope of § 1030(a)(2) to now include obtaining—and simply reading[44]—"*any information of any kind* so long as the conduct involved an interstate or foreign communication."[45] In addition, the EEA added a new computer extortion provision, bolstered various misdemeanor provisions with felony-triggering conduct, and expanded the scope of "harm" to include non-monetary damage such as "physical injury to any person."[46] Further, the EEA replaced references to "federal interest" computers with a class of

36. 18 U.S.C. § 1030(a) (1988) (current version at 18 U.S.C. § 1030(a) (2006)).

37. *See infra* Part I.B (detailing three competing approaches to interpreting unauthorized access).

38. Darden, *supra* note 34, at 332.

39. 18 U.S.C. § 1030(g) (1994) (current version at 18 U.S.C. § 1030(g) (2006)).

40. The 1996 amendment to § 1030(a)(5) was intended "to further protect computers and computer systems covered by the statute from damage both by outsiders, who gain access to a computer without authorization, and by insiders, who intentionally damage a computer." S. REP. NO. 104-357, at 9–10 (1996), *available at* 1996 WL 492169, at *9; *see also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1566 (2010) (explaining that this amendment expanded liability-triggering actions to include both accidental and non-negligent damage to computers).

41. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. Fed. 101, 125–26 (2001).

42. Pub. L. NO. 104-294, tit. II, 110 Stat. 3488, 3491 (codified as amended at 18 U.S.C. § 1030 (2006)).

43. Darden, *supra* note 34, at 331.

44. EEA tit. II, 110 Stat. at 3491.

45. Kerr, *supra* note 40, at 1567 (noting that Congress "effectively criminalized all interstate hacking" with this amendment because even reading system prompts or messages would reveal information to someone without authorized access).

46. 18 U.S.C. § 1030 (Supp. II 1996) (current version at 18 U.S.C. § 1030 (2006)); *see* Kerr, *supra* note 40, at 1567.

"protected computers," a change that, as discussed below, would have a dramatic impact on the scope of the statute.[47]

*2. Current actions triggering liability under the CFAA*

The current version of the CFAA provides for criminal and civil liability when an individual intentionally "accesse[s] a computer without authorization or exceed[s] authorized access" and engages in one of seven types of prohibited conduct.[48] Section 1030(a) proscribes these seven actions: (1) obtaining any restricted government information or information protected for reasons of national defense;[49] (2) using interstate communication to obtain any information from any protected computer;[50] (3) accessing a computer owned or used by the federal government;[51] (4) fraudulently obtaining anything of value from a protected computer unless the value is less than $5000 in a one-year period;[52] (5) damaging a protected computer or data stored therein;[53] (6) trafficking in passwords or similar information in certain situations;[54] and (7) threatening to cause damage or obtain information from a protected computer with intent to extort money or anything of value.[55]

Section 1030(b) punishes any attempts or conspiracies to commit the proscribed actions, while § 1030(c) outlines criminal sanctions, and § 1030(d) authorizes the Secret Service and Federal Bureau of Investigation to investigate violations of the prohibited conduct.[56] Section 1030(e) provides definitions of some statutory terms (with some notable absences), and § 1030(f) exempts "lawfully authorized" federal or state law enforcement or intelligence-related investigations.[57]

Section 1030(g) comprises the private right of action, specifically providing that "[a]ny 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

47. *See infra* Part I.A.3 (discussing the virtually limitless scope of the CFAA's jurisdiction over computers connected to the Internet).
48. 18 U.S.C. § 1030(a)(1)–(7) (2006).
49. *Id.* § 1030(a)(1).
50. *Id.* § 1030(a)(2).
51. *Id.* § 1030(a)(3).
52. *Id.* § 1030(a)(4).
53. *Id.* § 1030(a)(5).
54. *Id.* § 1030(a)(6).
55. *Id.* § 1030(a)(7).
56. *Id.* § 1030(b)–(d).
57. *Id.* § 1030(e)–(f).

other equitable relief."[58] To bring an action for civil relief, a party must establish two essential elements: (1) a violation of one of the seven proscribed activities in § 1030(a) resulting in damage or loss, and (2) a violation must involve one of the five aggravating factors delineated in § 1030(c)(4)(A)(i)(I)–(V).[59] Despite this somewhat confusing statutory structure, a civil claim may be brought under any of the delineated causes of action so long as the party demonstrates at least one aggravating factor.[60] The civil right of action also includes a two-year statute of limitations period and bars product-liability claims for negligent design or manufacture of a computer.[61]

*3. Current scope of the CFAA*

In 1996, Congress replaced the idea of a "federal interest" computer with a new class of "protected computer."[62] The phrase "protected computer" sparked some initial interpretive problems, but it is now viewed very broadly. Currently, a "protected computer" means a computer that is either

> (A) exclusively for the use of a financial institution or the United States Government . . . ; or (B) [] used in or affecting interstate or foreign 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.[63]

This definition marked a significant change from the pre-1996 idea of "federal interest" computers, which triggered liability under the statute only when a violator "used" computers in two or more states.[64]

---

58. *Id.* § 1030(g).

59. *Id.* The aggravating factors are:

> (I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

*Id.* § 1030(c)(4)(A)(i)(I)–(V).

60. P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 512 (3d Cir. 2005) ("We do not read section 1030(g)'s language that the claim must *involve* one or more of the numbered subsections of subsection [(c)(4)(A)(i)] as limiting relief to claims that are *entirely based only on* subsections [(a)(5)(A)–(C)], but, rather, as requiring that claims brought under other sections must meet, in addition, one of the five numbered [(c)(4)(A)(i)] 'tests.'").

61. 18 U.S.C. § 1030(g).

62. 18 U.S.C. § 1030(e)(2) (Supp. II 1996) (current version at 18 U.S.C. § 1030 (2006)).

63. 18 U.S.C. § 1030(e)(2)(A)–(B) (2006).

64. 18 U.S.C. § 1030(e)(2)(B) (Supp. IV 1987) (current version at 18 U.S.C.

The current definition, with the inclusion of "or affecting interstate or foreign commerce or communication," effectively expands the scope of the statute to mirror the breadth of the Commerce Clause.[65]

Under current Commerce Clause jurisprudence, Congress can regulate local economic activities so long as there is a rational basis and the activities are among an economic class of activities that substantially affect commerce, even in the aggregate.[66] Accordingly, the addition of the congressionally-recognized term of art "affecting" within the definition of "protected computer" broadens the CFAA's reach to every computer that can be regulated under the Commerce Clause.[67] Recently, several federal courts of appeals have recognized the broad reach of the CFAA as commensurate with Commerce Clause jurisdiction and have accordingly rejected jurisdictional challenges to CFAA enforcement actions.[68]

Additionally, the CFAA's definition includes foreign commerce,[69] stretching the definition of "protected computer" to the point where it ostensibly just means "computer."[70] The CFAA, however, defines "computer" very broadly and excludes only typewriters and hand-held

---

§ 1030 (2006)).

65. U.S. CONST. art. I, § 8; 18 U.S.C. § 1030(e)(2)(B) (2006); *see* Kerr, *supra* note 40, at 1569–71 (explaining that computers connected to the Internet need not be used in interstate commerce to fall within the scope of the CFAA).

66. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 18–19 (2005) (holding that marijuana is a fungible commodity, albeit an illegal one, such that Congress can regulate even local cultivation because the aggregate effect of home growing could substantially affect interstate commerce).

67. Kerr, *supra* note 40, at 1570; *see also* PROSECUTING COMPUTER CRIMES, *supra* note 24, at 2 (acknowledging that the scope of "protected computer" mirrors "the full extent of Congress's commerce power").

68. *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (rejecting a constitutional challenge that the CFAA did not cover the computer network of the not-for-profit Salvation Army, and explaining that the computers' connection to the Internet rendered them "part of 'a system that is inexorably intertwined with interstate commerce' and thus properly within the realm of Congress's Commerce Clause power" (quoting United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006))); United States v. Mitra, 405 F.3d 492, 493, 496 (7th Cir. 2005) (affirming a conviction under § 1030 for damaging an emergency response communications system of Madison, Wisconsin, and rejecting the argument that the intrastate nature of the attack placed the defendant's actions outside the CFAA's jurisdiction on the grounds that Congress can regulate conduct affecting a computer once the computer itself is used in interstate commerce).

69. 18 U.S.C. § 1030(e)(2)(B) ("[T]he term 'protected computer' means a computer . . . which is used in interstate or foreign 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." (emphasis added)).

70. Kerr, *supra* note 40, at 1571; *see also* United States v. Ivanov, 175 F. Supp. 2d 367, 373–75 (D. Conn. 2001) (acknowledging Congress's power to apply its statutes extraterritorially and finding the plain language of § 1030(e)(2)(B) to clearly extend the CFAA to foreign computers).

calculators.[71] Recently, the United States Court of Appeals for the Eighth Circuit decided to explicitly and unequivocally include even basic cell phones—those that only make calls and send text messages without Internet or app functionality—within the definition of "computer."[72] This broad definition, both in the statute and in courts' interpretations, means that unauthorized access of nearly every computational device, including smartphones, would fall under the CFAA.

### *B. Three Approaches to Interpreting Definitional Ambiguities and Omissions of the CFAA*

The CFAA does not define several key terms. Most notably, the statute fails to define "access" and "authorization,"[73] absences that have drawn academic criticism and led to judicial uncertainty.[74] Further, the CFAA provides only a vague and arguably circular definition for "exceeds authorized access," namely that it "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 so entitled to obtain or alter."[75] Accordingly, courts and academics have struggled to interpret these undefined and vague provisions and have looked to other areas of the law for guidance.[76] Over the past decade,

---

71. 18 U.S.C. § 1030(e)(1) (defining "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions . . . includ[ing] any data storage facility or communications facility directly related to or operating in conjunction with such device, but . . . not includ[ing] an automated typewriter or typesetter, a portable hand held calculator, or other similar device"); *see* Kerr, *supra* note 40, at 1571 (citing *Mitra*, 405 F.3d at 496) (commenting that "[e]verything else with a microchip or that permits digital storage is, arguably, covered").

72. *See* United States v. Kramer, 631 F.3d 900, 902–03 (8th Cir.) (affirming a sentence enhancement for using a basic cell phone in the commission of transporting a minor in interstate commerce with the intent to engage in criminal sexual activity), *cert. denied*, 131 S. Ct. 2977 (2011).

73. 18 U.S.C. § 1030(e)(6).

74. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (employing a variety of statutory construction techniques—including dictionary definitions and the rule of lenity—to reject an interpretation of unauthorized access grounded in agency-law principles); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (acknowledging the CFAA's failure to define authorization and interpreting it according to the nebulous idea of "expected norms of intended use or the nature of the relationship established between the computer owner and the user"); *see also* Kerr, *supra* note 23, at 1619–24 (differentiating between "virtual" and "physical" notions of access and authorization).

75. 18 U.S.C. § 1030(e)(6).

