"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

Nicholas R. Johnson[*]

I. INTRODUCTION

Imagine for a second that you are in law school. Your Professional Responsibility class is wearing on, and you cannot resist the temptation to use your laptop to log on to Facebook and update your user profile. Knowing that some employers use Facebook as a means to screen potential employees,[1] and knowing that taller, good-looking people are statistically likely to earn more money than shorter, less attractive people,[2] you decide to do some fudging: You describe yourself on your Facebook profile as "5'9", blue-eyed, and devastatingly handsome," despite the fact that you are really 5'4", brown-eyed, and showing distressingly early signs of male pattern baldness. For emphasis you upload a picture of a young Paul Newman that you found elsewhere on the Internet. Facebook's terms of use prohibit such white lies,[3] but you take little notice. Satisfied, you save your changes and return to the class discussion of ABA Model Rule 4.1. Have you just committed a federal crime?

As a matter of intuition, most people would say "no." But Lori Drew, the Missouri woman accused of creating a fake MySpace profile in order to "cyberbully" her daughter's former friend, might answer differently. Drew—

[*] J.D., University of Illinois College of Law, 2010; B.S., Northwestern University, 2005. I am indebted to William Breedlove and Carol Hayes of the Journal of Law, Technology & Policy for their critical assistance in seeing this piece through to publication. Thanks especially to my parents, whose love and guidance have helped me take every step on this long path toward a fulfilling legal career.

[1] Amy S. Clark, *Employers Look at Facebook, Too*, June 20, 2006, CBS NEWS, http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml.

[2] Martin Wolk, *Better Wealthy Than Handsome? Why Not Both?*, Apr. 7, 2005, MSNBC, HTTP://www.msnbc.msn.com/id/7420983/.

[3] *See* Facebook, *Statement of Rights and Responsibilities*, http://www.facebook.com/terms.php?ref=pf(last visited Mar. 10, 2009) ("You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission . . . You will not post content or take any action on Facebook that infringes or violates someone else's rights. . . If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.").

apparently in an effort to determine whether the friend, Megan Meier, had been spreading malicious rumors about her daughter—masqueraded on MySpace as "Josh Evans," an attractive boy who initially professed an interest in Megan. However, after being spurned by "Josh," Megan—who had a history of depression—committed suicide, and federal prosecutors charged Lori Drew under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq.

Certainly, there is nothing noble about Lori Drew's conduct, but her prosecution should raise the hackles of anyone who uses an online networking site such as Facebook or MySpace, or who even has clicked "I agree" to a website's terms of service without reading it. The government's extraordinarily broad theory of liability in the Drew case has the potential to criminalize the everyday conduct of millions of Internet users—a result that Congress surely could not have intended when it passed the Computer Fraud and Abuse Act in 1984 as an anti-hacking provision.

In Part II, this Recent Development will outline the facts of Lori Drew case, examine the Computer Fraud and Abuse Act and the intent of the legislators who passed it, and describe the ways in which computer users can protect private information they store on their websites. Part III will explore how courts have interpreted the meaning of access "without authorization" to a protected computer, making note of the fact that no court has ever held in a CFAA criminal case that violation of a public website's terms of service constitutes "unauthorized access." Finally, Part IV urges courts to reject a contract-based theory of liability under the CFAA, arguing instead that the adoption of a "code-based" standard to define the scope of "unauthorized access" is consistent with Congress's intent in passing the CFAA, as well as basic notions of due process and statutory construction.

II. BACKGROUND

A. The Facts of the Lori Drew Case

In 2005, Megan Meier, then a 13-year-old seventh-grader from Dardenne Prairie, Missouri, established an on-again, off-again friendship with Lori Drew's daughter. Tina Meier, Megan's mother, described Megan's transition into seventh grade as "a mess," and noted that her daughter was sensitive about her weight and "[tried] desperately to fit in."[4] Megan and Lori Drew's daughter would go on "jags of companionship," but eventually ended their friendship.[5]

In September 2006, Megan's parents allowed her to sign up for a MySpace account,[6] despite the fact that, at age 13, she was technically too

[4] Lauren Collins, *Friend Game*, THE NEW YORKER, Jan 21, 2008, *available at* http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_collins.

[5] *Id.*

[6] MySpace is an online social networking site—a Web-based community that allows its users to create a "profile" that serves as a virtual representation of themselves to the rest of the MySpace community. Once a member has established a profile—which typically includes a picture and a list of personal interests—

young to have one.[7] And shortly thereafter, Megan received a friendship request from "Josh Evans," a muscular, attractive 16-year-old boy with blue eyes and wavy brown hair.[8] What Megan did not know when she accepted Josh's friend request was that he was a fictional character—one allegedly created by Lori Drew in an effort to determine whether Megan had been spreading malicious rumors about Drew's daughter.[9] Megan and Josh sent messages back and forth for 29 days, and "[f]or 28 of those days, nothing negative was communicated."[10] However, the relationship between Megan and Josh deteriorated rapidly on October 16, 2005, when an "insult war" broke out.[11] The conversation ended "in substance, that the world would be a better place without [Megan] in it."[12] Shortly after that argument, Megan committed suicide.

B. The Indictment

After Megan's suicide, the state of Missouri examined the possibility of pressing criminal charges but ultimately determined that the facts of the case were not legally sufficient to charge Drew with harassment, stalking or child endangerment.[13] However, in May 2008, federal prosecutors in Los Angeles, California[14]charged Lori Drew with three felony counts of "accessing protected computers without authorization to obtain information" under 18 U.S.C. § 1030(a)(2)(C) and § 1030(c)(B)(ii) of the Computer Fraud and Abuse Act ("CFAA").[15]

The prosecution's theory of liability under the CFAA was as follows:

she may extend "friendship" invitations to other MySpace users and then communicate with them through a variety of media, such as e-mail and private instant messaging.

[7] At the time, MySpace's Terms of Use required users to be at least 14 years old. MySpace.com Terms of Use, July 15, 2006, *available at* http://web.archive.org/web/20060914024244/www.myspace.com/Modules/Common/Pages/TermsConditions.aspx, at 1. Currently, the Terms of Use allow users to be 13 years or older. MySpace.com Terms of Use, June 25, 2009, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Mar. 10, 2009) [hereinafter *MySpace Terms*].

[8] Collins, *supra* note 4.

[9] Why the Josh Evans profile was established—and who retained ultimate control of it—is not clear. Ashley Grills, then an 18-year-old-employee of the Drew family, testified at trial that she came up with the idea of creating a fake MySpace profile, but that Lori Drew agreed with the plan and "thought it was funny." Scott Glover, *Mother Saw Plan as Clever, Witnesses Say,* L.A. TIMES, Nov. 21, 2008, at B4.

[10] Drew Mot. to Dismiss for Failure to State an Offense at 3, n.2, United States v. Drew, No. CR-08-582-GW (C.D. Cal. July 23, 2008) [hereinafter "*Motion to Dismiss"*], available at http://online.wsj.com/public/resources/documents/drewfailuretostateoffense.pdf.

[11] Collins, *supra* note 4.

[12] Indictment at 8, United States v. Drew, No. CR-08-582-GW (C.D. Cal. Feb. 2008) [hereinafter "*Drew Indictment*"], *available at* http://blog.wired.com/27bstroke6/files/my_space_lori_drew_ indictment.pdf. Ron Meier, Megan's father, told a reporter that the exact statement from Josh was "you're a shitty person and the world would be a better place without you in it." Collins, *supra* note 4.

[13] Joel Currier & David Hunn, *Neighbor's Story Emerges in Suicide; Prosecutor Finds Insufficient Evidence to Charge Anyone in MySpace Case,* ST. LOUIS POST DISPATCH, Dec. 4, 2007, at A1.

[14] Personal jurisdiction existed in Los Angeles because MySpace's central servers—which house all content on MySpace, and which Lori Drew allegedly "accessed" by registering a MySpace account—are located in Beverly Hills, California.

[15] Scott Glover & P.J. Huffstutter, *Cyber Bully Fraud Charges Filed in L.A.; Woman is Accused of Creating a MySpace Persona Whose Comments May Be Linked to Girl's Suicide,* L.A. TIMES, May 16, 2008, at B1.

Section 1030(a)(2)(C) prohibits obtaining information from a "protected computer" by means of intentional, unauthorized access.[16] Use of the MySpace website is governed by its Terms of Use, which constitute a contract between MySpace and its users.[17]Those Terms of Use requires that users, *inter alia*, "provide truthful and accurate registration information" and "refrain from using any information obtained from MySpace services to harass, abuse, or harm other people."[18] Because Lori Drew's conduct violated MySpace's user contract, Drew therefore acted either without authorization or in excess of authorized access when she communicated with Megan Meier through MySpace's protected servers.[19] Unauthorized access under §1030(a)(2)(C) is generally a misdemeanor, but it becomes a felony if committed in furtherance of an intentional tortious act (here, intentional infliction of emotional distress).[20]

C. Conviction

On November 26, 2008, a jury in Los Angeles convicted Lori Drew of three misdemeanor counts of computer fraud under the CFAA.[21] Though the jury rejected the prosecution's theory that Drew intended to harm Megan Meier through her messages on MySpace—a necessary element of the felony charges—they did conclude that she had exceeded her authorized access to MySpace's servers by establishing a false profile in violation of the site's Terms of Service.[22] Importantly, a not-guilty verdict on the felony counts meant that the case was no longer about "cyberbullying." Instead, the post-verdict issue became "whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of the CFAA."[23]

[16] *See* 18 U.S.C. § 1030(a)(2)(C) (2006) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains. . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.").

[17] *See MySpace Terms, supra* note 7 ("This Terms of Use Agreement . . . sets forth the legally binding terms for your use of MySpace services. By using the MySpace services, you agree to be bound by this agreement . . . . You are only authorized to use the MySpace services (regardless of whether your access or use is intended) if you agree to abide by . . . the terms of this Agreement.").

[18] *Drew Indictment, supra* note 12, at 5. *See also MySpace Terms, supra* note 7, at 1, stipulating the terms for eligibility: "[b]y using the MySpace services, you represent that . . . all registration information you submit is truthful and accurate. . . .", and at 8, defining prohibited content/activity: "[p]rohibited activity includes . . . using any information obtained from MySpace services to harass, harm, or abuse another person . . . . ").

[19] *Drew Indictment*, *supra* note 12, at 9–10.

[20] *See* 18 U.S.C. § 1030(c)(2)(B)(ii) (noting that any offense committed under § 1030(a)(2) becomes a felony punishable by a prison term of no more than 5 years if it was committed "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State").

[21] Jennifer Steinhauer, *Woman Found Guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 27, 2008, at A25.

[22] *Id.*

[23] Decision on Defendant's F.R. Crim.P. 29(c) Motion, United States v. Drew, No. CR 08-0582-GW, slip op. at 2 (C.D. Cal. Aug. 28, 2009) [hereinafter *Drew Decision*].

D. Post-Verdict Dismissal

On July 2, 2009, U.S. District Judge George H. Wu dismissed the case on a post-verdict motion, noting in his verbal ruling that if Drew's conviction were to stand, anyone who violated the MySpace Terms of Service could potentially be convicted of a crime.[24] In a subsequent 32-page written opinion, Judge Wu framed the "pivotal issue" in the Drew case as whether a "conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine."[25]The court answered that question in the affirmative, holding:

> If any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[26]

As a threshold matter, Judge Wu noted that online terms of service can, "like any other contract, define the limits of authorized access as to a website and its concomitant computer/server(s)."[27] But the court then held the government's application of § 1030(a)(2)(C) to be void for vagueness, noting that the statute did not give sufficient notice to Internet users that breach of a website's terms of service, standing alone, could constitute a crime.[28]

The court gave three primary reasons for its decision: First, it noted that while Internet users might expect civil contract enforcement actions for intentional violations of online contracts, they would not expect criminal penalties—especially because MySpace offers its services to users free of charge and therefore runs no risk of being monetarily "defrauded" by its users.[29]

Second, the court reasoned that the government's theory of liability made the website owner the party who defines the criminal conduct at issue, thereby leading to further vagueness issues. For example, MySpace's Terms of Service prohibits its users from posting "sexually suggestive" or "unfair" imagery on their profiles.[30] Those terms, noted the court, were vague and gave website owners the opportunity to apply and enforce their own terms based on

[24] Alexandra Zavis, *Judge Tentatively Dismisses Case in MySpace Hoax That Led to Teenage Girl's Suicide*, L.A. TIMES, Jul. 2, 2009, http://latimesblogs.latimes.com/lanow/2009/07/myspace-sentencing.html. At an earlier hearing on the motion to dismiss, Judge Wu grilled Assistant U.S. Attorney Mark Krause on the implications of the State's theory of liability, asking, "Is a misdemeanor committed by the conduct which is done every single day by millions and millions of people? If these people do read [the Terms of Service] and still say they're 40 when they're 45, is that still a misdemeanor?" *Id.*

[25] *Drew Decision*, *supra* note 23, at 25.

[26] *Id.* at 32.

[27] *Id.* at 25.

[28] The court, citing to *United States v. Lanier,* 520 U.S. 259 (1997), and *Kolender v. Lawson*, 461 U.S. 352 (1983), held that the void-for-vagueness doctrine has "two prongs: 1). A definitional/notice sufficiency requirement, and, more importantly, 2). a guideline-setting element to govern law enforcement." *Drew Decision*, *supra* note 23, at 23. The court proceeded to analyze the void-for-vagueness doctrine under both prongs of this test.

[29] *Id.* at 25–26.

[30] *Id.* at 27.

ad hoc decisions and undelineated standards.

Third, and perhaps most importantly, the court ruled that if a website's terms of service could alone determine what was "unauthorized" (and therefore criminal) under § 1030(a)(2)(C), the statute would be unacceptably vague because it does not specify *which* violations will render access unauthorized.[31] The MySpace Terms of Service, noted the court, prohibit a wide range of user conduct, from "criminal and tortious activity" to "covering or obscuring the banner advertisements on your profile page."[32] The court noted that stating *any* terms of service violation to constitute unauthorized access would resolve this particular vagueness issue, but "would, in turn, render the statute incredibly overbroad . . . ."[33]

The overbreadth concern also led the court to rule that the government's application of § 1030(a)(2)(C) to violations of a website's terms of service was void for vagueness because it failed to establish " 'clear guidelines' or 'objective criteria' as to the prohibited conduct in the Internet/website or similar contexts."[34] Specifically, the court noted that the language of § 1030(a)(2)(C) was not limited only to cases in which a website owner complains to law enforcement about a terms of service breach, or cases in which the unauthorized access caused loss or damage, or violated privacy interests.[35] Simply holding that every intentional breach of a terms of service constituted unauthorized access, concluded the court, would result in a "standardless sweep" that would leave federal law enforcement officials "improperly free 'to pursue their personal predilections.' "[36]

This Recent Development will argue that Judge Wu's decision to dismiss the case was correct, and that, absent explicit Congressional direction to the contrary, courts should interpret the Computer Fraud and Abuse Act narrowly to avoid criminalizing the everyday behavior of millions of Internet users. However, it will also expand upon a point that Judge Wu's ruling barely touched upon: The idea that § 1030(a)(2)(C) was enacted primarily to protect information on private computer networks.[37] As we will see, the idea of privacy protection runs as a theme throughout the legislative history of § 1030(a)(2). The CFAA was enacted before there were any public computer networks, and though Congress has expanded the CFAA's reach over the past 25 years, not once has it implied that the statute was meant to apply to obtaining information from publicly available websites, though it has had ample opportunity to do so. This idea of privacy requires us to examine the public/private dichotomy in the (very public) world of the Internet today, and

[31] *Id.* at 26.

[32] *Id.*

[33] *Id.*

[34] *Id.* at 30.

[35] *Id*.

[36] *Id.* at 31–32.

[37] In its ruling, the court noted that its conclusion that a website's terms of service, standing alone, was not sufficient to constitute unauthorized access under § 2030(a)(2)(c) was "especially the case with MySpace and similar internet venues which are publically [sic] available for access and use." *Id.* at 31. The court elaborated no further.

examine the measures that computer users may take to protect private information on their computers and websites.

E. The Computer Fraud and Abuse Act

1. Background

The Computer Fraud and Abuse Act, originally passed in 1984 as part of the Comprehensive Crime Control Act of 1984, was intended to address, in a single federal statute, the then-novel and growing problem of computer crime.[38] At its core, the Act is intended to protect the "confidentiality, integrity, and security of computer data and networks" by prohibiting misuse of a computer and providing civil and criminal sanctions for knowing or intentional violations.[39] At the time the Act was passed, computers, though not yet widely used for personal purposes, had already become an integral part of the national defense and finance sectors. The statute therefore applied only to certain non-public computers—those that contained private financial data or national security information, or those that were under government operation.[40] Hackers, naturally interested in the information that banks and governments kept behind their new computerized walls, quickly found surreptitious ways to satisfy their curiosity.[41]

Over the years, Congress has subsequently expanded the CFAA to respond to new types of computer crime. The Act currently contains seven criminal provisions, each designed to guard against a specific misuse of a computer or data network. Specifically, the Act provides criminal penalties for anyone who, without authorization to do so, (1) knowingly obtains classified national security information;[42] (2) compromises the confidentiality of data by obtaining information from a protected computer;[43] (3) intentionally trespasses in a government or federal interest computer;[44] (4) knowingly accesses a protected computer with intent to defraud and thereby obtains something of value;[45] (5) causes damage to a computer, either by the knowing transmission of code or by intentional trespass;[46] (6) "knowingly and with intent to defraud trafficks" in computer passwords;[47] or (7) with intent to extort money or

[38] *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473. 98 Stat. 2190, reprinted in 1984 U.S.C.C.A.N. 3689, 3691–97 (discussing the growing problem of computer crime and explaining the inadequacies of current wire and mail fraud statutes in prosecuting such activity).

[39] S. Rep. 104–357 at * 3 (1996).

[40] Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2255 (2004).

[41] *See* Pub. L. No. 98–473, reprinted in 1984 U.S.C.C.A.N. 3689, 3694 (citing an ABA report that estimated annual losses due to computer crime of $145 million to $730 million).

[42] 18 U.S.C. § 1030(a)(1) (2008); U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, PROSECUTING COMPUTER CRIMES 10–11 (Scott Eltringham ed., 2007), http://www.usdoj.gov/criminal/cybercrime/ccmanual/ccmanual.pdf [hereinafter PROSECUTING COMPUTER CRIMES].

[43] 18 U.S.C. § 1030(a)(2); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 15–17.

[44] 18 U.S.C. § 1030(a)(3); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 19–21.

[45] 18 U.S.C. § 1030(a)(4); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 22–24.

[46] 18 U.S.C. § 1030(a)(5); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 29–32.

[47] 18 U.S.C. § 1030(a)(6); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 46–48.

something else of value, threatens to damage a protected computer.[48] In addition, Congress in 1994 added a civil provision to the Act which allows certain victims of computer abuse to bring a claim against the perpetrator if economic losses as a result of the damage total $5,000 or more during any one-year period.[49]

2. *Section § 1030(a)(2)(C)*

When § 1030(a)(2)(C) was added to the CFAA in 1996, Congress stated rather succinctly: "The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. This information, stored electronically, is intangible, and it has been held that the theft of such information cannot be charged under more traditional criminal statutes. . . ."[50] Section 1030(a)(2)(C) is therefore essentially a theft provision—it punishes people who steal private and confidential information stored on computers.[51]

Courts have read this language as incorporating three elements that the government must prove: (1) that the defendant intentionally accessed a computer, (2) that the access was without authorization or in excess of authorized access, and (3) that the defendant obtained information from a protected computer.[52] "Protected computer" has been construed to mean any sort of computer at all,[53] and courts have also made clear that this section requires only the mens rea to access without authorization—no further showing of intent is required.[54] Further, § 1030(a)(2)(C) is a subsection of § 1030(a)(2), and therefore must be read within the context of that section.[55] Congress has noted that "the premise of [1030(a)(2)] is privacy protection."[56]

[48] 18 U.S.C. § 1030(a)(7); PROSECUTING COMPUTER CRIMES, *supra* note 42, at 49–50.

[49] 18 U.S.C. § 1030(g) (2008); S. REP. NO. 104–357, at 14 (1996).

[50] S. REP. NO. 104–357, at 7 (1996).

[51] *See id.* at 7–8 (noting that the the "crux of the offense [under §1030(a)(2)(C)]" is "abuse of the computer to obtain [intangible] information.").

[52] United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007).

[53] *E.g.,* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2003) (holding that a processing chip in an emergency response system constituted a "protected computer" for purposes of the CFAA). *See also* Bellia, *supra* note 40, at 2167 (noting that the term "protected computer" likely includes any computer connected to the Internet). As enacted in 1996, 18 U.S.C. § 1030(a)(2)(C) prohibited obtaining information from "any protected computer *if the conduct involved an interstate or foreign communication.*" However, the 2008 amendments to the Act eliminated this jurisdictional requirement. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110–326, 122 Stat. 3560, Title II, § 203.