76. *See, e.g.*, Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass, and Privacy*, 62 BUS. LAW. 1395, 1398–99 (2007) (proposing a view of unauthorized access statutes grounded in classical trespass law); *see also* Lawrence Lessig, *The Death of Cyberspace*, 57 WASH. & LEE L. REV. 337, 344 (2000) (opposing a property-rights oriented approach in favor of a more restrictive view of unauthorized access to avoid

three distinct approaches have emerged for how to interpret and apply what it means to access a computer without, or in excess of, authorization: (1) the contract-based approach; (2) the agency-based approach; and (3) the code-based approach.

*1. The contract-based approach*

Under the contract-based approach, one "exceeds authorized access," in violation of the CFAA, when accessing a computer in such a way that violates an existing "contract."[77] In this context, "contract" includes not only traditional contracts, such as employment contracts[78] or network service provider agreements,[79] but also more informal agreements, including employer computer-use policies or other company handbooks.[80]

The United States Court of Appeals for the First Circuit in *United States v. Czubinski*[81] developed the contract-based approach, though only in dicta. In *Czubinski*, an Internal Revenue Service (IRS) employee signed a contract containing a policy of limiting access to IRS files for only "official purposes."[82] The court assumed, in dicta and without any additional explanation, that Czubinski's perusal of files on the IRS database for personal reasons "unquestionably exceeded authorized access to a Federal interest computer."[83] While

---

economic waste).

77. Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2212 (2004) (explaining that a computer owner may control access by providing notice of terms of use); Nicholas R. Johnson, Note, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 570 (explaining that a computer owner may control access by a contract and that protections against unauthorized access derive from traditional contract law principles).

78. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (holding that breach of an employment-related confidentiality agreement exceeded authorized access, but not deciding whether the access itself was unauthorized).

79. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252–53 (S.D.N.Y. 2000) (finding that Verio's use of "search robots" on Register.com's "WHOIS" domain-name registration database breached Register.com's policy forbidding the use of "WHOIS" data for marketing purposes and thereby violated § 1030(a)(2)(C) and (a)(5)(a)), *aff'd*, 356 F.3d 393 (2d Cir. 2004); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (finding that LCGM violated § 1030(a)(2)(C) when it used "extractor software" to harvest e-mail addresses from AOL for the purpose of sending bulk-spam advertisements in violation of AOL's TOS agreement).

80. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1260–65 (11th Cir. 2010) (affirming the conviction under the CFAA of a SSA teleservices agent who violated the SSA's computer-use policy when he accessed the SSA database to obtain personal information of women in whom he was romantically interested), *cert. denied*, 131 S. Ct. 2166 (2011).

81. 106 F.3d 1069 (1st Cir. 1997).

82. *Id.* at 1071.

83. *Id.* at 1078.

the First Circuit continued to apply the contract-based approach in the employment law context,[84] other courts and academics have also discussed the contract-based approach in website or network service provider terms-of-service (TOS) "clickwrap" agreements.[85] Under this application, "a website owner or service provider can establish criminal liability through . . . [rarely read] terms of service,"[86] granting broad discretion to the owner or service provider to choose what might constitute a criminal violation of the CFAA.[87]

The recent and tragic case *United States v. Drew*[88] involved an attempted application of the contract-based approach to website TOS agreements.[89] In *Drew*, Lori Drew was charged with violating § 1030(a)(2)(C) for creating a fake profile on MySpace.com to contact and befriend thirteen-year-old Megan Meier.[90] After several weeks of communicating with Meier through the fake profile of "Josh Evans," Drew, posing as "Evans," sent a message to Meier indicating that "Evans" no longer liked her and that "the world would be a better place without her in it."[91] That same day, Meier committed suicide.[92] Drew was then charged with violating § 1030(a)(2)(C) for unauthorized access because she had violated the Myspace TOS "contract" by creating the fake profile.[93] The trial judge, Judge Wu, however, did not accept this novel approach and granted Drew's motion for acquittal.[94] In holding that violations of website TOS agreements would encourage discriminatory enforcement,[95] Judge Wu stated that such an approach would "transform[] section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals."[96]

Recently, the United States Court of Appeals for the Eleventh

---

84. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (holding that violation of a confidentiality agreement can constitute exceeding unauthorized access).

85. Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 241 n.62 (2010) (defining a "clickwrap contract" as "one in which a computer user indicates assent with a mouse click rather than a signature").

86. *Id.* at 241.

87. *Id.* at 242.

88. 259 F.R.D. 449 (C.D. Cal. 2009).

89. *Id.* at 457.

90. *Id.* at 452.

91. *Id.*

92. *Id.*

93. *Id.* at 452–53.

94. *Id.* at 467.

95. *Id.* at 463–65.

96. *Id.* at 466.

Circuit adopted another variation of the contract-based approach in *United States v. Rodriguez*.[97] In *Rodriguez*, a Social Security Administration (SSA) teleservices agent allegedly used his access to the SSA database to obtain information about women in whom he was romantically interested.[98] Rodriguez, however, refused to sign an agreement acknowledging the SSA's policy prohibiting access to SSA database information for a purpose other than a "business reason," though the SSA reinforced its policy through mandatory training sessions, office notices, and a daily alert on company computers.[99] The court held that, even though there was no formal contract in place, violating a corporate computer-use policy can be sufficient to constitute "exceed[ing] authorized access" and, therefore, Rodriguez's actions amounted to a criminal violation of § 1030(a)(2)(B).[100]

After the Eleventh Circuit's decision in *Rodriguez*, the United States Court of Appeals for the Ninth Circuit clarified its position in *United States v. Nosal*.[101] In *Nosal*, a former employee of an executive search firm allegedly convinced several current employees to access the firm's proprietary executive database, in apparent violation of existing computer-use policies, to further the creation of his own competing firm.[102] Notably, the district court found that Nosal's conspirators had authority to obtain the allegedly proprietary information for legitimate business purposes and did not exceed authorized access even if they acted with fraudulent intent.[103]

In reversing the district court's decision, a panel of the Ninth Circuit held that "as long as the employee has knowledge of the employer's limitations on that authorization, the employee 'exceeds authorized access' when the employee violates those limitations."[104] However, the entire Ninth Circuit sitting en banc changed course and affirmed the district court's decision, holding that "'exceeds authorized access' in the CFAA does not extend to violations of use restrictions."[105] The court's holding has created a definitive circuit

97. 628 F.3d 1258 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (2011).
98. *Id.* at 1260–61.
99. *Id.* at 1260.
100. *Id.* at 1263.
101. 642 F.3d 781 (9th Cir. 2011), *rev'd en banc*, No. 10-10038, 2012 WL 1176119 (9th Cir. Apr. 10, 2012).
102. *Id.* at 783.
103. *Id.* at 785 (discussing United States v. Nosal, No. C 08-0237-MHP, 2010 WL 934257, at *1 (N.D. Cal. Jan. 6, 2010)).
104. *Id.* at 788. The court added "it is as simple as that." *Id.*
105. United States v. Nosal, No. 10-10038, 2012 WL 1176119, at *7 (9th Cir. Apr. 10, 2012) (en banc).

split with the Fifth, Seventh, and Eleventh circuits,[106] raising the distinct possibility of review by the Supreme Court. In adopting a narrow interpretation of "exceeds authorized access," the court joined the ranks of numerous federal district courts and academics that have routinely criticized the contract-based approach,[107] citing the rule of lenity[108] as well as overbreadth and vagueness concerns.[109]

*2. The agency-based approach*

The agency-based approach employs common law agency tenets to argue that an agent acts "without authorization" when he breaches a state law duty of loyalty or fiduciary duty to the principal.[110] The most common application of this approach occurs between employers and employees.[111] The agency-based approach was introduced in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[112] In this case, plaintiff Shurgard alleged defendant Safeguard hired away Shurgard employees who had access to confidential business plans and other trade secrets.[113] Shurgard argued the former employees were no longer its agents when they sent e-mails to their new employer "containing various trade secrets and proprietary information"

106. *See id.* at *6 (refusing to adopt an interpretation of "exceeds authorized access" grounded in "culpable behavior" and commenting that other federal circuit courts have "failed to consider the effect on millions of ordinary citizens caused by the statue's unitary definition"); *see also id.* at *10 (Silverman, J., dissenting) (discussing how the en banc majority's decision is also at odds with the Eighth Circuit's implicit adoption of the contract-based approach in United States v. Teague, 646 F.3d 1119, 1121–22 (8th Cir. 2011)).

107. *See id.* at *7 (majority opinion) (collecting cases holding that the CFAA does not prohibit unauthorized disclosure, misuse, or misappropriation of information).

108. *Id.* (reasoning that the rule of lenity necessitates a narrow interpretation of "exceeds unauthorized access" in order to ensure that both citizens and Congress will have fair notice of criminal conduct under the law as to avoid "unintentionally turn[ing] ordinary citizens into criminals").

109. *See id.* at *6 (reasoning that criminalizing inherently transitory, and generally vague, terms of service agreements invites arbitrary and discriminatory enforcement); *see also* Chung, *supra* note 85, at 242–43 (noting that courts have found the contract-based approach to be contrary to the plain language of the CFAA, established public policy, copyright law, First Amendment law, state employment regulation, and trade secret law).

110. Katherine Messenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 823 (2009) (discussing the evolution of the agency-based theory as a direct application of agency law to interpret authorization).

111. *See, e.g.*, ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 610–13 (M.D. Tenn. 2010) (discussing how several federal courts of appeals and numerous federal district courts have addressed allegations that an employee exceeds authorized access when he obtains information for a use that is adverse to the employer's interests).

112. 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

113. *Id.* at 1123.

without Shurgard's knowledge or permission.[114] The court, relying primarily on the *Restatement (Second) of Agency*, held that authorization ceases when accessers, here, the former Shurgard employees, sever the agency relationship by breaching a duty of loyalty to the employer/principal.[115] Accordingly, the court concluded that the former employees acted without authorization in violation of § 1030(a)(2)(C).[116]

In 2006, the United States Court of Appeals for the Seventh Circuit adopted the agency-based approach in *International Airport Centers, L.L.C. v. Citrin*.[117] In *Citrin*, former employee Citrin allegedly violated his employment contract when he quit his job to establish a rival business.[118] After deciding to resign, Citrin utilized a secure-erasure program on a work-issued laptop to delete all of the real-estate acquisition targeting data that he had collected for his former employer as well as evidence of Citrin's misconduct.[119] In adopting the agency-based approach, the court held that Citrin breached his duty of loyalty to his employer when he quit to establish a competing business, thereby severing the agency relationship and revoking his authorization to access the laptop.[120]

The Ninth Circuit, however, explicitly rejected the agency-based approach in *LVRC Holdings, LLC v. Brekka*.[121] In *Brekka*, a former LVRC employee, while still employed at LVRC, allegedly e-mailed documents from his work computer to himself and to his wife to establish a competing business.[122] The court rejected LVRC's agency-based argument that authorization terminates the moment that an employee's interests becomes adverse to his employer, and expressly rejected *Citrin* in holding that Brekka neither acted without authorization nor exceeded his authorized access.[123] Instead, the

---

114. *Id.*

115. *Id.* at 1125; *see* RESTATEMENT (SECOND) OF AGENCY § 112 (1958) (stating that agency terminates if an agent, without knowledge of the principal, acquires an adverse interest or commits a serious breach of loyalty to the principal).