[54] *See, e.g., Willis,* 476 F.3d at 1126 (rejecting defendant's argument that § 1030(a)(2)(C) requires a further intent to defraud, or even proof that the defendant knew the value of any information obtained)*;* Shamrock Foods v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (quoting *Brett Senior & Assocs., P.C. v. Fitzgerald,* 2007 U.S. Dist. LEXIS 50833, at *3 (E.D. Pa. July 13, 2007)) (noting that "the plain language of *1030(a)(2)* . . . targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation."). However, the legislative history of the CFAA makes it clear that specific intent to access without authorization is required, as "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the [Senate Judiciary] Committee intends to proscribe." S. REP. NO. 99–432, at 6 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2483.

[55] 18 U.S.C. § 1030(a)(2) (2008).

[56] S. Rep. No. 104–357, at *7 (1996). Specifically, § 1030(a)(2)(A) prohibits the theft of financial information; § 1030(a)(2)(B) prohibits the theft of information "from any department or agency of the United States."

This is certainly in part why Congress defined its terms so broadly in § 1030(a)(2). For example, Congress made clear that "information" obtained from a computer meant not only physical objects, like disks or hardware, but also information stored in "intangible form."[57] Further, Congress intended the term "obtaining information" to apply to a computer user who merely reads or views information—there is no requirement that the user copy, download, or otherwise alter the data contained on the protected computer.[58] Congress noted that this rationale was "critically important because, in an electronic environment, information can be 'stolen' without asportation."[59]

Section 1030(a)(2)(C)'s focus on "privacy protection" leads to two important conclusions. First, it explains the presence of the terms "without authorization" and "exceeds authorized access" in the Act; [60] after all, everyone by definition is "authorized" to view information that is not private. Second, it implies that a computer user must take certain measures in order to make the information on her computer private. The question, then, is what measures the CFAA's definition of privacy contemplates.

F. Protection of "Private" Information

The history of the CFAA must be read in conjunction with the development of computer technology. When Congress passed the original CFAA in 1984, there were no computer networks available to the general public. Rudimentary examples existed outside of the governmental and financial sectors, but they were confined to academia and other private institutions.[61] The World Wide Web was not established until 1991, and did not burgeon until the mid-1990s, when Internet service providers such as AOL, Prodigy, and CompuServe began offering service to members of the public.[62] However, unlike the private networks from which public websites originated, the new concept of "cyberspace" was thought to be very public—the "modern equivalent of the Western Frontier," where users could roam freely without limitations.[63]

In other words, the advent of the World Wide Web gradually flipped computer users' expectations of privacy on computer networks. In 1984, when the CFAA was passed, all computer networks were thought to be private (inaccessible unless one was given a right of access). Today, the computer network that the vast majority of us use—the Internet—is thought to be public (accessible unless one is denied a right of access).

[57] *Id.*

[58] *Id.*

[59] *Id.* at *8.

[60] 18 U.S.C. § 1030(a)-(e) (2008).

[61] For example, BITNET (Because It's Time Network) connected IBM mainframes around the educational community and the world to provide mail services beginning in 1981. Walt Howe, A Brief History of the Internet, http://www.walthowe.com/navnet/history.html (last visited Mar. 12, 2009).

[62] *Id.*

[63] Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 442–43 (2003). *See also* Lawrence Lessig, *The Death of Cyberspace*, 57 WASH. & LEE L. REV. 337, 344 (2000) (describing how the Internet developed largely in ignorance of basic property norms).

But just as on the Western Frontier, computer users soon began to stake claims to cyber-territory, reinvigorating the idea of private space on computer networks.[64] The question, then, is how users on the world's biggest computer network can create private space in order to protect the information stored on their computers from outsiders. Some legal scholars have suggested two different methods: code-based protections and contract-based protections.

1. Code v. Contract-Based Protection

Code-based protection is, in essence, technical barriers to access that the computer owner programs by code into the computer software.[65] Typical code-based "gatekeepers" include password protection, or a routing system that directs every would-be user to a main login page.[66] The privacy advantages of code-based protection are twofold. First, it puts exclusionary control of the site in the hands of the computer owner (she may set password access and then assign passwords to users as she deems appropriate).[67] Second, the computer itself, through the technical measures imposed by the owner, takes affirmative steps to control access by excluding members of the public who do not meet the site's coded access criteria. Importantly, technical code-based protection measures "actually have to control access to some degree," as opposed to indicating the permissible limits of access to a computer or website.[68] In other words, code-based protection is the digital equivalent of a locked safe—a physical barrier around information that the user intends to keep private.

In comparison, a computer owner may control access by contract: She posts terms and conditions to which a user must agree before he is "permitted" to use the computer or the website.[69] Common examples are a "terms of use" statement on or linked from the main page of a website, or a "click-through" agreement that stipulates terms to which the prospective user must affirmatively agree before she is granted access.[70] However, unlike code-based protection, contract-based protection is not coded into the computer system. Instead, contract-based protection works "on the honor system, or perhaps more accurately, the honor system backed by contract law remedies."[71]

Because of these distinctions, some commentators view code-based measures as a "strong" method of protecting computerized information—one that may even trigger Fourth Amendment protection.[72] The reasoning is

[64] Hunter, *supra* note 63, at 443.

[65] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. Rev. 1596, 1644 (2003).

[66] Bellia, *supra* note 40, at 2212.

[67] *See* Kerr, *supra* note 65, at 1644 (noting that code-based restrictions allow the computer owner to "require every user to have an account with a unique password, and can assign privileges based on the particular account, limiting where the user can go and what she can do . . . .").

[68] Bellia, *supra* note 40, at 2212.

[69] *Id.; see also* Kerr, *supra* note 65, at 1645.

[70] Kerr, *supra* note 65, at 1645.

[71] *Id*.

[72] *See, e.g.,* Michael Froomkin, *The Metaphor is the Key: Crytography, the Clipper Chip, and the*

simple: if an unauthorized user wishes to gain access to a website protected by code, she either must steal the password or attempt to guess it—a process of "safecracking" that could theoretically occupy "millions of years."[73]

No such affirmative protection exists with regulation of websites by contract. A user may have no intent to obey a term of use that says, "This site is private, and access is conditioned upon your agreement to not reveal any information contained herein," yet she may still be granted access to the website if she clicks "I agree." The important point for purposes of the Lori Drew prosecution is that code-based measures are far more effective at protecting private information than regulation by contract, and Drew was charged under § 1030(a)(2)(C)—the provision of the CFAA that prohibits theft of private and confidential information stored on computers. The question, then, is the type of protection measures, if any, on the MySpace website.

2. MySpace—Regulation by Code or by Contract?

An examination of the MySpace site makes clear that it is a public website regulated by contract, not a private website regulated by code. Setting up a user profile requires becoming a member of MySpace, which requires affirmatively clicking "I agree" to MySpace's Terms of Service—clear contractual protection.[74] Certain features of the site, such as the registration page at issue in the Drew case, require a login ID and password and therefore may initially appear to be code-based protection—but they are not. That is because MySpace's methods of access—even the password and ID system—place no physical controls on access to the site. When a new user registers, she inputs a name and a valid e-mail address, and then she—not MySpace—chooses her own ID and password to the MySpace site before she affirmatively clicks the "I agree" button. In real-world terms, this is somewhat akin to a bank letting customers mint their own key to the safe when they sign up for a checking account. The practical effect of such a system is that anybody at all—Lori Drew, "Josh Evans," or Grendel, the monster from *Beowulf* [75]—can establish a MySpace profile.

In fact, MySpace explicitly acknowledges that the content on its site is

Constitution, 143 U. PA. L. REV. 709, 871 (1995) (analogizing coded encryption measures to use of a safe to protect private contents, thereby triggering a reasonable expectation of privacy in those contents). *But see* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 516 (2001) (arguing that, for Fourth Amendment purposes, a computer user has no reasonable expectation of privacy in encrypted e-mails). This Recent Development takes no position on whether code-based protection triggers protection from unreasonable government searches and seizures under the Fourth Amendment, which is a different question than whether code-based protection effectively excludes most members of the public from private information on websites. Instead, it is sufficient to agree with Professor Kerr when he writes that, from a practical perspective, "the privacy regime that protects Internet communications extends strong privacy protections even if [code-based] protection itself does not trigger the Fourth Amendment." *Id.* at 529.

[73] Kerr, *supra* note 72, at 504.

[74] Signup For MySpace, http://signups.myspace.com/index.cfm?fuseaction=signupy (last visited Sept. 29, 2009).

[75] MySpace Profile of Grendel, http://profile.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=5272436 (last visited Sept. 29, 2009).

not private, despite its password access system. The very first piece of advice on MySpace's safety page is this: "Don't forget that your profile and MySpace forums are public spaces. Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen names, or specific whereabouts)."[76] In other words, protecting personal information is up to the user, not MySpace.[77] Such a system is not code-based protection.[78]As one commentator has noted, "[w]hen a system is technically configured to allow particular uses, the default presumption should be that the system owner consents to the allowed use because the system owner is in a better position to convey limits [on use] . . . ."[79] Lori Drew may have violated a contract term to gain access to MySpace, but the system is "technically configured" to allow her use—as well as the use of 246 million others.

With this code-based versus contract-based dichotomy in mind, this Recent Development will now address judicial interpretations of the term "without authorization" under the CFAA. While some courts have held in a civil context that violation of a website's terms of use can constitute "unauthorized access," none have done so in a criminal case. And equally importantly, all *criminal* prosecutions under § 1030(a)(2)(C) have involved circumvention of code-based protective measures.

III. ANALYSIS

A. "Without Authorization" and "Exceeds Authorized Access" – Definitions

As one commentator has noted, "the crucial question in applying [the CFAA] to a [computer] owner's efforts to curtail unwanted uses of her system is what it means for access of a system to be 'without authorization,"[80] yet the true meaning of that term has proven to be frustratingly elusive. Congress, "perhaps assuming that the words speak for themselves," did not define the term "without authorization."[81] But the CFAA explicitly defines "exceeds authorized access" as "[accessing] a computer with authorization and to use such access to obtain or alter information that the accesser is not so entitled to

[76] MySpace Safety Tips and Settings, http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips (last visited Nov. 8, 2009).

[77] In fact, courts have rejected the idea that MySpace has any affirmative duty to confirm the age or personal information submitted to its website. *See, e.g.*, Doe v. MySpace, 474 F. Supp. 2d 843, 851 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008) (rejecting plaintiffs' claim that MySpace had a duty to enact safety measures to protect underage users from sexual predators).