116. *Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d. at 1125. Notably, the court also rejected defendant's arguments that: (1) information protected under the CFAA was limited to that which could affect the public; (2) § 1030(a)(5)(C), which proscribes anyone from "intentionally access[ing] a protected computer without authorization," and, as a result of such conduct, causes damage, applies only to "outsiders" and not to employees; and (3) appropriation of information is insufficient to constitute "damage." *Id.* at 1125–27.

117. 440 F.3d 418 (7th Cir. 2006).

118. *Id.* at 419.

119. *Id.*

120. *Id.* at 420–21.

121. 581 F.3d 1127 (9th Cir. 2009).

122. *Id.* at 1129–30.

123. *Id.* at 1133–35. The court also employed the rule of lenity to reject reading any state law duty of loyalty into the definition of "authorization," noting that a

court held that "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when that person has not received permission to use the computer for any purpose [such as a hacker], or when the employer has rescinded permission . . . and the defendant uses the computer anyway."[124] Given this apparent circuit split on the viability of the agency-based approach,[125] courts and academics have looked to other areas of the law in attempting to interpret the scope of "authorization."[126]

*3. The code-based approach*

In expressing some concerns over the agency and contract theories, Professor Orin Kerr articulated a third approach to interpreting the scope of authorization: the code-based approach.[127] Under this view of technical computer-based protections, access to a protected computer is unauthorized when a person circumvents some form of computer code built into the network or system, such as a username/password or a firewall.[128]

Early intimations of this approach can be seen in the infamous university-hacking case, *United States v. Morris*.[129] In *Morris*, a Cornell graduate student wrote and transmitted malicious code[130] that spread

---

"defendant would have no reason to know that making personal use of [a] company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA." *Id.* at 1135.

124. *Id.* The court also explained that "nothing in the CFAA suggests that a defendant's authorization to obtain information stored in a company computer is 'exceeded' if the defendant breaches a state law duty of loyalty to an employer, and we decline to read such a meaning into the statute." *Id.* at 1135 n.7.

125. *See* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 610–13 (M.D. Tenn. 2010) (analyzing the case law stemming from *Citrin* and *Brekka* and ultimately rejecting the agency-based approach as incompatible with the CFAA's plain language in light of the rule of lenity). *Compare Citrin*, 440 F.3d at 421 (adopting the agency-based approach where authorization ends when an agent "'voids the agency relationship'" by "'[v]iolating the duty of loyalty, or failing to disclose adverse interests'" to those of the principal (quoting State v. DiGiulio, 835 P.2d 488, 492 (Ariz. Ct. App. 1992))), *with Brekka*, 581 F.3d at 1134 (refusing to adopt the agency theory and sever authorization when the defendant's "mental state changed from loyal employee to disloyal competitor").

126. *See, e.g.*, Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-ORL-31, 2006 WL 2683058, at *6–7 (M.D. Fla. Aug. 1, 2006) (explicitly rejecting the agency-based approach in favor of a "plain meaning" interpretation of authorized access); Field, *supra* note 110, at 821 nn.6–7 (listing various district court cases employing contract or code-based interpretations rather than the agency theory).

127. Kerr, *supra* note 23, at 1649.

128. *Id.* at 1644–45 (discussing code-based circumventions as involving a user either: (1) "masquerad[ing] as another user who has greater [access] privileges"; or (2) "exploit[ing] a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges").

129. 928 F.2d 504 (2d Cir. 1991).

130. While Morris wrote the malicious code on a computer at the Cornell lab to which he had been given authorization, he ultimately transmitted it from a computer

uncontrollably to ultimately infect and crash university, medical research, and military servers around the country.[131] The court rejected Morris' argument that liability for accessing a computer "without authorization" was limited to the computer that Morris actually used to inject the malicious code.[132] Rather, the court looked to the "intended function" of the university computer in holding that Morris' program allowed him to "access" (through the malicious code) federal interest computers to which he did not have authorization to use.[133] Professor Kerr expanded upon this idea of the "intended function" test in developing his code-based approach, explaining that "a user who exploits a weakness in code to trick the victim computer into granting the user extra privileges does so by using the code in a way contrary to its intended function."[134]

To date, no court has explicitly adopted the code-based approach, but the view is often conflated with a similar theory, described as the plain-meaning theory, because the scope of authorization often rests on a computer-based safeguard, such as a password.[135] Nonetheless, this approach remains one of the leading academic approaches to addressing the statutorily-undefined and ambiguous provisions of the CFAA.[136]

### *C. The Vagueness Doctrine and the CFAA*

The vagueness doctrine embodies the idea that due process requires Congress to enact statutes such that: (1) the public can understand what conduct is prohibited; and (2) the courts have meaningful standards to enforce.[137] In effect, the doctrine places a

---

at the Massachusetts Institute of Technology in order to disguise the code's origin. *Id.* at 506.

131. *Id.*

132. *Id.* at 510.

133. *Id.*

134. Kerr, *supra* note 23, at 1645.

135. *See* Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 934–35 (W.D. Tenn. 2008) (asserting that "the plain meaning of 'exceeds authorized access' is 'to go beyond the access permitted'" and the "plain meaning [of without authorization] is 'no access authorization'"); Lockheed Martin Corp. v. L-3 Comm. Corp., No. 6:05-cv-1580-Orl-31KRS, 2007 WL 569994, at *1 (M.D. Fla. Feb. 20, 2007) (declining to adopt an expanded view of authorized access beyond the plain language); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006) (noting that "the plain meaning [of exceeds authorized access] brings clarity to the picture and illuminates the straightforward intention of Congress").

136. Chung, *supra* note 85, at 244 n.83 (citing Bellia, *supra* note 77, at 2258; Sara M. Smyth, *Back to the Future: Crime and Punishment in Second Life*, 36 RUTGERS COMPUTER & TECH. L.J. 18, 41 (2009)). *But see* Winn, *supra* note 76, at 1419 (criticizing the code-based approach as "flatly inconsistent" with the CFAA's separation of "unauthorized access" and "access in excess of authorization").

137. *See* Giaccio v. Pennsylvania, 382 U.S. 399, 403–04 (1966) (reversing a

due-process backstop[138] behind Congress to allow courts to reign in broad and ambiguous statutes by substituting narrower readings of vague provisions.[139]

The doctrine was introduced by Justice Sutherland in *Connally v. General Construction Co.*[140] In *Connally*, the Court invalidated an Oklahoma statute criminalizing the failure of state contractors to pay employees fair wages in line with those paid in the locality.[141] In doing so, the Court ordered that the terms of a criminal statute must explicitly state the prohibited conduct and its penalties in clear, unambiguous language, or risk violating due process of law.[142]

Further, the doctrine has been interpreted to provide grounds for invalidating a statute not only when the statute does not provide "fair notice" to the public, but also when it inures law enforcement to engage in arbitrary and discriminatory enforcement of the law.[143] While the vagueness doctrine is often considered a "powerful tool"[144] in First Amendment freedom-of-speech litigation,[145] vague laws unrelated to speech regulation violate due process when a reasonable person cannot tell what conduct is prohibited.[146] Notably, the due process rights implicated through application of the vagueness doctrine are not limited to individuals, as due process also extends to corporate entities.[147]

---

conviction for misdemeanor gun charges on due process vagueness grounds because the Pennsylvania statute lacked legally-fixed standards for both juries and judges).

138. *See* Kolender v. Lawson, 461 U.S. 352, 357 (1983) (explaining the constitutional roots of the vagueness doctrine).

139. *Compare* City of Chicago v. Morales, 527 U.S. 41, 57, 64 (1999) (invalidating a Chicago anti-loitering ordinance for failing to provide fair notice, thus rendering the statute unconstitutionally vague in violation of the Due Process Clause), *with id.* at 112 (Thomas, J., dissenting) (arguing that the ordinance should be upheld under a narrow reading of the ambiguous statutory language).

140. 269 U.S. 385 (1926).

141. *Id.* at 395.

142. *Id.* at 391.

143. *See* United States v. Williams, 553 U.S. 285, 304 (2008) (explaining that a statute is found to violate due process if it is so vague it enables "seriously discriminatory enforcement"); *Kolender*, 461 U.S. at 358 ("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.'" (quoting Smith v. Goguen, 415 U.S. 566, 575 (1974))).

144. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 943 (4th ed. 2011).

145. *Kolender*, 461 U.S. at 370 (White, J., dissenting) (describing how precise drafting is required for First Amendment cases because the vagueness doctrine demands a "greater degree of specificity" when concerning expression).

146. CHEMERINSKY, *supra* note 144, at 941–43; *see also* United States v. Mazurie, 419 U.S. 544, 550 (1975) ("It is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in light of the facts of the case at hand.").

147. *See* Grosjean v. Am. Press Co., 297 U.S. 233, 244 (1936) (holding that a state law deprived a newspaper corporation of the liberty guaranteed under the

In the context of the CFAA, application of the vagueness doctrine revolves largely around the nebulous concepts of "authorization" and "access." There are certainly clear examples of unauthorized access to a protected computer that do not raise vagueness concerns.[148] Such instances include the injection of malicious code or the use of other hacking techniques to bypass a firewall, or infecting a website with malicious code to collect network passwords so the wrongdoer can sell them or otherwise disclose their contents.[149] These types of cases appear to be clear-cut examples of hacking that should implicate liability for unauthorized access. However, a significant gray area exists primarily in instances of "insider" access.[150] Courts are therefore tasked with striking a balance that both prevents over-punishment and deters unauthorized access, while staying within the boundaries of due process.

## II. BROAD INTERPRETATIONS OF UNAUTHORIZED ACCESS MAY RENDER THE CFAA UNCONSTITUTIONALLY VAGUE

The broadest and most troublesome provision of the CFAA is § 1030(a)(2)(C), which creates criminal liability for whoever "intentionally . . . exceeds authorized access, and thereby obtains . . . information from any protected computer."[151] Many users easily satisfy the "obtains information" prong by simply observing

---

Fourteenth Amendment); Louis K. Liggett Co. v. Baldridge, 278 U.S. 105, 111 (1928) (explaining that it is well settled that "a corporation is a 'person' within the meaning of the due process clause" and accordingly may not be deprived of property without due process of law).

148. *See, e.g.*, United States v. Willis, 476 F.3d 1121, 1125–26 (10th Cir. 2007) (affirming a conviction under § 1030(a)(2)(C) when a collection agency employee gave access to customer accounts to his drug dealer in exchange for methamphetamine).

149. *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 368–69 (D. Conn. 2001) (denying motion to dismiss under a plain-meaning approach when the defendant hacked into a "financial transaction clearinghouse," obtained network passwords, and then blackmailed the company).

150. "Insider" access is closely linked to the idea of "exceeds authorized access," namely that one who has initial authorization and then later exceeds it is said to have done so from the "inside." By comparison, the idea of an "outsider" is associated with the idea of acting "without authorization" and embodies the typical conception of a hacker. *See, e.g.*, United States v. Nosal, No. 10-10038, 2012 WL 1176119, at *3 (9th Cir. Apr. 10, 2012) (en banc) ("'[W]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."); S. REP. NO. 104-357, at 6 (1996) ("The amendment specifically covers the conduct of an [outsider] who deliberately breaks into a computer without authority, or an insider who exceeds authorized access, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities.").

151. 18 U.S.C. § 1030(a)(2)(C) (2006).

information, including routine actions such as checking e-mail or visiting a website.[152] In addition, almost anything with a microchip qualifies as a "protected computer."[153] Accordingly, criminal liability turns on the first prong: what does it mean to exceed authorized access?[154] The answer to this question is critical, yet the statute does not provide any meaningful guidance.[155] Broad interpretations, including those that would find liability for violations of written access agreements[156] or breaches of agency law duties,[157] raise significant problems of overbreadth and vagueness necessitating a more narrowly-tailored approach.

While the current approaches to interpreting unauthorized access under the CFAA may offer viable options for some factual scenarios, mobile app data privacy cases present new concerns not adequately addressed by these theories. The contract-based approach, most frequently applied in employment contract cases, does not translate to the world of mobile apps where there typically are no privacy-policy agreements between an app developer and an app user.[158] Even if an app includes a privacy policy, the app developer writes the terms and therefore can dictate the ambit of authorization.[159] This

152. *See supra* notes 44–45 and accompanying text (describing the broad scope of the statute); *see also* United States v. Tolliver, No. 08-26, 2009 WL 2342639, at *5 (E.D. Pa. 2009) (citing S. REP. NO. 99-432, at 2484 (1986)) (stating that "obtaining information" under the statute requires merely observing, not actually removing, the information), *aff'd*, 451 F. App'x 97 (3d Cir. 2011).

153. *See supra* Part I.A.3 (discussing the scope of "protected computer" as concurrent with the breadth of commerce clause jurisdiction).

154. *See generally* 18 U.S.C. § 1030 (defining "authorized access" and laying out the criminal elements of computer fraud); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (interpreting § 1030 and what constitutes "authorized access"), *cert. denied*, 131 S. Ct. 2166 (2011).

155. *See* 18 U.S.C. § 1030(e)(6) (providing an arguably-circular definition of "exceeds authorized access"—"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 to so obtain or alter"—but failing to define the scope of entitlement).

156. *See, e.g.*, *Rodriguez*, 628 F.3d at 1263 (employing the contract-based approach to criminally punish a SSA employee for violating the administration's computer terms of use agreement); United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (ultimately rejecting the contract-based approach when applied to website terms of service agreements).

157. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134–35 (9th Cir. 2009) (criticizing and rejecting the agency-based approach); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (adopting the agency-based approach).

158. *See* Thurm & Kane, *supra* note 10 (finding that forty-five out of the 101 most popular apps do not have privacy policies); Mark Hachman, *Most Mobile Apps Lack Privacy Policies: Study*, PCMAG.COM (Apr. 27, 2011, 7:30 AM), http://www.pcmag.com/article2/0,2817,2384363,00.asp (describing a recent study concluding that only nineteen percent of the top 340 free apps utilize privacy policies).

159. *See* United States v. Nosal, No. 10-10038, 2012 WL 1176119, at *4 (9th Cir. Apr. 10, 2012) (en banc) (detailing how a broad, contract-based interpretation of

discretion essentially allows the developer to manipulate the policy "so as to turn [the user-developer relationship] into one policed by the criminal law."[160] Problems of fair notice and arbitrary or discriminatory enforcement consequently arise when criminal liability "turn[s] on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read."[161] Similarly, application of the agency-based approach presents fair notice problems. As the agency-based approach interprets unauthorized access as a breach of a duty of loyalty, app developers would engage in unauthorized access any time a user felt that the app infringed on his subjective interests.[162] Accordingly, under either the contract- or agency-based theory, app developers do not have fair notice of what conduct is either without authorization or exceeding authorized access, and the CFAA therefore runs afoul of the vagueness doctrine.

### *A. The Contract-Based Approach Raises Fair Notice Concerns for Mobile Apps*

To apply the contract-based approach to mobile apps, the first task is to identify which documents or agreements constitute contracts.[163] The most obvious examples are app privacy policies. Applying the contract-based theory, an app developer who violates the terms of a privacy policy and obtains information from a user's phone would have accessed information in excess of his authorization.[164]

---

"exceeds authorized access" would criminalize innocuous Internet browsing if such activities technically violated an employer's terms of use agreement); *see also* Letter from Laura W. Murphy, Director, ACLU Washington Legislative Office et al., to U.S. Sens. Leahy & Grassley (Aug. 3, 2011), *available at* http://cdt.org/files/pdfs/CFAA_Sign-on_ltr.pdf (describing, as a "gross misuse of the law," the adherence to a strict contract-based interpretation to allow private corporations to establish what conduct violates federal criminal law).

160. *See Drew*, 259 F.R.D. at 465 (articulating that vagueness problems will result if a website owner can set the scope of criminal conduct through a terms of service agreement).

161. *See Nosal*, 2012 WL 1176119, at *4 (explaining that while many computer-use policies limit employee use to only "business purposes," such a restriction is inherently vague and also virtually meaningless in light of the fact that employers rarely discipline the occasional use of work computers for personal purposes).

162. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (finding a former employee liable for access "without authorization" under § 1030(a)(2)(C) when he acquired interests adverse to those of his employer).

163. *See supra* notes 78–80 and accompanying text (describing various types of documents that can be considered contracts, including both formal and informal agreements).

164. *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that violating the Social Security Administration computer-use policy, considered by the court to be a contract, constituted "exceeding authorized access"); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (noting that corporate policies can define "the purposes for which access is 'authorized'" such that a violation of the corporate

Accordingly, the app developer would have violated § 1030(a)(2)(C)'s prohibition on merely obtaining information from a protected computer in excess of authorization.[165] The problem with this approach, however, is that app developers, not end-users, write the privacy policies. Therefore, the policy is open to manipulation that would protect developers while still leaving end-users vulnerable to broad privacy policies with no consequences for infringing developers.

It may be easiest to see the problem by looking at the typical cases in which courts employ the contract-based approach: employment disputes. In the typical employment case, an employee violates the terms of an employment contract by accessing files on his employer's network to which the employee either: (1) has not been given express permission, known as access without authorization;[166] or (2) uses information to which he had initial access in a manner inconsistent with the scope of his employment, known as exceeding authorized access.[167] Analogizing to the world of mobile applications, it is the end-user that should be viewed as the "employer" and the app developer as the "employee," since it is the app developer who is acting without or in excess of his authorized access.[168] Given this strange juxtaposition, an app developer has the power to dictate the terms by which he may access the user's data.[169] Accordingly,

---

policy is an impermissible access in excess of authorization); United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997) (holding that violation of employment contract limiting computer use to "official purposes" constituted "exceeding authorized access").

165. 18 U.S.C. § 1030(a)(2)(C) (2006).

166. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (differentiating "without authorization" as "access[ing] a computer [or portion thereof] without any permission at all," from "exceeds authorized access" as a person who "has permission to access the computer, but accesses information on the computer that the person is not entitled to access"); *see also* United States v. Phillips, 477 F.3d 215, 220–21 (5th Cir. 2007) (upholding, on "without authorization" grounds, the conviction of a student who used his privileges on a university computer to access part of the system to which he did not have a password).

167. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001) (concluding that a former employee exceeded authorized access by violating a broad confidentiality agreement when he created a high-speed "scraper" program to mine a former employer's public website for pricing information).

168. *See* Complaint ¶ 45, Hines v. OpenFeint, Inc., No. CV-11-3084 (N.D. Cal. June 22, 2011), 2011 WL 2471471 (alleging breach of contract when mobile-gaming network company accessed, without authorization, users' personal information for marketing analytics and targeted advertising profiles); Complaint at 3–4, 68–70, Lalo v. Apple, Inc., No. 10-cv-05878 (N.D. Cal. Dec. 23, 2010), 2010 WL 5393496 (alleging that app developers and mobile advertisers acted without authorization or exceeded authorized access when their apps acquired personal information such as gender, age, race, geographic location, and household income without express permission from the user).

169. *See* United States v. Drew, 259 F.R.D. 449, 465 (C.D. Cal. 2009) ("[T]erms of

developers have little incentive to even include a privacy policy, let alone draft one to include anything less than the broadest possible authority to access a user's information.[170] Essentially, this approach puts app developers in a position to manipulate privacy policies by simultaneously altering the user-developer relationship into one governed by criminal law while drafting broad enough policies to insulate the developer from any liability.[171] This, in turn, implicates the vagueness doctrine by failing to provide adequate notice of what specific conduct constitutes a violation of law while concurrently inviting arbitrary and discriminatory enforcement.

The recent case *Drew* illustrates this point.[172] While the court in *Drew* refused to find a violation of a website TOS agreement tantamount to a § 1030(a)(2)(C) violation, the court did not pronounce that TOS agreements may never govern authorization.[173] Rather, the court reasoned that creating a situation where some TOS agreements (or merely some provisions), but not others, dictate the scope of authorized access creates an inherently unclear situation where users do not have fair notice as to what conduct implicates criminal liability.[174] This approach also fails the second prong of the vagueness doctrine because the statue would lack minimum guidelines to preclude arbitrary and discriminatory enforcement.[175]

---

service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users.").

170. *See id.* ("[W]ebsite owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards.").

171. Those in favor of a contract-based approach to determine the scope of authorized access have also turned to the tort of trespass for support. *See* Brief for Oracle Am. Inc. as Amicus Curiae Supporting Plaintiff-Appellants, United States v. Nosal, 642 F.3d 781 (9th Cir. 2011) (No. 10-10038), *available at* http://volokh.com/wp/wp-content/uploads/2011/12/Oracle-America-Amicus.pdf (citing the *Restatement (Second) of Torts* to argue that the tort of trespass can govern written restrictions on access because any conclusions are derived from factually-driven, common-sense, totality of the circumstances analyses). This trespass-oriented approach, however, fails to support the use of written access restrictions in the CFAA context because the CFAA is a criminal statute subject to vagueness concerns whereas the standard for the common law trespass tort is inherently unclear. *See* Orin Kerr, *The Trespass Tort Versus the CFAA: A Response to the Oracle Amicus Brief in* Nosal, VOLOKH CONSPIRACY (Dec. 5, 2011, 6:30 PM), http://volokh.com/2011/12/05/the-trespass-tort-versus-the-cfaa-a-response-to-the-oracle-amicus-brief-in-nosal/ (discussing the conceptual differences between physical trespass and computer-based trespass to discount the trespass-tort approach as unpersuasive and improperly applied to the CFAA).

172. 259 F.R.D. 449 (C.D. Cal. 2009); *supra* notes 88–96 and accompanying text (discussing the *Drew* decision).

173. *Drew*, 259 F.R.D. at 466.