[78] Kerr, *supra* note 65, at 1646 ("[A] computer owner could set up a website that appears to require a username and password to access the contents of the site, but that actually grants access for any username and password combination. Such a site would appear to a user to regulate by code, but would actually work more like a system of regulation by contract."). *Cf.* Snow v. DirecTV, 450 F.3d 1314, 1322 (11th Cir. 2006) (defendant's website was "readily accessible" to the general public despite password protection, because gaining access to the site required only registering, creating a password, and agreeing to the terms of use).

[79] Bellia, *supra* note 40, at 2248.

[80] *Id.* at 2234.

[81] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n. 10 (1st Cir. 2001).

obtain or alter."[82] It is also clear that the CFAA contemplates a distinction between "insiders" and "outsiders": Specifically, outsiders are those who access a computer "without authorization," and insiders are those who have some authorized access to a computer but then "exceed" it in some way.[83]

Yet courts and commentators alike have had difficulty keeping the terms "without authorization" and "exceeds authorized access" separate.[84] Indeed, at Lori Drew's trial, the prosecution did not explicitly argue that Drew's access was one or the other, instead apparently proceeding upon both theories at once.[85] Given the lack of statutory guidance on the meaning of "without authorization," courts have defined the term in various ways. Many of them apply the plain meaning of the word "authorization," turning to dictionaries for reference.[86] Some courts cite to *United States v. Morris*,[87] which holds that a user who has some authorization to use a computer may nonetheless act "without authorization" if she uses the computer in a manner that is not related to the computer's intended function.[88] Later courts have explained that the scope of a user's authorization under the *Morris* "intended function" test hinges upon "the nature of the relationship established by the computer owner and the user."[89]

Finally, courts have held that a violation of a contract can constitute "unauthorized access" under the CFAA. This is the government's theory of liability in the Lori Drew case, so it is worth exploring in depth some of these decisions. Notably, while courts have applied the *Morris* "intended function"

[82] 18 U.S.C. § 1030(e)(6) (2008).

[83] *See* S. REP. NO. 104–357, at 11 (1996) (describing differing circumstances in which insiders and outsiders would face criminal liability under the CFAA).

[84] *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (Posner, J.) (noting that the difference between "without authorization" and "exceeds authorized access" is "paper thin . . . but not quite invisible."); Kerr, *supra* note 65, at 1630 ("Although courts have struggled to distinguish between these two phrases, prohibitions against exceeding authorization appear to reflect concerns that users with some rights to access a computer network could otherwise use those limited rights as an absolute defense to further computer misuse.").

[85] *See Drew Indictment*, *supra* note 12, at 5, 9 (using the phrase "without authorization and in excess of authorized access" consistently throughout).

[86] *See, e.g.*, Healthcare Advocates v. Harding, Earley, Follmer, & Frailey, 497 F. Supp. 2d 627, 644, 648 (E.D. Pa. 2007) (noting that Congress did not define the term "authorization" in the CFAA and therefore using a dictionary to ascertain the "plain meaning" of the word). In the Drew trial, Judge Wu instructed the jury that "access without authorization" means "to access a computer without the approval, permission, or sanction of the computer's owner." Government's Resp. to Def.'s Supplement to Rule 29 Mot. at 4, United States v. Drew, No. 08-582-GW (C.D. Cal. Dec. 30, 2008) ("*Government's Response"*), *available at* The Volokh Conspiracy, http://volokh.com/files/DrewResponse.pdf.

[87] 928 F.2d 504 (2d Cir. 1991).

[88] *Id.* at 510. In 1988, Robert Tappan Morris was given access to a computer at Cornell University that connected to the INTERNET, which was then a private nationwide network of federal interest, military, and university computers. *Id.* at 505. Seeking to expose security flaws on that network, Morris released a virus that ended up causing substantial damage. *Id.* at 506. Morris was convicted under a provision of the CFAA that prohibited only access without authorization, not exceeding authorized access, and he argued to the Court of Appeals for the Second Circuit that because he indeed had access to some computers on the Internet, he was not fully "without authorization" but at most exceeded the authorization he was given. *Id.* at 509. The court, however, ruled that because Morris did not use the INTERNET for e-mailing and research purposes—the intended function of the network—his release of a malicious worm constituted unauthorized access. *Id.* at 510. Incidentally, Morris is now a tenured associate professor in the Computer Science department at MIT. Robert Morris, http://pdos.csail.mit.edu/~rtm/ (last accessed Sept. 29, 2009).

[89] United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).

test in a criminal context, none have extended the contract theory of liability to criminal defendants. And equally importantly, all criminal prosecutions under § 1030(a)(2)(C) have involved circumvention of code-based protective measures.

B. Judicial Interpretations of "Unauthorized Access"

1. Contractual Theory of "Unauthorized Access" – Civil Cases

In its trial brief for the Drew case, the government emphasized the "great weight of circuit authority holding that contractual terms can identify what is 'unauthorized' . . . within the meaning of Section 1030."[90] This statement is not baseless: The rise in Internet commerce over the past ten years has led to more websites with "clickwrap" licenses—essentially, online terms of use to which the user must agree while accessing the site or downloading products from it.[91] Generally, courts have found that such "clickwrap" agreements can constitute binding contracts.[92]

Assuming such online contracts are binding, the prosecution is correct that some courts interpreting the CFAA's civil provisions have held that a breach of contract can constitute unauthorized access. However, the bulk of these cases involve anti-competitive behavior between businesses and their employees in relationships governed by offline paper agreements. For example, a rival company might use some sort of program or code to mine a competitor's website for valuable data, in violation of a confidentiality agreement or express prohibition not to do so.[93] Or an employee might quit his job at company A but take proprietary computer data along with him to company B in violation of a confidentiality or non-compete agreement.[94]

[90] *Government's Response, supra* note 86, at 10.

[91] Specht v. Netscape Commc'ns. Corp., 150 F. Supp. 2d 585, 593–94 (S.D.N.Y. 2001) ("A click-wrap license presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an icon. The product cannot be obtained or used unless and until the icon is clicked.") More precisely, "clickwrap" agreements typically govern tangible products, such as downloadable software, while Terms of Use govern use of a website. Courts have held both to be enforceable contracts, and the terms are treated as interchangeable for purposes of this Recent Development.

[92] *See, e.g.,* A.V. v. iParadigms Ltd. Liability Co., 544 F. Supp. 2d 473, 480 (E.D. Va. 2008) (holding that defendants had agreed to abide by website terms of use by clicking "I agree" to the terms on the site, and collecting cases enforcing online clickwrap and terms of service provisions as binding contracts).

[93] *See, e.g.,* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580–82 (1st Cir. 2001) (noting that, for purposes of preliminary injunction, plaintiff could likely prove that defendant's use of a scraper program to mine data on plaintiff's website constituted access without authorization where the scraper program was created using information protected by a confidentiality agreement).

[94] *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (Posner, J.) (reasoning that defendant's authorized access to his company-issued laptop terminated when he "[decided] to quit IAC in violation of his employment contract . . . . [and] resolved to destroy files . . . that were . . . the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee."). *Citrin* involved an employee contract, but some courts have gone further and used agency principles to find unauthorized access to computers even in the absence of an offline contract. The most striking example of this broad theory of application is Shurgard Storage Ctrs. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (holding that the employee in question lost his "authorized access" to his company's computers the

However, the Lori Drew case presents a narrower question: Outside the realm of competing business entities, does violation of a public website's terms of service constitute "unauthorized access"? A few courts have answered in the affirmative, at least in a civil context. One such example is *America Online, Inc. v. LCGM, Inc.*:[95] There, online service provider AOL brought a civil claim against the defendant LCGM under § 1030(a)(2)(C) and § 1030(g) of the CFAA, alleging that the defendants, in violation of AOL's terms of service, collected the e-mail addresses of thousands of AOL members and transmitted to them nearly 100 million spam emails advertising pornographic websites.[96] The court granted AOL summary judgment on the CFAA claim, noting rather succinctly: "Defendants have admitted to maintaining an AOL membership and using that membership to harvest the e-mail addresses of AOL members. . . . Defendants' actions violated AOL's Terms of Service, and as such was [sic] unauthorized."[97]

Yet some courts interpreting the CFAA in a civil context have waffled on the issue of whether violation of website's terms of use constitutes "unauthorized access,"[98] or have dodged the question altogether.[99] Even more notably, one court has questioned the idea that the CFAA applies to use of public websites, regardless of any terms of use. In *Healthcare Advocates, Inc. v. Harding, Earley, Follmer, & Frailey,*[100] the defendants, in the course of intellectual property litigation, used the Internet Archive's Wayback

instant he began acting as an agent for the competing entity). This theory of "unauthorized access" has been expressly rejected by some courts and commentators as too broad an application of the CFAA. *See, e.g.*, Condux Int'l Inc. v. Haugum, No. 08–4824, 2008 U.S. Dist. LEXIS 100949 at *12–15) (D. Minn. Dec. 15, 2008) (collecting cases rejecting the *Shurgard* agency theory of unauthorized access and noting that it "incorrectly focuses on what a defendant did with the information after he accessed it" instead of the correct question of whether the defendant's access was unauthorized); Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions,* 2009 U. ILL. J.L. TECH. & POL'Y 429 (2009).

[95] 46 F. Supp. 2d 444 (E.D. Va. 1998).

[96] *Id.* at 448.

[97] *Id.* at 450. *See also* Ticketmaster L.L.C. v. RMG Techs. Inc., 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (granting preliminary injunction on CFAA claim against defendant company where it used a scraper program to glean information off Ticketmaster's public website in violation of the site's terms of use); Hotmail Corp. v. Van$ Money Pie Inc., No. C 98-20064, 1998 WL 388389, U.S.P.Q.2d 1020, at *6 (N.D. Cal. Apr. 16, 1998) (finding likelihood of success on the merits of CFAA and breach of contract claims where defendants violated Hotmail's terms of service by sending spam and pornographic emails).

[98] *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273–75 (N.D. Iowa 2000) (noting on motion for summary judgment that "it is not clear that a violation of AOL's membership agreements results in 'unauthorized access,'" and that the Senate Judiciary Committee, in revising the CFAA in 1986, expressly rejected the idea of enacting a comprehensive federal statute that left no computer crime uncovered); Southwest. Airlines Co. v. Boardfirst, L.L.C., No. 3: 06-CV-0891-B, 2007 U.S. Dist. LEXIS 96230, at *44–45 (N.D. Tex. Sept. 12, 2007) (questioning whether defendant violated the CFAA simply by using plaintiff's website for "commercial gain" as prohibited by the site's terms of service, and asking parties to brief the question of whether the "rule of lenity" should apply to this interpretation of the CFAA).

[99] *See* Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004) (in case where defendant allegedly used scraper program to collect information from Southwest's website in violation of its terms of use, the court noted that regardless of whether the terms of use agreement constituted a valid contract, the defendant's actions were nonetheless "without authorization" because the plaintiff had directly informed the defendant that it objected to use of the scraper).

[100] Healthcare Advocates, Inc. v. Harding, Earley, Follmer, & Frailey, 497 F.Supp.2d 627 (E.D. Pa. 2007).

Machine[101] to view archived copies of Healthcare Advocates' public website.[102] Normally the public would have been denied access to these images, but Internet Archive's servers happened to be malfunctioning and granted the defendants access.[103] The plaintiffs brought a civil claim under § 1030(a)(2)(C), arguing that the Harding firm exceeded its authorized access by using the Wayback Machine to view the archived screenshots.[104] The court, in language that is instructive to the Drew prosecution, granted the defendants summary judgment on the plaintiffs' CFAA claim:

> The facts do not show that the Harding firm did anything other than use the Wayback Machine in the manner it was intended to be used. . . . [T]he Harding firm accessed the Internet Archive's website with only an ordinary web browser [and] they did not employ any special tools. . . . [T]he Harding firm obtained [the disputed] images because Internet Archive's servers experienced a condition that made them forget about protective controls. . . .Healthcare Advocates argues that the Harding firm's access was unauthorized because the images were viewed without its explicit permission. This fact is irrelevant. The statute only penalizes persons who exceed authorization. The Harding firm was given the power to view the images by the Wayback Machine. . . . The Harding firm got lucky, because the servers were malfunctioning, but getting lucky is not equivalent to exceeding authorized access . . . . A cursory review of applicable case law shows that defendants need to [do] something more than merely using a public website in the manner it was intended to be liable under the CFAA.[105]

The *Healthcare Advocates* decision is important for two reasons: First, the court recognized that using a public website in the manner for which it was intended does not fall within the scope of the CFAA's provisions—criminal or civil. Second, the decision is important because it recognizes that a user cannot "exceed authorized access" to a site that she has been given permission to enter—even if the owner of the content does not want the user to see the material in question. Ostensibly, that reasoning would hold even where the content owner states her intentions in the terms of service on a website.

In sum, courts are hesitant to construe a violation of a website's terms of service as "unauthorized access" under the CFAA, doing so only to combat anticompetitive business practices or bulk e-mail spamming. And the *Healthcare Advocates* decision shows reluctance to use § 1030(a)(2)(C) against computer users who are granted open access to a public website.

[101] The Wayback Machine is a public, online library that houses more than 85 billion screenshots of websites from different periods in time, allowing users to examine previous versions of websites that have changed, or that may no longer exist. *Id.* at 631.

[102] *Id.* at 632.

[103] *Id.* The Wayback Machine allows owners of public websites to opt out of its archiving process, which Healthcare Advocates elected to do. *Id.* When a user opts out, Wayback Machine blocks public access to prior versions of the user's website—which is what would have happened had the Harding firm run its searches on a day when the Internet Archive's servers were not malfunctioning. *Id.*

[104] *Id.* at 646.

[105] *Id.* at 648–49.

Finally, it is important to remember that the cases discussing violation of a website's terms of service have all involved the civil provisions of the CFAA. As we will see, no court has held that violation of a contract (let alone violation of a website's terms of service) constitutes "unauthorized access" for purposes of the CFAA's criminal provisions.

2. Contractual Theory of "Unauthorized Access"—Criminal Cases

Three circuits—the First, Fifth, and the Tenth—have considered CFAA criminal prosecutions in which some sort of contract governed use of the computer in question. In none of these prosecutions did the contract ultimately determine the defendant's liability under the CFAA, and in all three of these cases the contract was discussed as a peripheral matter (if it was discussed at all). Still, these decisions are worth examining in detail to understand where prosecutors bringing charges under § 1030(a)(2) of the statute have previously focused their attention. Notably, no court has ever held that obtaining information from a public website with no code-based protection violates the CFAA's criminal provisions.

The First Circuit, in *United States v. Czubinski,*[106] took up the issue in the employee-employer context. Richard Czubinski, an IRS employee, signed the IRS's Rules of Conduct, which prohibited employees from using IRS computer systems for anything outside of "official" duties.[107] Nonetheless, Czubinski knowingly disregarded those rules by browsing the tax returns of various people, including Boston city officials and a former girlfriend.[108] Czubinski was convicted under § 1030(a)(4), which at that time made it a felony to "knowingly and with intent to defraud" access without authorization, or in excess of authorized access, a federal interest computer and obtain "anything of value."[109]

On appeal, Czubinski argued that his browsing of tax returns was an act of "idle curiosity," and that the government failed to prove that in doing so he obtained anything "of value."[110] The First Circuit agreed and reversed Czubinski's conviction.[111] However, as a threshold matter, the court—citing only to the CFAA's definition of "exceeds authorized access"—stated that Czubinski "unquestionably exceeded authorized access to a federal interest computer."[112] The court elaborated no further on this proposition, but it appears that it was doing more than just applying the plain wording of the definition. Under the CFAA, to "exceed authorized access" means to "access a computer with authorization and to use such access to obtain . . . information in the computer that the accesser is not entitled so to obtain . . . ."[113] Czubinski

[106] 106 F.3d 1069 (1st Cir. 1997).
[107] *Id.* at 1071, n. 1.
[108] *Id.* at 1071–72.
[109] *Id.* at 1078.
[110] *Id.*
[111] *Id.* at 1079.
[112] *Id.* at 1078.
[113] 18 U.S.C. § 1030(e)(6) (2006).

was indeed authorized by the IRS to use the database in which he browsed, so the only way to say that he exceeded authorized access by browsing IRS returns out of curiosity is to give life to the contractual provision prohibiting access to the IRS databases for any non-work-related purposes.

Two things, however, limit the reach of the First Circuit's language in *Czubinski* as applied to §1030(a)(2)(C) (which, unlike the provision under which Czubinski was charged, requires no further showing of fraud). First, the court ultimately reversed Czubinski's conviction on all counts,[114] making its interpretation of "unauthorized access" merely dicta. Second, and more critically, the IRS database which Czubinski accessed was not accessible to the general public—instead, it was a government computer that contained sensitive personal data[115]. In many respects, the facts of *Czubinski* are precisely what Congress had in mind when it defined "exceeding authorized access": A computer user who, within the context of a closed network not available to the general public, "while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data . . . that he is not supposed to look at."[116] Put simply, *Czubinski* does not involve a publicly accessible website regulated only by contract, and therefore must be distinguished from the Drew case.[117]

The Fifth Circuit also had a chance to squarely address the issue of liability based on contract terms in *United States v. Phillips*,[118] but ultimately declined to do so. When Andrew Phillips matriculated at the University of Texas at Austin (UT) in 2001, he signed UT's standard computer use agreement, which banned, *inter alia,* port scans[119] and other hacking activity.[120] Shortly thereafter, however, Phillips began using his university computer account to perform port scans on hundreds of websites, including those of private businesses, various U.S. Government agencies, and the British Armed Services network.[121] UT's Information Security Office quickly caught on to Phillips's port scanning and warned him on three separate occasions to stop, but Phillips nonetheless continued.[122]

Phillips then used the information he had collected through port scanning to launch a "brute force attack"[123] on a secure UT website ("TXClass")

[114] United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997). In addition to the CFAA charges, Czubinski was initially charged with nine counts of wire fraud under 18 U.S.C. §§ 1343 and 1346. *Id.* at 1071.

[115] *Id.* at 1071.

[116] S. REP. NO. 99–432, at 7 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2485.

[117] One commentator has further distinguished *Czubinski* by placing it in a line of CFAA cases that deal with access "without authorization" in the employer/employee context discussed in note 95, *supra*, arguing that the *Czubinski* court's brief dicta about exceeding authorized access suggest "that employers have a right to limit their employees' use of company computers to work solely motivated by a desire to serve the company." Kerr, *supra* note 65, at 1634.

[118] United States v. Phillips, 477 F.3d 215 (5th Cir. 2007).

[119] The *Phillips* court described port scanning as the sending of codes or other programs to various computers and networks in order to detect potential vulnerabilities in those computers—often as a prelude to a full-scale hacking attack. *Id.* at 217 n.1.

[120] *Id.* at 217.

[121] *Id.*

[122] *Id.* at 217–18.

[123] Essentially, a hacker launches a "brute-force attack" by collecting thousands of random password

intended only for university staff, bombarding it with random password combinations until a match granted him access to the site and the personal data contained thereon.[124] That had the effect of bringing down the UT computer system on several separate occasions, rendering the university's payroll, accounting, and medical records inaccessible.[125] Phillips was convicted under § 1030(a)(5)(A) of the CFAA,[126] which makes it a crime to "knowingly cause[] the transmission of a program . . . or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[127]

On appeal to the Fifth Circuit Court of Appeals, Phillips argued that he had "de facto" authorization to browse the Internet as a public user, and that because he was able to at least view TXClass's login page (if not the content on the site), he merely "exceeded" his authorization to the site by going beyond the login portal and therefore could not be considered an "unauthorized user" under § 1030(a)(5)(A).[128] However, the Fifth Circuit rejected this argument, noting that "access" to the login page was not in fact "access" to the site itself because of the code-based protections on the TXClass site: A user could only log on to TXClass by using a social security number password to which UT has "affirmatively granted access," and "[n]either Phillips, nor members of the public, could obtain such authorization from UT merely by viewing a login page, or clicking a hypertext link."[129] Then, in dicta, the court said this:

> [C]ourts have recognized that authorized access typically arises only out of a contractual or agency relationship. While Phillips was authorized to use his UT email account and engage in other activities defined by UT's acceptable use policy, he was never authorized to use TXClass. The method of access he used makes this fact even more plain.[130]

The prosecution in the Drew case seized upon this language—especially the first sentence—to support its proposition that "accessing protected computers in violation of written agreements by computer owners is 'unauthorized' within the meaning of Section 1030."[131] But that interpretation is missing a very important caveat: The court's language in *Phillips* only makes sense in light of its explicit recognition that TXClass was a private website with code-based password protection—a site not available to the general public. Without that limitation, the statement that authorized access to computer networks or websites arises *only* out of a contractual or agency relationship would be absurdly untrue: It ignores the millions of Internet users

combinations and then repeatedly blasting the secure site with them until one of the randomly generated passwords "matches" an authorized site password, thereby allowing access. *Id.* at 218.