174. *See id.* at 464 (explaining that a contract-based interpretation of the CFAA fails to provide fair notice because "it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will").

175. *See id.* at 467 (concluding that a contract-based approach would result in §

Permitting website owners to dictate the line for criminality in the form of easily-amendable TOS agreements, which few people actually read,[176] creates a similarly non-definite situation encouraging arbitrary and discriminatory enforcement in contravention of the vagueness doctrine.[177]

The website TOS approach is directly analogous to mobile app privacy policies. By placing the power in the hands of app developers not only to dictate initial access rights, but to freely amend the terms to comport with the developer's whims with minimal, if any, notice to users, the CFAA's prohibitions on access without authorization would not have sufficient clarity to provide fair notice as to what conduct actually violates the statute.

### *B. The Agency-Based Approach Raises Arbitrary Enforcement Concerns for Mobile Apps*

The agency-based approach focuses on the idea that an agent violates the CFAA's unauthorized access prohibitions by breaching a fiduciary duty of loyalty to the principal.[178] Further, the agent is said to breach that duty of loyalty by engaging in conduct inconsistent with the interests of the principal.[179] On its face, it is difficult to extrapolate the agency-based approach to mobile apps, since there is no obvious principal-agent relationship between an app developer and an end-user akin to a typical employer-employee relationship.[180]

---

1030(a)(2)(C) "becom[ing] a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]'" (quoting City of Chicago v. Morales, 527 U.S. 41, 64 (1999))).

176. *See, e.g.*, Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I.S.J.L.P. 543, 555, 565 (2009) (calculating that the average website privacy policy takes approximately ten minutes to read and estimating that to read every privacy policy for each website visited would require approximately 201 hours per person per year and cost each person about $3534 in lost annual productivity); *Privacy Policy Infographic*, SELECTOUT.ORG (Jan. 28, 2011), http://selectout.org/blog/privacy-policy-infographic/ (analyzing the 1000 most-visited websites and calculating that the average privacy policy is 2462 words long with the longest policy over 11,000 words long).

177. *See* Kerr, *supra* note 40, at 1582 & n.163 (describing the infrequency with which users read terms-of-service contracts, and discussing the absurd results that can follow from allowing these agreements to govern access rights).

178. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (invoking § 387 of the *Restatement (Second) of Agency* to conclude that a former employee violated his duty of loyalty when "he resolved to destroy files . . . that were . . . the property of his employer").

179. RESTATEMENT (SECOND) OF AGENCY § 112 (1958); *see also* WILLIAM A. GREGORY, THE LAW OF AGENCY AND PARTNERSHIP 103 (3d ed. 2001) (explaining that beginning work for a competitor is tantamount to obtaining an adverse interest).

180. *See* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006) ("[B]y reading *Restatement* [*(Second) of Agency*] § 112 legalese into the meaning of 'without authorization,' the term becomes equipped with a breadth that effectively shaves 'exceeds authorized access' down to a

The app developer, however, is the party "obtaining" information purportedly in violation of the interests of the app user,[181] and, as such, the app developer is in the same position as the employee/agent for purposes of the principal-agent connection. The key problem with trying to employ the agency-based approach to mobile app cases, however, is that there may be millions of users of a single app, each with invariably different "interests."[182] Accordingly, an app's information-collection plan may comport with the interests of some users but directly conflict with those of others.[183] The agency-based approach would then permit criminal prosecution and civil liability when the app collects information adverse to the subjective interests of a single user.[184] Such an approach falls short of providing developers with fair notice of what information their apps may obtain to avoid exceeding authorized access and implicating liability.[185]

The recent case *Nosal* illustrates the difficulty of applying the

---

mere sliver of what its plain meaning suggests."); *see also* Field, *supra* note 110, at 843–44 (discussing the difficulties of applying the "elusive and nebulous" principles of common-law fiduciary duties to a statutory setting, and noting agency law's "potential for manipulability" to obtain outcomes commonly "cloaked in moralistic terms").

181. *See* Complaint ¶ 47, Hines v. OpenFeint, Inc., No. CV-11-3084 (N.D. Cal. June 22, 2011), 2011 WL 2471471 (alleging that the use of personal information collected through a mobile-gaming app for purposes of marketing and targeted advertising violated user's privacy interests); Complaint at 68–70, Lalo v. Apple, Inc., No. 10-cv-05878 (N.D. Cal. Dec. 23, 2010), 2010 WL 5393496 (alleging that the collection of purportedly personal information through mobile apps violated users' privacy interests).

182. *See Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location*, NIELSEN.COM (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location (finding that mobile app users' concerns over privacy vary based on both gender and age demographics). Nielsen's research shows, for example, that only a slight majority of men (fifty-two percent) and women (fifty-nine percent) are concerned about privacy relating to location-based apps. *Id.*

183. *Id.*; *see Lockheed Martin*, 2006 WL 2683058, at *7 (rejecting the agency-based approach in part because "the 'adverse interest' inquiry affixes remarkable reach to the [CFAA]" such that an employee checking e-mail on company time could implicate criminal liability).

184. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (upholding an employee's liability under the CFAA when he breached a duty of loyalty to his employer, thereby severing the agency relationship, and therefore acting without authorization); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (applying the *Restatement* to hold that authorization ceases when an agent acts with an interest adverse to that of the principal).

185. Despite the potential fair-notice problems and the inconsistencies of importing agency law principles into the CFAA, some courts continue to rely on the *Citrin* approach if there is a "pattern of activity adverse to [an] employer's interests." *See* Deloitte & Touche L.L.P. v. Carlson, No. 11 C 327, 2011 WL 2923865, at *4–5 (N.D. Ill. July 18, 2011) (denying a motion to dismiss a CFAA claim against a former employee who destroyed data on a company-issued laptop, and holding that a breach of a duty of an employee's duty of loyalty can support a "without authorization" claim under § 1030(a)(2)).

agency-based approach without implicating vagueness concerns.[186] In *Nosal*, the majority en banc ultimately concluded that an employee does not exceed authorized access when that access violates an employer's computer-use restrictions.[187] Accordingly, the employee was not liable under the CFAA despite acting contrary to his employer's interest and breaching a state-law duty of loyalty.[188] In reversing the panel decision, which reached a contrary conclusion in large part because Nosal was charged with violating § 1030(a)(4) and not the broader § 1030(a)(2)(C),[189] the court reasoned that principles of statutory construction foreclosed interpretation of "exceeds authorized access" in different ways for each subsection when Congress provided only one statutory definition.[190]

The en banc court corrected the panel's failure to recognize that the panel's interpretation of "exceeds authorized access" under § 1030(a)(4) would drastically change the scope of the already broader § 1030(a)(2)(C), which has no intent-to-defraud requirement.[191] By contrast, the en banc court reasoned that by utilizing an employer's computer-use restrictions to define the boundaries of "exceeding authorized access" under § 1030(a)(4), anyone who obtains information from a computer connected to the Internet, in contravention of those restrictions, violates § 1030(a)(2)(C).[192] Such an interpretation creates a situation not only where criminal liability rests on employer restrictions that are "not necessarily drafted with the definiteness or precision that would be required for a criminal statute,"[193] but would also make the CFAA ripe for arbitrary and

186. *See supra* notes 101–09 and accompanying text (discussing the *Nosal* decision).

187. No. 10-10038, 2012 WL 1176119, at *7 (9th Cir. Apr. 10, 2012) (en banc).

188. *See id.* at *9 (Silverman, J., dissenting) (articulating how the court's decision in *Brekka* foreclosed "exceed[ing] authorized access" liability for duty of loyalty breaches).

189. Section 1030(a)(4) requires both intent to defraud and violative access that furthers the intended fraud. 18 U.S.C. § 1030(a)(4) (2006). In contrast. § 1030(a)(2)(C) has no such mens rea requirement. *Id.* § 1030(a)(2)(C).

190. *Nosal*, 2012 WL 1176119, at *4.

191. *Compare* 18 U.S.C. § 1030(a)(4) (covering "[w]hoever *knowingly and with intent to defraud* [accesses] a protected computer without authorization" (emphasis added)), *with id.* § 1030(a)(2) (covering "[w]hoever *intentionally accesses* a computer without authorization or exceeds authorized access" (emphasis added)).

192. *Nosal*, 2012 WL 1176119, at *5; *see also* United States v. Nosal, 642 F.3d 781, 790 (9th Cir. 2011) (Campbell, J., dissenting) (arguing, on similar vagueness grounds, against the broader interpretation of "exceeds authorized access" in order to avoid criminalizing innocuous computer use), *rev'd en banc*, No. 10-10038, 2012 WL 1176119 (9th Cir. Apr. 10, 2012). *But see Nosal*, 2012 WL 1176119, at *10 (Silverman, J., dissenting) (arguing that the en banc majority improperly "posit[ed] a laundry list of wacky hypotheticals" under § 1030(a)(2)(C) instead of focusing purely on § 1030(a)(4)).

193. *Nosal*, 642 F.3d at 790 (Campbell, J., dissenting).

discriminatory enforcement[194] and render the statute unconstitutionally vague.[195]

These vagueness concerns similarly arise in attempting to apply the agency theory to mobile app data privacy cases. Reading a duty of loyalty into the relationship between app developers and users would mean that anytime an app obtained any information from a user's phone, in violation of the interests of the user, the app developer would be guilty of a federal crime under § 1030(a)(2)(C).[196] While the panel majority in *Nosal* tried to counter this line of argument by imposing a requirement that the employee/agent "ha[ve] knowledge" of the employer/principal's limitations in order to implicate liability, this requirement has no support in either the text of the CFAA nor the legislative history, "and only becomes necessary upon adopting the [panel] majority's interpretation of 'exceeds authorization.'"[197]

Application of the agency-based approach essentially means that each time an agent "obtains" information from a protected computer that does not further the principal's interest, such as checking personal e-mail or a personal Facebook account, each instance can amount to a federal crime.[198] In the context of mobile apps, each time an app accesses a piece of user information for purposes other than what the user considers to be within the scope of his interests, the app developer is obtaining information from a protected computer in violation of § 1030(a)(2)(C).[199] Accordingly, the agency-

194. *Nosal*, 2012 WL 1178119, at *6 (rejecting the government's assurance that it would not prosecute minor violations and noting that "the difference between puffery [in the form of lying about age or height on a social media website] and prosecution may depend on whether you happen to be someone an AUSA has reason to go after").

195. *Id.* at *6–7 (combining a discussion of the vagueness doctrine's fair notice and arbitrary or discriminatory enforcement prongs with the court's related rule of lenity concerns).

196. *See Nosal*, 642 F.3d at 788 ("[A]s long as the employee has knowledge of the employer's limitation on that authorization, the employee 'exceeds authorized access' when the employee violates those limitations.").

197. *Id.* at 790 n.3 (Campbell, J., dissenting).

198. *See* Kerr, *supra* note 40, at 1586–87 ("[A] broad agency theory of authorization would turn millions of employees into criminals [and] give the government the power to arrest almost anyone who had a computer at work . . . ."); *see also* Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug. 1, 2006) (cautioning against the agency-based approach and suggesting that merely checking personal e-mail at work could amount to CFAA liability).

199. *See Nosal*, 2012 WL 1176119, at *5 (noting that merely visiting ESPN.com or playing sudoku from a work computer would be transformed into a federal crime); *Nosal*, 642 F.3d at 790 (Campbell, J., dissenting) (explaining that merely "viewing" information for any purpose adverse to the interest of the computer owner would be grounds for a federal crime).

theory approach does not provide fair notice to app developers as to what kinds of specific information an app may obtain without implicating liability under the CFAA. Absent such fair notice, the CFAA fails to comport with due process under the vagueness doctrine.[200]

### *C. The Code-Based Approach is Under-Inclusive Because it Ignores the Problem of Insider Misuse of Information*

At first blush, the code-based approach seems like a simple and attractive way to define the limits of authorized access to computers.[201] However, the theory does not adequately address the issue of insider misuse of information by failing to protect unsophisticated users, limiting liability to only those acting without authorization, and failing to provide a remedy for unauthorized access to data stored by third parties.

Under this view, a person acts without authorization by circumventing computer-code-based restrictions.[202] Similarly, the person acts in excess of authorization if she has initial permission to access a computer but then bypasses a code-based restriction to access other information on a different part of the computer or network.[203] The code-based approach therefore places the burden of safeguarding information on the computer owner, instead of burdening the accesser to rigidly comply with either the express terms of a contract or the vague notion of the owner's interests.[204] By punishing the exploitation of vulnerabilities through malicious code

---

200. *See* City of Chicago v. Morales, 527 U.S. 41, 57, 64 (1999) (expounding the notion that criminal statutes must provide fair notice in order to comport with due process and avoid constitutional vagueness).

201. *See* Kerr, *supra* note 23, at 1649 (arguing that the code-based approach strikes a balance between the often-conflicting goals of Internet regulation: Internet-freedom and data-protection).

202. *See* Garrett D. Urban, Comment, *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, 1379–80 (2011) (describing access in excess of authorization as requiring a person with initial access to "fake identification, 'exploit a weakness in the code,' or affirmatively act to misuse the computer in some way").

203. *Id.*; *see also* Fink v. Time Warner Cable, 810 F. Supp. 2d 633, 638, 643 (S.D.N.Y 2011) (denying a motion to dismiss a complaint against mega-ISP Time Warner for "throttling" peer-to-peer file-sharing speeds, and employing a "plain meaning," dictionary-definition approach to determine the scope of access).

204. *See* Urban, *supra* note 202, at 1380 n.66 (citing State v. Riley, 988 A.2d 1252, 1258 (N.J. Super. Ct. Law Div. 2009)) (acknowledging that courts have not yet adopted a code-based interpretation for the CFAA, but identifying one such judicial interpretation in reference to a state computer fraud statute); *see also* Sw. Airlines Co. v. BoardFirst, L.L.C., No. 3:06 Civ. 0891-B, 2007 WL 4823761, at *8 (N.D. Tex. Sept. 12, 2007) (utilizing a dictionary-definition approach to define access as "to get at" or "gain access to" similar to the code-based approach).

or "tricking" the computer by using someone else's username and password, the code-based theory comes closest to addressing the original intent of the CFAA as an anti-hacking provision,[205] and therefore provides a strong remedy for outsider access that is inherently "without authorization."

However, this focus on bypassing security as the sole means of defining unauthorized access in effect blurs the line between access "without authorization" and access that "exceeds authorization," a distinction that both the plain text of the CFAA[206] and legislative history strongly support.[207] Absent this distinction, the CFAA would offer no protection to unsophisticated users, such as a homeowner who fails to secure a wireless network or a careless business owner.[208] More importantly, this approach would fail to implicate liability for an insider who is given authorization to access a computer, but then later misuses information on the computer.[209] There would be no cause of action even if the insider causes significant damage either to the computer itself—deleting files, inserting malicious code, etc.—or to its owner, perhaps through disclosure or sale of sensitive information to a third party.[210] Applying the code-based approach to

---

205. *Compare* Kerr, *supra* note 23, at 1644–45 (discussing circumvention of regulation by code through masquerade or malicious manipulation of computer weaknesses), *with* S. REP. NO. 99-432, at 6–7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485 (discussing the need to balance concern for authorized users "against the legitimate need to protect Government computers against abuse by 'outsiders'").

206. *See* 18 U.S.C. §§ 1030(a)(2), (4)–(5) (2006) (specifically prohibiting *either* access without authorization *or* actions that exceed authorized access). Collapsing these two phrases into one does not comport with the Supreme Court's recurrent position that statutory interpretations should avoid rendering terms superfluous. Nken v. Holder, 556 U.S. 418, 442 (2009); Negonsott v. Samuels, 507 U.S. 99, 106 (1993) (citing Moskal v. United States, 498 U.S. 103, 109 (1990)); Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979).

207. *See* S. REP. NO. 104-357, at 4 (1996) (discussing the dichotomy between the CFAA's privacy protection coverage for outsider perpetrators who obtain nonclassified information via unauthorized computer access on one hand and "[g]overnment employees who abuse their computer access to obtain Government information that may be sensitive and confidential"); *see also* Chung, *supra* note 85, at 246 (citing United States v. Drew, 259 F.R.D. 449, 460 (C.D. Cal. 2009)) (discussing the distinction between "without authorization" and "exceeds authorization" language).

208. Winn, *supra* note 76, at 1421.

209. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1272–73 (N.D. Iowa 2000) (recognizing that access in the CFAA context cannot be defined without considering the "freedom or ability to . . . make *use* of something" (emphasis added) (quoting MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 6 (10th ed. 1994)) (internal quotation marks omitted)). The court there further explained that "[f]or purposes of the CFAA, when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of computers until it reaches its destination, the sender is making use of all of those computers, and is therefore 'accessing' them." *Id.* at 1273.

210. *See* Winn, *supra* note 76, at 1420 (analogizing to the tort of trespass to chattels to argue that the code-based approach "leaves data subjects with no legal remedy

mobile app cases, an app developer would only be subject to liability under the CFAA if the developer circumvents some kind of safeguard built into the phone, such as a username/password or other security measure, but not if the developer seriously misuses any information obtained through the app or damages the user's phone.

Critics of the code-based approach have raised similar concerns over its rigid and under-inclusive nature, noting "code-based theory limits data owners' flexibility in the ways they might choose to protect their data."[211] Moreover, the code-based approach does not appear to provide an avenue for relief for users' data stored by a third party, such as in the instance of cloud computing.[212] In short, the code-based approach's attempt to simplify unauthorized access fails to offer a remedy for harm resulting from access in excess of authorization despite the CFAA's explicit distinction between insider and outsider access.

## III. COURTS SHOULD LIMIT INTERPRETATIONS OF UNAUTHORIZED ACCESS TO TRADITIONAL NOTIONS OF HACKING OR SERIOUS MISUSE OF INFORMATION

As the broader agency- and contract-based views raise significant vagueness concerns, commentators have stressed the importance of a narrow view in order to not only avoid constitutional issues,[213] but also to shift the focus of the statute towards its original intent as an anti-hacking provision.[214] The code-based approach, which limits unauthorized access to the circumvention of any computer-code restrictions, appears superficially to provide a straightforward method for interpreting unauthorized access.[215] However, this view blurs the

against unauthorized intruders into their private data").

211. Chung, *supra* note 85, at 247; *see also* Winn, *supra* note 76, at 1419 (arguing that the code-based approach "artificially restricts the set of norms to which courts are permitted to look, to . . . a system of 'norms by nerds'").

212. *See* Chung, *supra* note 85, at 247 (criticizing Kerr's argument about incentives due to situations involving third-party possession of data including cloud computing).

213. *See* Kerr, *supra* note 23, at 1658–59 (advocating a code-based approach to avoid the overbreadth and vagueness concerns associated with a contract-based approach to interpreting unauthorized access).

214. *See* Urban, *supra* note 202, at 1406–10 (proposing a fraud-based amendment to the CFAA in order to realign the statute with the original focus on hackers and outsiders); *see also* Darden, *supra* note 34, at 356, 359 (arguing that absent a simplified approach to interpreting unauthorized access under the CFAA, Congress needs to adopt an entirely new statute to cover post-access conduct such as cyberbullying and online harassment).

215. *See* Kerr, *supra* note 23, at 1649 ("Access should be deemed 'without authorization' only when it either violates the *Morris* intended function test, or else uses false identification to trick the computer into granting the user greater privileges.").

line between access without authorization and access in excess of authorization, and it also fails to provide a remedy for cases of insider misuse of information.[216] By limiting the scope of unauthorized access to traditional notions of hacking for outsider cases and misuse of information for insider cases, courts can promote the CFAA's original intent as an anti-hacking statute and address insider cases without implicating the vagueness doctrine.[217]

### *A. Legislative History Does not Unambiguously Support the Agency-, Contract-, or Code-Based Approaches*

As courts struggle to interpret the scope of authorized access under the CFAA, judges often rely on legislative history for insight into legislative purpose or intent.[218] Courts and commentators tend to agree that instances of traditional hacking by "outsiders" present relatively uncomplicated questions of unauthorized access liability, so the focus of legislative history analysis often revolves around discussion of insider liability.[219] This approach also makes sense for evaluating mobile app data privacy cases, as apps gain access to user data through user-download of the app and not some kind of forced entry into the phone through malicious code.[220] Courts, however,

---

216. *See* Winn, *supra* note 76, at 1419 (arguing that the code-based approach is "flatly inconsistent" with both the plain language of the statute and the 1996 legislative history).

217. The Supreme Court recently addressed the vagueness doctrine, albeit in the context of the "honest-services" doctrine of mail- and wire-fraud statutes, by articulating that concerns about constitutional vagueness necessitate a narrower statutory construction. *See* Skilling v. United States, 130 S. Ct. 2896 (2010) (finding the application of 18 U.S.C. § 1346 to bribery and kick-back schemes did not violate either prong of the vagueness doctrine: (1) fair notice and (2) arbitrary and discrimination prosecutions). In *Skilling*, the Court ultimately held that 18 U.S.C. § 1346—prohibiting wire fraud that causes harm in the form of the denial of the "injured" party's right to the offender's "honest services" even though the betrayed party suffered no deprivation of money or property—did not violate the vagueness doctrine. *Id.* at 2933. Notably, the Court said that narrow and limited statutory constructions must be considered prior to striking a federal statute as unconstitutionally vague. *Id.* at 2929 (citing Hooper v. California, 155 U.S. 648, 657 (1895)).

218. *See* Stephen Breyer, *On the Uses of Legislative History in Interpreting Statutes*, 65 S. CAL. L. REV. 845, 848–61 (1992) (discussing five reasons for turning to legislative history to interpret a statute, including (1) avoiding an absurd result, (2) correcting drafting errors, (3) deciphering specialized terms, (4) discerning the "reasonable purpose" of a particular provision, and (5) deciding between competing "reasonable purposes").