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] 18 U.S.C. § 1030(a)(5)(A)(i) (2008).

[128] *Phillips*, 477 F.3d at 219. Recall that unlike § 1030(a)(2)(C), § 1030(a)(5) does not include the language "exceeds authorized access."

[129] *Id.* at 220.

[130] *Id.*

[131] *Government's Response, supra* note 86, at 7.

who are freely "authorized" to peruse public websites with *no* restrictions whatsoever—contractual, code-based, or otherwise. The *Phillips* court, then, meant to say that authorized access *to private websites with code-based protection* typically only arises out of a contractual or agency relationship.

The only reported case to touch upon contract liability in the context of a prosecution under § 1030(a)(2)(C) is *United States v. Willis.*[132] There, the defendant, who worked for a credit collection agency, was given password access to a proprietary financial information services website (Accurint.com) that contained the names, addresses, social security numbers, and other property data of private citizens.[133] Though agency employees were not authorized to use any information on Accurint.com for personal use, Willis nonetheless began funneling information on the site to Michelle Fischer, who Willis met through his drug dealer.[134] Willis later gave Fischer a defunct password and helped her log on to the site to obtain more information.[135] Fischer subsequently was arrested for identity theft, and Willis was charged with aiding and abetting the accessing of a protected computer without authorization in violation of 18 U.S.C. §§ 2(a) and 1030(a)(2)(C).[136] The Tenth Circuit affirmed Willis's conviction on other grounds not relevant here, and because Willis conceded that Fischer did not have authorized access to the Accurint.com site, the Tenth Circuit did not discuss the nature of the contract or formal policy (if any) that governed the use of the Accurint.com Web site.[137]

However, the facts of the case clearly indicate that the database was private—precisely because it was protected by strong code-based measures (a username and password issued by the computer owner). To that extent, the *Willis* case is analogous to *Czubinski* and *Phillips* in standing for the proposition that owners who allow some users access to their private, code-protected Web sites may in some cases dictate the scope of that access by contract. The few other criminal prosecutions brought under § 1030(a)(2)(C) have followed the same mold: theft or abuse of sensitive information from a code-protected, private database.[138] In fact, that theme persists uniformly throughout all criminal prosecutions under CFAA provisions that have "without authorization" as an element—most notably §§ 1030(a)(4)[139] and

[132] 476 F.3d 1121 (10th Cir. 2007).

[133] *Id.* at 1123.

[134] *Id.*

[135] *Id.*

[136] *Id.* at 1124.

[137] *See id.* at 1126 ("Mr. Willis does not contest that he provided Ms. Fischer unauthorized access to Accurint.com."). If the prosecution's theory was simply that Ms. Fischer's access was unauthorized, then that could presumably be established by showing that she was not an employee of Credit Collections, Inc. and therefore not party to that company's user agreement with LexisNexis, which governed access to the site. *See id.* at 1123.

[138] *See* United States v. Johnson, 58 Fed. Appx. 926, 927 (3d Cir. 2003) (stating that defendant accessed Pennsylvania State Police computer system in order to provide fraudulent drivers licenses); United States v. Galietti, No. 3:06CR161 (EBB), 2007 U.S. Dist. LEXIS 80492, at *4 (D. Conn. 2007) (stating that defendant, a Connecticut State Trooper, allegedly used a state police computer database to obtain license plate numbers in order to further a racketeering scheme); United States v. Ivanov, 175 F.Supp. 2d 367, 369–70 (D. Conn. 2001) (stating that defendant hacked into corporation's internal network and demanded $10,000 to make the system secure again).

[139] *See, e.g.*, United States v. Green, 428 F.3d 1131, 1132–33 (8th Cir. 2005) (stating that defendant

1030(a)(5).[140]

Put another way, the overwhelming bulk of criminal case law under these sections of the CFAA involves defendants who have circumvented code-based measures on private Web sites, not to everyday Internet users who violate the terms of a publicly accessible Web site. That is precisely how the statute should be applied, and in the next section, this Recent Development argues that this application is consistent with congressional intent, canons of statutory interpretation, and basic constitutional protections.

IV. Resolution and Recommendation

A. Code-Based Interpretation of "Without Authorization" Under § 1030(a)(2)(C)

Because of the sheer number of Internet users who access public Web sites with terms of service on a daily basis, the prosecution's overly broad

paid SBC Communications employees to steal the names and social security numbers of SBC customers, which he then used to buy flat-screen televisions on credit); United States v. Soo Young Bae, 250 F.3d 774, 775 (D.C. Cir. 2001) (stating that defendant, licensed by the State to operate a computer terminal that generated lottery tickets, generated tickets without paying for them and then tried to redeem the winnings); United States v. Sadolsky, 234 F.3d 938, 940 (6th Cir. 2000) (stating that defendant accessed his employer's computers to fraudulently credit money for phantom "returned merchandise" to his own credit card); United States v. Czubinski, 106 F.3d 1069, 1078–79 (1st Cir. 1997) (stating that defendant was charged with exceeding authorized access after browsing tax returns on an internal IRS database); United States v. Petersen, 98 F.3d 502, 504 (9th Cir. 1996) (stating that defendant hacked into Pacific Bell computer system in order to seize the phone lines of a radio station); United States v. Sykes, 4 F.3d 697, 698 (8th Cir. 1993) (stating that defendant was charged with computer access fraud for unauthorized use of a stolen ATM card and PIN); United States v. Morris, 928 F.2d 504, 505–06 (2d Cir. 1991) (stating that defendant released virus onto networked computers); United States v. Grooters, No. 1:07-CR-001, 2008 U.S. Dist. LEXIS 48222, at *8 (W.D. Mich. June 24, 2008) (stating that defendant used a non-public database at a federal public defender's office to obtain personal addresses and social security numbers).

[140] *See, e.g.*, United States v. Heckencamp, 482 F.3d 1142, 1143–45 (9th Cir. 2007) (stating that defendant was charged for using computer on university network to hack into Qualcomm Corporation's internal network); United States v. Perry, 479 F.3d 885, 887 (D.C. Cir. 2007) (stating that fired employee was charged for using home computer to remotely hack into former employer's internal network and disable the server); United States v. Phillips, 477 F.3d 215, 218 (5th Cir. 2007) (stating that defendant launched brute-force password attack on secure university Web site); United States v. Shea, 493 F.3d 1110, 1113–14 (9th Cir. 2007) (stating that defendant placed "time bomb" program on company's internal database of debtor accounts); United States v. Trotter, 478 F.3d 918, 919–20 (8th Cir. 2007) (stating that defendant used a remote computer to hack into a former employer's internal database, deleting files and leaving obscene messages); United States v. Millot, 433 F.3d 1057, 1058–60 (8th Cir. 2006) (stating that former employee retained network access card and used it to access his former employer's internal computer network system); United States v. O'Brien, 435 F.3d 36, 37–38 (1st Cir. 2006) (stating that former employee was charged for using remote computer to hack into tour company's internal database and cancel customer reservations); United States v. Schuster, 467 F.3d 614, 615 (7th Cir. 2006) (stating that former employee of wireless provider used access information of former clients to log onto his former employer's internal network, disrupting the ability to provide wireless services); United States v. Mitra, 405 F.3d 492, 493 (7th Cir. 2005) (stating that defendant was charged for using remote radio transmitter to jam computer-controlled emergency response system); United States v. Lloyd, 269 F.3d 228, 231 (3d Cir. 2001) (stating that defendant was charged for planting a computer "time bomb" on the central file sever of his employer's internal computer network); United States v. Middleton, 231 F.3d 1207, 1208–09 (9th Cir. 2000) (stating that former employee used his retained e-mail account and "switch user" program to gain administrative user access to company's internal network); United States v. Sablan, 92 F.3d 865, 866–67 (9th Cir. 1996) (stating that former bank employee, using password she had retained after being fired, accessed bank's mainframe computer and damaged files therein).

interpretation of the CFAA threatens to criminalize the conduct of millions of people. Therefore, when analyzing criminal charges of accessing a protected computer "without authorization" under § 1030(a)(2)(C) of the CFAA, courts must ask a series of questions that focuses on both the content on the Web site and the protective barriers that the site owner has erected around that content.

The first question to ask is whether the Web site in question is private or public. The answer is as simple as the mode of protection: a Web site—or perhaps more accurately, the part of a computer or Web site a defendant has tried to access—should be defined as "private" if the Web site owner has erected strong code-based measures that affirmatively regulate and control public use of that part of the site. If he has only stipulated terms of use while still allowing free access to his Web site, the site is public and the user is presumed to have full authorization to access it. Therefore, § 1030(a)(2)(C) does not apply to any information obtained from the site, and the court's analysis is over.[141]

If the Web site is private—in other words, if the Web site's owner has erected strong code-based controls to exclude public access—then the question of authorization turns on whether the user is an "insider" or an "outsider" as contemplated by the CFAA. To make that determination, courts must ask what kind of user rights, if any, have been specifically delegated to the user by the Web site owner. If the computer owner has granted the user at least some right to use the Web site for some purpose, then she is "authorized" to access the site for purposes of the CFAA and should be considered an "insider." Such "right" of access could consist of a password code assigned to the user by the Web site owner, or the Web site owner could have a network administrator responsible for registering authorized users.

If the user has been given a right of access, courts must then determine if the user nonetheless used her authorized access to "obtain or alter information" on the Web site to which she is not entitled to obtain or alter—in other words, whether her use "exceeds authorized access." And in deciding whether a user has accessed or obtained information to which she is not entitled to obtain or alter, courts may use the *Morris* "intended function" test to determine the "reasonable expectations" of the Web site owner and the user—taking into consideration things like usage contracts if necessary.

Finally, if a private Web site's owner has not specifically granted the user in question any specific rights to access the site, then she is "without authorization" for purposes of § 1030(a)(2)(C) if she obtains information by

[141] This does not mean that the CFAA *as a whole* can never apply to public Web sites. For example, if a hacker uses a remote virus to commandeer control of the *New York Times*' online Web page and defiles it with Swastikas and other hate propaganda, he has certainly "accessed" a public Web site, but he has done so in a way that circumscribes code-based protection and is therefore subject to prosecution under § 1030(a)(5)(A), which prohibits "knowingly caus[ing] the transmission of a program . . . and as a result of such conduct, intentionally caus[ing] damage without authorization . . . to a protected computer." If, however, a user browsing the *New York Times*' public Web site stumbled across proprietary information about editor salaries that had been inadvertently released to the site, she could not be subject to prosecution under § 1030(a)(2)(C) if she were to post that salary information on her own blog—no matter how much the Times *intended* to keep that information private—because she did not circumvent code-based protection to obtain the information. *See supra* Part III.B.1, notes 98–105 and accompanying text.

circumventing the code-based protections the owner has put in place. For example, she might defeat code-based protection by transmitting a virus, or by using an illegally obtained password, or by electronically bombarding the login page with random passwords until the proper combination triggers access. As explained below, this proposal is consistent with both the legislative intent of Congress in passing the CFAA, as well as traditional notions of statutory interpretation and due process.

B. A Code-Based Interpretation of "Without Authorization" Is Consistent with Congressional Intent

This code-based interpretation of "without authorization" under § 1030(a)(2)(C) is consistent with Congress's intentions for the CFAA for several reasons.[142] First, when Congress passed the CFAA, all the computers to which the Act applied were "private," and they were private because the government and financial institutions used code-based protections to shield their sensitive data from public access.[143] As the Senate Judiciary Committee observed in 1984,

> Most systems use some sort of variant of an identification/code password system. . . . Until recently, this form of security was sufficient, since most users only had the ability to use "dumb" terminal devices for access. . . . [But the] personal computer allows its user to employ the power of the computer to break into other computer systems by systematically speeding up what would otherwise be a slow, hit or miss process [of manual password-guessing].[144]

This arguably also explains why Congress chose not to define the phrase "without authorization" while at the same time differentiating that term from access "in excess" of authorization. In a world where all computer networks are private, the phrase "without authorization" is self-explanatory: Any outsider who somehow gets into a private network clearly has no authorization to do so. Yet Congress envisioned hierarchical levels of authorized access among "insiders" to government and financial computer networks (certainly, a low-level CIA staffer would not be granted the same level of access to information as the agency's director), and therefore defined the term "exceeds authorized access."[145]

[142] The leading commentators who have proposed a code-based interpretation of the CFAA's "without authorization" provisions have not squarely addressed this issue. See Kerr, *supra* note 65, at 1657–63, where Professor Kerr discusses the implications of using a code-based standard of "without authorization" under § 1030(a)(2)(C), but does not address whether that interpretation is consistent with congressional intent. *See also* Bellia, *supra* note 40, at 2255–58, where Professor Bellia discusses Congress's intent in passing the CFAA, but within the context of her argument for a broad definition of the term "access."

[143] *See* Bellia, *supra* note 40, at 2254 ("[P]rovisions [of the CFAA] clearly contemplate conduct that involves obtaining information not generally available to the public . . . . Since the information is not available to the public, it is necessarily segregated by code—whether by a password or other technical measure . . . .").

[144] Comprehensive Crime Control Act of 1984, Pub. L. No. 98–473, 1984 U.S.C.C.A.N. (98 Stat. 1837) 3182, 3696.

[145] The Senate Judiciary Committee gave another example in the 1986 Amendments to the CFAA: "[A

But even in the multitude of CFAA amendments that have been passed since public Internet use has become widespread, Congress has never suggested that the Act applies to obtaining information from computers and websites that do not include code-based privacy protection measures—though it has had ample opportunity to do so. For example, in the 2002 revisions, Congress expressed its concern over "zombie attacks"[146] on home computers—essentially a process by which a hacker takes remote control over a user's personal computer by embedding malicious codes onto the computer's hardware.[147] And in 2008, Congress strengthened the CFAA to combat the surreptitious placement of spyware on private computers.[148] Both of these types of computer invasions involve circumvention of code-based protection on a user's computer.

Second, a code-based interpretation is in line with CFAA's overall purpose, which is to protect the "confidentiality, integrity, and security of computer data and networks."[149] Certainly, one way of doing that is to provide criminal penalties for serious computer crime violations, but the legislative history of the Act shows that Congress was also interested in encouraging computer owners to protect their data in the most effective way possible. It is somewhat ironic that courts have held that violation of a website's terms of use can constitute a civil violation of the CFAA's provisions, because the civil remedy was added to the CFAA in part to encourage computer owners to improve their computer security measures.[150] Holding a violation of a website's terms of service to be "unauthorized access" arguably *discourages* website owners from using more complex and effective code-based measures to protect their data. If a self-written contract on a webpage is construed as sufficient privacy protection measures for purposes of the CFAA, computer users in many cases will surely not incur the additional time and expense of coding protection onto their sites.

Finally, this interpretation is consistent not only with the statutory structure of the CFAA, but also with the intended scope of the CFAA's reach. Certainly, Congress has spoken of its desire to "ensure that the [CFAA] is up-to-date and provides law enforcement with the necessary legal framework to

government] employee who uses his department's computer and, without authorization, forages into data belonging to another department, [has] engaged in conduct directly analogous to an 'outsider' tampering with Government computers." S. REP. NO. 99–432, at 8 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

[146] *See* Zxsmby, Zombie Computers—Spreading the Virus, http://www.zsxmby.com/zombie-computers-spreading-the-viruses.html (last visited Sept. 29, 2009) (describing a zombie computer as "virtually a home PC tainted with a virus"). For an example of a zombie attack warning of zombie attacks, visit http://gizmodo.com/5141800/hacked-construction-signs-warn-of-zombie-attack-in-austin.

[147] *See* H.R. REP. NO. 107–497, at 8 (2002) (noting that "zombie" computers have been used to launch denial-of-service attacks on Internet service providers, resulting in millions of dollars worth of damage).

[148] *See* Press Release, Office of Senator Patrick Leahy, Leahy-Authored Anti-Cyber Crime Provisions Set to Become Law (Sept. 15, 2008), *available at* http://leahy.senate.gov/press/200809/091508b.html (describing the growing problem of the use of spyware to steal sensitive personal information off of computers). Spyware has been generally defined as "software that performs certain behaviors, generally without appropriately obtaining your consent first, such as: [a]dvertising, [c]ollecting personal information, [or] [c]hanging the configuration of your computer[.]" Microsoft.com, What is Spyware, http://www.microsoft.com/security/spyware/whatis.aspx (last visited Sept. 29, 2009).

[149] S. REP. NO. 104–357, at *3 (1996).

[150] 146 CONG. REC. S10, 916 (daily ed. Oct. 24, 2000) (statement of Sen. Leahy).

fight computer crime,"[151] and this language has led some courts to conclude that the Act's provisions should be interpreted broadly.[152]

Importantly, though, Congress expressly envisioned an outer limit to that legal framework. In expanding the CFAA, Congress has at the same time made clear that it does not intend for the Act to criminalize minor instances of computer crime—even intentional ones.[153] Recognizing that states are free to pass their own computer laws, Congress evinced intent to take federal jurisdiction only over computer crimes in which there is a "compelling federal interest."[154] The CFAA's legislative history is filled with examples of malicious computer access that threatens national security or economic interests,[155] jeopardizes sensitive private financial or personal identifying data,[156] or has the potential to cause serious physical harm.[157] By itself, violating a public website's terms of service does none of those things.

Further, courts have consistently warned against interpreting statutes in a manner that criminalizes a broad range of conduct,[158] yet as Judge Wu noted in

[151] S. REP. NO. 104–357 at 5 (1996).

[152] *See, e.g.,* United States v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2000) (noting that Congress has consciously broadened the CFAA since it was first enacted); United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (Easterbrook, J.) (" Well of course Congress did not contemplate or intend this particular application of the [CFAA]. . . . Legislation is an objective text approved in constitutionally prescribed ways; its scope is not limited by the cerebrations of those who voted for or signed it into law.").

[153] *See* S. REP. NO. 99–432 at 4 (1986), *as reprinted in* 1986 U.S.S.C.A.N. 2479, 2482 (rejecting the idea that "Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered"); 146 CONG. REC. S10, 916 (daily ed. Oct. 24, 2000) (statement of Sen. Leahy) ("Our federal laws do not need to reach each and every minor, inadvertent and harmless computer abuse—after all, each of the 50 states has its own computer crime laws. Rather, our federal laws need to reach those offenses for which federal jurisdiction is appropriate.").

[154] S. REP. NO. 99–432 at 4 (1986), *as reprinted in* 1986 U.S.S.C.A.N. 2479, 2482. *See also* Reid Skibell, *Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003) (noting that when Congress expanded the CFAA in 1986, "a key . . . concern was differentiating between computer trespass and more damaging types of computer crime. Part of the rationale for this distinction was a belief that the law's focus should be on combating computer abuses that would either result in significant economic harm or threaten the integrity of sensitive data.").

[155] *See, e.g.,* S. REP. NO. 104–357 at 5–6 (1996) (citing examples of hacking incidents at Grifess Air Force Base in New York, the Defense Department, and NASA); 142 CONG. REC. S10,889 (daily ed. Sept. 18, 1996) (statement of Sen. Leahy) (citing examples of unauthorized computer access to Operation Desert Storm data, federal courthouse records, and individual IRS tax returns, and further noting that financial losses as a result of breaches of computer systems in the private sector totaled $2 billion to $4 billion in 1995); 142 CONG. REC. 23,783 (1996) (statement of Sen. Kyl) (noting that the Act will strengthen current computer crime law in order to "protect the national information infrastructure," as well as "banks, hospitals, and other information-sensitive businesses which maintain sensitive computer files. . . ."); *id.* at 27, 119 (statement of Sen. Leahy) (noting that the revisions to the Act "will help safeguard the privacy, security, and reliability of our national computer systems and networks and the information stored in, and carried on, those networks").

[156] *See, e.g.*, Press Release, Office of Senator Patrick Leahy, Leahy-Authored Anti-Cybercrime Provisions Set to Become Law, *available at* http://leahy.senate.gov/press/200809/091508b.html (Sept. 15, 2008) (noting that the 2008 amendments to the CFAA were designed to combat identity theft perpetuated by hackers who use spyware to steal sensitive information off of personal computers).

[157] H.R. REP. NO. 107–497, at 8 (2002) (noting that "denial-of-service" attacks perpetuated by hackers on emergency response networks could prevent prompt aid, thereby potentially causing injury or death); *See* S. REP NO. 99–432, at 2–3 (1986), *reprinted in* 1986 U.S.S.C.A.N. 2479, 2480 (noting an incident in which a group of hackers broke into the computer system at the Memorial Sloan-Kettering Medical Center in New York, giving them the ability to alter the radiation treatment levels of more than 6,000 patients).