219. *See* Field, *supra* note 110, at 831 (explaining that "outsider" liability—traditional hackers breaking into computers—is clearly articulated in legislative history, but the scope of "insider" access has been consistently unclear).

220. *See* Claire Cain Miller, *For Hackers, The Next Lock to Pick: Companies See Opportunity In Cellphone Security*, N.Y. TIMES, Sept. 28, 2011, at B1 (discussing how app users can be tricked into downloading infected apps laden with malicious code, but also noting the possibility of remote hacks similar to traditional computer break-ins).

tend to use legislative history to merely support the approach that they have already decided to adopt.[221]

Early congressional discussions of insider liability arguably lend some support to both agency- and contract-based interpretations.[222] Specifically, commentary surrounding the 1984 act suggests that Congress wanted to preclude liability for access in furtherance of a "legitimate business purpose . . . pursuant to an express or implied authorization," yet failed to clarify what would constitute a legitimate business purpose.[223] Further, congressional discussions of the 1986 amendments focused on the "improper" nature of access, but still did not detail how insiders were to ascertain what was, in fact, proper.[224] On one hand, discussions of "legitimate purposes" arguably lend support for the agency-based view, which focuses on the amorphous interests of a principal to define limits of the agent's authorization.[225] By attempting to limit liability to only harmful, illegitimate purposes, the legislative history supports the notion that Congress intended the scope of authorization to be defined according to employer policies or perhaps accepted norms of typical employee computer usage.[226] On the other hand, "legitimate business purposes" or the scope of proper access could be clearly defined in some form of contract.[227]

---

221. Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (relying on legislative history to support a plain-meaning approach nearly identical to a code-based view); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127–29 (W.D. Wash. 2000) (utilizing legislative history to support the agency-based approach and to "demonstrate the broad meaning and intended scope of the terms 'protected computer' and 'without authorization'").

222. *See* H.R. REP. NO. 98-894, at 21 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3707 (explaining that insider liability will not arise in instances of "information incidentally obtained or . . . obtained legitimately," and also "does not extend to any type or form of computer access that is for a legitimate business purpose"); *see also* Field, *supra* note 110, at 831 (explaining that congressional discussions suggested that its understanding of authorization centered around the "purpose of access," which could fit with either the agency- or contract-based approach).

223. *See* H.R. REP. NO. 98-894, at 21, *reprinted in* 1984 U.S.C.C.A.N. at 3707 (explaining only that the CFAA is designed to "impose[] criminal sanctions upon 'hackers' and other criminals who access computers without authorization" but does not extend to any "normal and customary business procedures and information usage").

224. *See* H.R. REP. NO. 99-612, at 7 (1986) (noting, without elaboration, that "[t]he improper modifications, destructions or disclosures by authorized users . . . are covered presently by [§ 1030(a)(3)]").

225. H.R. REP. NO. 98-894, at 15, *reprinted in* 1984 U.S.C.C.A.N. at 3701 (articulating an exemption from criminal liability for "incidential [sic] use[s] of the computer . . . [such as] do[ing] homework or play[ing] computer games").

226. *See* Field, *supra* note 110, at 831–32 (explaining that the "original understanding [of insider liability] was more on par with the agency-based or contract-based interpretations later used by courts than the code-based interpretations").

227. *See generally* United States v. Phillips, 477 F.3d 215, 219–21 (5th Cir. 2007) (noting that website owners can establish the extent to which the public may access

However, the 1986 amendments also replaced notions of "purpose" in the definition of "exceeds authorized access" with the current language precluding access to information to which the accesser is not "entitled."[228] This shift towards entitlement does little more than confuse the issue further, as there is no indication of whether entitlement is to be defined by some code-based limitations (i.e. username/password), contractual provisions, or a broader concept of employee loyalty.[229] Accordingly, legislative history lends some support to each of the three interpretations and does not provide a clear roadmap for which interpretation Congress intended to govern the scope of authorized access.

### *B. The Shortcomings of Current Theories of Interpreting Authorization Necessitate a Narrower View in Line with the Original Intent of the Statute as an Anti-Hacking Law*

While the broader agency- and contract-based approaches present vagueness concerns[230] and the code-based approach is inherently under-inclusive,[231] a narrower focus may be required to address mobile apps cases arising under the CFAA. By limiting interpretations of without authorization to impose liability for traditional hacking, such as the use of malicious code or various social-engineering techniques,[232] causes of action under the CFAA may harmonize with the primary intent of the statute as an anti-

---

information on its website through some form of user agreement); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001) (same); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 245–46 (S.D.N.Y. 2000) (same).

228. *Compare* Urban, *supra* note 202, at 1382 (describing the 1986 amendment to CFAA with a definition of authorization focusing on the user's purpose), *with* 18 U.S.C. § 1030(e)(6) (2006) (defining exceeding authorized access as access to information "that the accesser is not entitled so to obtain or alter").

229. Field, *supra* note 110, at 832.

230. *See supra* Parts II.A–B (describing the deficiencies of the contract- and agency-based approaches).

231. *See supra* Part II.C (describing the infirmities of the code-based approach in blurring the distinction between "without authorization" and "exceeds authorized access").

232. One common social engineering technique is called "phishing," which entails a "virtual trap set by cyber-thieves that uses official-looking e-mails to lure [the target] to fake websites and trick [the target] into revealing . . . personal information," and the variant called "spear-phishing" typically involves the criminal having some inside information about the target in order to convince the target of the authenticity of the fake email or website. *Spear Phishers: Angling to Steal Your Financial Info*, FBI.GOV (Apr. 1, 2009), http://www.fbi.gov/news/stories/2009/april/spearphishing_040109. For a detailed overview of social engineering techniques, see *Online Privacy, Social Networking, and Crime Victimization: Hearing before the Subcomm. on Crime, Terrorism, & Homeland Security of the H. Comm. on the Judiciary*, 111th Cong. 5–12 (July 28, 2010) (Remarks and Statement of Gordon M. Snow, Asst. Dir. Cyber Division, Federal Bureau of Investigation).

hacking provision.[233] In the context of mobile app cases, this view shifts the focus of the liability analysis away from invariably divergent interpretations of whether an app maker has an airtight privacy policy[234] or acts in accordance with the nebulous interests of a multitude of users.[235] Concurrently, by imposing liability on misuse of information for insider cases, the CFAA would also address instances of exceeding authorized access where data is obtained through non-pernicious and authorized means but ultimately used for harmful purposes.

The putative class action case *In re iPhone Application Litigation*[236] presents an instructive scenario. Here, a class of Apple iPhone owners alleged that they incurred damages as a result of certain mobile applications accessing purportedly personal information, including geo-location data, address book, and keystroke history.[237] The allegations further asserted that app developers and advertisers gained access to this personal information both without and in excess of authorization in violation of § 1030(a)(2)(C) and then profited from the sale of users' information for targeted advertising and marketing analytics purposes.[238] Applying the code-based approach, the class does not appear to have sufficient grounds to support an unauthorized access claim, since there is no circumvention of any code-based security measures.[239] Furthermore, the class appears to only allege vague damages or losses of more than $5000 aggregating over a one-year period, so the specific nature of the actual harm is

233. *See* S. REP. NO. 104-357, at 3 (1996) (articulating that the CFAA was "originally enacted . . . to provide a clear statement of proscribed activity concerning . . . those tempted to *commit crimes* by unauthorized access to computers" (emphasis added)); *id.* at 7 (noting that "subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign *theft* of information by computer" (emphasis added)); S. REP. NO. 101-544, at 4–5 (1990) (explaining that the CFAA's private right of action was intended to redress serious computer abuse by outsiders); S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482 (asserting that the CFAA was "aimed at deterring and punishing certain 'high tech' crimes").

234. *See supra* notes 169–70 and accompanying text (discussing the difficulties of employing privacy policies as the foundation for CFAA liability).

235. *See supra* notes 183–84 and accompanying text (discussing the propensity for arbitrary enforcement when employing users' interests as the basis for defining the scope of authorization).

236. No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865 (N.D. Cal. Sept. 20, 2011).

237. *Id.* at *9.

238. *Id.* at *9–10.

239. The class alleged that mobile advertisers obtained information from the user's phone after the user initiated and completed the download of an app. Second Amended Complaint at 3–5, *iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865 (No. 11-MD-02250-LHK). The complaint does not, however, make any mention of code-based restrictions in place to safeguard the purportedly personal information.

unclear and may only be the existence of more highly-targeted banner advertisements.[240]

Judge Koh recognized these concerns and dismissed the complaint, with leave to amend, for three reasons: (1) negligent software design is insufficient to support a CFAA claim; (2) users did not sufficiently allege that the defendants accessed their phones "without authorization" or that the defendants "exceed authorized access" by accessing their phones; and (3) app users have failed to identify specific economic damages.[241] The rationale behind this second deficiency in the complaint is particularly instructive, namely that the voluntary nature of the user's download of the app effectively precludes a "without authorization" claim.[242] This reasoning supports the idea that the CFAA should be limited to traditional hacking cases in the context of mobile apps, as the court appears to imply that only forcible intrusions into users' phones, like involuntarily downloaded apps, will support a "without authorization" claim.[243] Concurrently, the court left open the possibility that a claim against an app developer could still exist for accessing data in excess of authorization, but such a claim would require a specific harm to the user caused by the developer's access and not merely a generalized claim of privacy infringement.[244]

Rather than continually expanding the CFAA to address specific

---

240. *Id.* at 10.

241. *iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *35–37. Notably, Judge Koh used *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), for the definitions of "without authorization" and "exceeds authorized access," reliance on which indicates that the court would reject the agency-based approach. *iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *39.

242. *See iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *35–36 (citing *In re* Apple & ATTM Antitrust Litig., No. C 07-05152-JW, 2010 U.S. Dist. LEXIS 98270, at *26 (N.D. Cal. July 8, 2010)) (emphasizing that "voluntary installation runs counter to the notion that the alleged act was a trespass and to the CFAA's requirement that the alleged act was '*without authorization*' as well as the CPC's requirement that the act was '*without permission*'" (emphasis added)). Even in cases of voluntary download, there are numerous instances of apps accessing data on mobile devices beyond what was initially allowed in end user permissions. *See supra* note 21 (collecting cases involving allegations that apps, although voluntarily downloaded, improperly accessed personal information on a user's phone).

243. *iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *35–36; *see also* La Court v. Specific Media, No. SACV 10-1256-GW(JCGx), 2011 U.S. Dist. LEXIS 50543, at *17–18 (C.D. Cal. Apr. 28, 2011) (rejecting a similar data-privacy-based claim for failing to allege specific damages and unsuccessfully demonstrating that defendant intended damage to plaintiff's computers by inserting tracking cookies).