[158] United States v. LaMacchia, 871 F. Supp. 535, 544 (D. Mass. 1994) (dismissing wire fraud action against student who illegally downloaded computer software, noting that "[w]hile the government's objective is a laudable one . . . its interpretation of the wire fraud statute would serve to criminalize the conduct of . . .

his ruling, that is precisely what the government's interpretation of "unauthorized access" in the Lori Drew prosecution threatened to do.[159] As one commentator has noted, a contract-based interpretation of "unauthorized access" under the CFAA would allow a computer owner to "set up a public web page, announce that 'no one is allowed to visit my web page,' and then refer for prosecution anyone who clicks on the site out of curiosity."[160] In enacting the CFAA, Congress did not contemplate such a slippery slope to federal criminal jurisdiction.

C. A Code-Based Approach to "Unauthorized Access" is Consistent with Canons of Statutory Interpretation

As Judge Wu correctly pointed out in his ruling to dismiss the Drew case, the government's interpretation of §1030(a)(2)(C) renders the statute void for vagueness because it "[fails] to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits . . . . "[161] Did Congress intend to make criminals out of those who violate a website's terms of service? The plain terms of the statute do not provide an answer. Further, terms of service are often subject to change without warning,[162] which ostensibly makes it difficult for a user to know whether she is in compliance with all terms at all times.

As to issue of vagueness, it is critically important to understand why the CFAA was passed in the first place—a consideration which Judge Wu did not address in his ruling. The legislative history of the 1984 Act shows that in addressing the rise of computer crime, Congress faced both a legal problem and an attitudinal problem—both of which led it to enact, for the first time, a specific piece of federal legislation dealing with computer crime. The legal problem was that the existing wire fraud and mail fraud statutes were inadequate bases for capturing the emerging body of computer crime law.[163]

the myriad of home computer users who succumb to the temptation to copy even a single software program for private use. It is not clear that making criminals of a large number of consumers of computer software is a result that even the software industry would consider desirable."); *See also,* Dowling v. United States, 473 U.S. 207, 227 (1985) (declining to extend the criminal provisions of the federal Stolen Property Act to defendant's bootlegging activity where doing so would have the effect of criminalizing a wide variety of activity typically regulated by civil copyright law).

[159] *Drew Decision, supra* note 23, at 17.

[160] *Kerr, supra* note 65, at 1650–51.

[161] City of Chicago v. Morales, 527 U.S. 41, 56 (1999). *See also* Drew Decision, supra note 23, at 24–25 (noting the vagueness of the statute due to lack of notice given to "ordinary people" of their legal exposure); McBoyle v. United States, 283 U.S. 25, 25–27 (1931) (Holmes, J.) (reversing defendant's conviction where federal theft statute did not clearly contemplate an airplane as a "motor vehicle," and holding that "it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear."); United States v. Lacher, 134 U.S. 624, 628 (1890) ("Before a man can be punished, his case must be plainly and unmistakably within the statute").

[162] *See, e.g., MySpace Terms , supra* note 7, at ¶ 4 ("MySpace.com may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace.com on the MySpace Website. You agree to be bound to any changes to this Agreement when you use the MySpace Services after any such modification is posted.").

[163] *See* 98 Stat. at 3691 ("Even if an approach is devised that apparently covers the alleged acts in computer related crimes [under the mail or wire fraud statutes], it still must be treated as an untested basis for

More fundamental was the attitudinal problem: Most people viewed hacking conduct as harmless "intellectual pranksterism"[164] rather than conduct that had potentially serious economic and national security ramifications.[165] Therefore, a major goal of the 1984 Act was to provide clear notice that Congress intended to proscribe—and indeed, criminalize—certain forms of computer activity.[166] The solution was therefore a new federal statute that lowered the bar for felony prosecution of hacking conduct.

Today, as in 1984, we are faced with a "tremendous attitudinal problem."[167] In our current online world, self-sharing, voyeurism, and deception are often the norm in public social networking communities like MySpace,[168] and chat room flame wars and hate speech ricochet off the backstop of First Amendment protections. Such conduct—which often violates the terms of use on those websites—is consistently dismissed by many Internet users as harmless "pranksterism."[169] If Congress wishes to criminalize such conduct, then a "clearer statement of proscribed activity" is necessary for compliance with fundamental constitutional notions of due process.[170] Therefore, absent plain and unmistakable congressional intent to impute criminal liability to computer users who violate a website's terms of service, courts should refrain from interpreting the CFAA in such an expansive manner.[171]

Such fundamental notions of due process go hand-in-hand with the rule of lenity, which essentially posits that courts must interpret ambiguous statutes in a way that favors criminal defendants[172]—a proposition that some courts

prosecution in the Federal trial courts.").

[164] *Id.* at 3696. The Senate Judiciary Committee put it this way: "[T]here is a tremendous attitudinal problem that gives the Committee some concern. People can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about taking information by use of a device called a computer even if it costs the economy millions and potentially billions in the future." *Id.* at 3697.

[165] *Id.* at 3695–97.

[166] Continuing Appropriations, 1985—Comprehensive Crime Control Act of 1984, Pub. L. No. 98–473, 1984 U.S.C.C.A.N. (98 Stat. 1837) 3182, 3692 ("The Committee concluded that the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access to them, require a clearer statement of proscribed activity."); S. REP. NO. 104–357, at *3 (1996) ("The Computer Fraud and Abuse Act was originally enacted in 1984 to provide a clear statement of proscribed activity concerning computer. . . . Rather than having to "boot-strap" enforcement efforts against computer crimes by relying on statutory offenses designed for other offences, the [CFAA], . . . set forth in a single statute computer-related offenses.").

[167] 98 Stat. at 3697.

[168] *See* Randall Stross, *When Everyone's a Friend, Is Anything Private?,* N.Y. TIMES, Mar. 7, 2009, at BU3 ("Facebook and other social networking sites has promoted the sharing of all things personal, dissolving the line that separates the private from the public.").

[169] 98 Stat. at 3696. *See, e.g.,* Mattathias Schwartz, *The Trolls Among Us*, N.Y.TIMES MAGAZINE, Aug. 3, 2008, *available at* http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html (describing the practice of online "trolling," by which Internet users anonymously harass other users primarily for their own entertainment).

[170] 98 Stat. at 3692.

[171] *See, e.g.,* United States v. Bass, 404 U.S. 336, 348 (1971) ("[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity."); United States v. Wiltberger, 18 U.S. 76, 95 (1820) ("It is the legislature, not the court which is to define a crime, and ordain its punishment").

[172] *See, e.g.,* Liparota v. United States, 471 U.S. 419, 427 (1985) (recognizing the longstanding principle that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity. . . .

interpreting "without authorization" under the CFAA have rightly heeded.[173] As one court has put it: "To the extent 'without authorization' or 'exceeds authorized access' can be considered ambiguous terms, the rule of lenity . . . requires a restrained, narrow interpretation . . . ."[174]

V. CONCLUSION

In the wake of tragedy often comes new law. As we have seen, it was never Congress' intent to enact a vast piece of computer crime legislation that definitively brings all forms of computer crime within the reach of federal prosecutors; rather, it recognized that states could—and should—continue to enact their own computer crime laws. And indeed, on June 30, 2008, Missouri governor Matt Blunt signed into law an amendment to the state's harassment statute which makes it a felony for an adult to "harass" anyone under the age of 17.[175] Under the amended provision, "harassment" is defined to include "knowingly frighten[ing], intimidat[ing], or cau[sing] emotional distress to another person by anonymously making . . . an electronic communication."[176] Other states have quickly followed Missouri's lead in passing similar anti-cyberbullying statutes.[177]

Courts, however, must resist the urge to vastly expand the reach of § 1030(a)(2)(C) in the absence of clear Congressional intent to criminalize the violation of a website's terms of use. Instead, they should interpret the Act to apply only to computer networks and websites that have strong code-based protections, rejecting the idea that online terms of use can constitute such

Application of the rule of lenity ensures that criminal statutes will provide fair warning concerning conduct rendered illegal and strikes the appropriate balance between the legislature, the prosecutor, and the court in defining criminal liability.") (citations omitted).

[173] *See, e.g.*, Condux Intl. Inc. v. Haugum, No. 08–4824, 2008 U.S. Dist. LEXIS 100949, at *16 (D. Minn. Dec. 15, 2008) ("[P]rinciples of statutory construction require the adoption of a narrow view of the CFAA. When a court is confronted with two rational readings of a criminal statute, it is required to construe the statute in favor of the defendant."); Shamrock Foods v. Gast, 535 F.Supp.2d 962, 966–67 (D. Ariz. 2008) ("The rule of lenity guides the Court's interpretation of the CFAA because it has both criminal and noncriminal applications. Such rule [sic] requires a court confronted with two rational readings of a criminal statute, one harsher than the other, to choose the harsher only when Congress has spoken in clear and definite language. The rule weighs in favor of adopting the narrower approach.") (citations omitted).

[174] Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *23 (M.D. Fla. August 1, 2006).

[175] Joel Currier, *Gov. Blunt Signs Law Against Cyber-Bullying*, ST. LOUIS POST-DISPATCH, July 1, 2008, at D3.

[176] MO. REV. STAT. § 565.090(1)(3) (2008).

[177] *See State Action on Cyberbullying*, USATODAY.COM, 'http://www.usatoday.com/news/nation/2008-02-06-cyber-bullying-list_N.htm (last visited Mar. 12, 2009) (describing anti-cyberbullying statutes passed in 2006 and 2007 by Arkansas, Delaware, Idaho, Iowa, Minnesota, New Jersey, Oregon, South Carolina, and Washington). Even more notably (and perhaps an implicit concession that the CFAA does not reach online behavior such as Lori Drew's), Representatives Linda Sanchez (D-CA) and Kenny Hulshof (R-MO) recently proposed the "Megan Meier Cyberbullying Prevention Act," which would have criminalized the use of "electronic means" to "coerce, intimidate, or harass" another user. H.R. 6123, 110th Cong., 2d Sess. (May 22, 2008). Interestingly enough, the bill was not proposed as an amendment to the CFAA, but to Chapter 41 of Title 18 of the U.S. Code (18 U.S.C. § 871 et. seq.), which generally deals with threats, blackmail and extortion. However, the bill died in the House Subcommittee on Crime, Terrorism, and Homeland Security. Govtrack.us, HR 6123: Megan Meier Cyberbullying Prevention Act, http://www.govtrack.us/congress/bill.xpd?bill=h110-6123 (last visited Mar. 12, 2009).

protection. And most of all, they must resist the urge, in the words of one court interpreting the CFAA, "to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony."[178] Millions upon millions of Internet users are counting on it.

[178] United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997).