244. *See iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *36–37 (citing Bose v. Interclick, Inc., No. 10 Civ. 9183 (DAB), 2011 U.S. Dist. LEXIS 93663, at *12–14 (S.D.N.Y. Aug. 17, 2011)) (explaining that collection of personal information for advertising purposes, even if conducted "without permission," is insufficient to support a CFAA claim, but recognizing that identification of a "single act of harm" plus a showing of economic damage could suffice).

problems that happen to occur in the mobile space, utilizing other statutes may be a more effective means of combating certain types of abuses. For cases involving privacy interests of children, the Children's Online Privacy Protection Act (COPPA) affords specific remedies.[245] Indeed, the Federal Trade Commission (FTC) is now seeking to explicitly include mobile privacy cases involving children under the age of thirteen within COPPA and the FTC's COPPA Rule.[246] Further, the FTC's COPPA enforcement efforts leave little doubt that COPPA applies to mobile apps.[247] For identity theft claims, the Identity Theft and Assumption Deterrence Act of 1998 offers a more tailored means of prosecution and recovery.[248] Cases involving privacy infringement associated with mobile messaging can be addressed through the Wiretap Act.[249] Other claims related to improper access to voicemail or e-mail are covered under the Stored Communications Act.[250] Phishing cases involving mobile apps that steal bank account or credit card numbers are covered under the federal statute that governs access device fraud.[251] E-mail or other commercial advertisement spam claims that occur through mobile apps can be addressed through the CAN-SPAM Act.[252] Each of these statutes is highly tailored to specific types of conduct, and application to the mobile space does not require the same kind of creative interpretive techniques as under the CFAA.

From a normative perspective, criminal and civil liability under the CFAA makes sense for traditional hackers or fraudsters.[253] However,

---

245. 15 U.S.C. §§ 6501–05 (2006).

246. Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).

247. *See* Consent Decree & Order at 2–4, United States v. W3 Innovations, LLC, No. CV-11-03958-PSG, FTC File No. 102 3251 (N.D. Cal. Sept. 8, 2011), *available at* http://www.ftc.gov/os/caselist/1023251/110908w3order.pdf (settling charges under COPPA and the FTC's COPPA rule that the defendant illegally collected—via a mobile app—and disclosed personal information from tens of thousands of children under the age of thirteen without their parents' prior consent).

248. 18 U.S.C. § 1028 (2006). For example, § 1028(a)(7) makes it a federal crime to "knowingly transfer . . . or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, . . . any unlawful activity [that violates Federal, State, or local law]," where "means of communication" explicitly includes telecommunication identifying information. *Id.* § 1028(a)(7); *see also* The Identity Theft Penalty Enhancement Act, 18 U.S.C. § 1028A (2006) (imposing heightened penalties for aggravated identity theft when a defendant commits identify theft in relation to a variety of felony offenses).

249. 18 U.S.C. § 2511(1)(a)–(b) (2006).

250. 18 U.S.C. § 2701 (2006).

251. 18 U.S.C. § 1029 (2006).

252. 18 U.S.C. § 1037 (2006).

253. *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1265 (11th Cir. 2010) (affirming the conviction of a Social Security Administration teleservices agent who accessed the SSA database to obtain information about women in whom he was

when the end result is only slightly more targeted advertisements on a cell phone app to which some users take offense,[254] imposing criminal and civil liability does not comport with either the intent of the statute or sound public policy.

### *C. Proposed Amendments to the CFAA*

After sixteen years without substantive change and numerous conflicting judicial opinions, the CFAA is ripe for amendments aimed at limiting its scope and clarifying its ambiguities. Amidst growing concerns that the CFAA is overbroad and vague, the 112th Congress considered proposed amendments to the CFAA.[255] In September 2011, the Senate Judiciary Committee approved the Grassley/Franken Amendment to Senator Leahy's Personal Data Privacy and Security Act to change the definition of "exceeds authorized access" in § 1030(e)(6).[256] Specifically, the proposed amendment would strike the word "alter" and insert the following:

> alter, but 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.[257]

The Bono Mack amendment introduced as part of the SECURE IT Act mirrors this language verbatim.[258] These amendments appear to add much needed clarity to the "exceeds authorized access"

---

romantically interested, and then pursued those women through disquieting phone calls or unannounced home visits); United States v. Ivanov, 175 F. Supp. 2d 367, 373–75 (D. Conn. 2001) (denying a motion to dismiss filed by the defendant, a Russian hacker, who allegedly violated the CFAA by stealing network passwords and attempting to extort money from the company in exchange for making their network secure again).

254. *See In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *9–10 (N.D. Cal. Sept. 20, 2011) (describing allegations that defendants "exploit[ed]" purportedly personal information for "advertising and analytics purposes").

255. *See* Personal Data Privacy and Security Act, S. REP. NO. 112-91, at 10–12 (2011) (discussing the amendments proposed by Senator Grassley and Senator Leahy on September 15 and November 17, 2011, respectively). In addition, Representative Bono Mack introduced a similar bill in the United States House of Representatives. Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT Act of 2012), H.R. 4263, 112th Cong. (introduced Mar. 27, 2012 by Rep. Bono Mack).

256. *See* S. REP. NO. 112-91, at 11–12 (discussing the five proposed amendments to the Act as amended by the Senate Commission on the Judiciary).

257. *Id.* at 43.

258. *Compare* S. REP. NO. 112-90, at 10–12 (2011) (incorporating the Grassley amendment over the Leahy amendment), *with* SECURE IT Act of 2012, H.R. 4263, 112th Cong. (recommending identical language).

definition and essentially prevent the Department of Justice from pursuing the *Drew*-type litigation. By specifically excluding violations of written access agreements that form the sole basis for determining access, the amendments appear to solve the core overbreadth and vagueness issues that plague the contract-based approach by removing the possibility of criminalizing a breach of contract.[259] Moreover, these amendments take the power of determining the line for criminal liability away from drafters of often arbitrary or nonsensical terms of use policies. In other words, these small amendments remove the potential for prosecuting ordinary Internet usage as felonies.

In November 2011, Senator Leahy introduced a revised amendment that would rewrite § 1030(A)(2) by defining the specific types of information that would have to be obtained in excess of authorization in order to trigger liability.[260] Specifically, the amendment would create liability only when the offense "involves" certain types of personally identifiable information, including "government-issued identification numbers . . . trade secrets, commercial business information, or other similar information."[261] This amendment, though aimed at providing broader protections for personal data, does not seem to address the core issues of overbreadth and vagueness. The use of phrases such as "involve" and "other similar information" likely will not provide sufficient clarity and may lead to further confusion.[262] While limiting liability to only specific types of information may be a valid way of solving the frivolous prosecution problem, the Leahy amendment attempts to

259. *See Bill Tweaked in Senate: Terms of Service No Longer Terms of Felony*, CTR. FOR DEMOCRACY & TECH. (Sept. 16, 2011), http://www.cdt.org/blogs/joshua-gruenspecht/169senate-tweaks-bill-terms-service-no-longer-terms-felony (discussing how the revised bill would remove "contractual fine print . . . criminal liability," but noting that several senators suggested an alternate approach involving a revision of DOJ guidelines for such cases instead of a statutory fix).

260. *See supra* note 255 (discussing proposed bills in the House and the Senate). Senator Leahy's amendments were loosely based on a proposal by Professor Kerr articulated during House testimony. *See Cyber Security: Protecting America's New Frontier: Hearing before the H. Comm. on the Judiciary*, 112th Cong. 6–8 (Nov. 15, 2011) (testimony of Orin S. Kerr) (advocating for the Grassley/Franken amendment while also proposing an alternative, though more restricted, version of the Leahy amendment).

261. Orin Kerr, *My Assessment of Senator Leahy's Proposed Amendment to the CFAA*, VOLOKH CONSPIRACY (Nov. 22, 2011, 5:53 PM), http://volokh.com/2011/11/22/my-assessment-of-senator-leahys-proposed-amendment-to-the-cfaa/.

262. *See id.* (arguing that while the idea of limiting the type of liability-triggering information is "sensible," the Leahy amendment uses overly broad and ambiguous language that not only may raise more interpretive problems than it solves, but also that it fails to expressly prohibit the prosecution of *Drew*-type terms of service violations).

expand personal data protections to cover too many issues under one umbrella.[263]

The recent legislative activity surrounding the CFAA demonstrates, at least in part, congressional recognition that the decades-old anti-hacking statue is in need of a face-lift. Although the Leahy amendment arguably raises more problems than it solves, it represents a step in the right direction towards limiting the scope of arguably vague provisions.

## CONCLUSION

The CFAA has broken free of its moorings as an anti-hacking law and now sits on the precipice of becoming an oppressively broad statute when applied to mobile app cases. Application of the contract- and agency-based approaches raises vagueness concerns involving both fair notice and the potential for arbitrary and discriminatory enforcement. Concurrently, the under-inclusive code-based approach blurs the CFAA's clear distinction between insider and outsider liability. Accordingly, courts should limit "without authorization" liability to traditional hacking cases to promote the original intent of the statute, while "exceeds authorized access" claims should be similarly limited to instances of serious misuse of information. Moreover, absent congressional or judicial clarification, specific problems such as children's privacy, identity theft, or mobile messaging are better addressed through more highly-targeted and narrowly-tailored statutes.

Despite the uncertainty surrounding the scope of unauthorized access, lawmakers and regulators continue to propose CFAA amendments to impose increasingly harsh penalties.[264] Raising penalties, including making it easier for law enforcement to bring felony charges, without first addressing the underlying vagueness concerns and definitional ambiguities, is a recipe for arbitrary enforcement.[265] Even as these proposals percolate through Congress,

---

263. *See id.* (discussing how the inclusion of "trade secrets" in the Leahy amendment has the potential to circumvent the intent requirement for trade secret theft liability under 18 U.S.C. § 1832).

264. *See* Personal Data Privacy and Security Act, S. REP. NO. 112-91, at 13–14 (2011) (proposing harsher penalties for specific crimes, such as password-trafficking, but also attempting to carve out a prosecutorial exemption for violations of website terms of service agreements that form the sole basis of an unauthorized access claim).

265. *See* Remarks of Orin Kerr, Federalist Society Cybersecurity Symposium (June 28, 2011), *available at* http://volokh.com/2011/07/05/federalist-society-symposium-on-cybersecurity/ (criticizing proposed CFAA amendments as opening a Pandora's box for law enforcement to bring unauthorized access cases on a whim).

several lawmakers have recognized the problems inherent in applying the current state of the CFAA to mobile applications.[266]

As mobile apps present new challenges of data privacy for end-users, app developers, and law enforcement, courts can adopt a narrower interpretation of unauthorized access limited to instances of hacking or serious misuse of user-data until Congress offers more highly tailored legislation. In the interim, causes of action against mobile app developers and advertisers should fail under any current interpretation of "without authorization" or "exceeds authorized access" absent evidence of hacking or serious information misuse. By limiting the scope of CFAA liability through narrow interpretations, courts can avoid vagueness concerns and potentially limitless liability for the mobile data field.

266. *See* Letter from United States Sens. Al Franken and Richard Blumenthal to Assistant Att'y Gen. Breuer (Apr. 12, 2011), *available at* http://franken.senate.gov/files/letter/041112_Franken_Blumenthal_Letter_AG_Breuer_CFAA.pdf ("Because many smartphone apps lack privacy policies, many of the applications being investigated by the U.S. Attorney General's Office may fall into this legal gray area.").