April 13, 2009

"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 ............................................................................................................................. 2

II. Background .......................................................................................................................... 4
   A. MySpace ............................................................................................................................... 4
   B. The Facts of the Lori Drew Case ........................................................................................ 5
   C. The Indictment ..................................................................................................................... 7
   D. The Computer Fraud and Abuse Act ............................................................................... 10
      1. Structure of the Law ....................................................................................................... 11
      2. Origins of the CFAA ...................................................................................................... 12
      3. Section §1030(a)(2)(C) of the CFAA ............................................................................. 14
   E. Protection of “Private” Information ................................................................................... 16
      1. Code v. Contract-Based Protection ................................................................................ 18
      2. MySpace – regulation by code or by contract? .............................................................. 20

III. Analysis .............................................................................................................................. 22
   A. “Unauthorized Access” and “Exceeds Authorized Access” – Definitions .................. 23
   B. Judicial interpretations of “without authorization” ......................................................... 24
      1. Contractual Theory of “Unauthorized Access” – Civil Cases ..................................... 26
      2. Contractual Theory of “Unauthorized access” - Criminal Cases ................................. 31

IV. Resolution and Recommendation ...................................................................................... 38
   A. Code-Based Interpretation of Unauthorized Access ..................................................... 38
   B. A Code-Based Interpretation of Access “Without Authorization” is Consistent with
      Congressional Intent .......................................................................................................... 40
   C. A Code-Based Approach to “Unauthorized Access” is Consistent with Canons of
      Statutory Interpretation ...................................................................................................... 46

V. Conclusion .......................................................................................................................... 48
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 prospective employers use Facebook as a means to screen potential employees,¹ and knowing that taller, good-looking people are statistically more 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?

³ See Facebook Terms at “User Conduct” (“[Y]ou agree not to use the Service or Site to . . . impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity. . . .”), and at “User Content Posted on the Site” (“You may not post, transmit, or share User Content on the Site or Service that you did not create or that you do not have permission to post.”), http://www.facebook.com/home.php#!/terms.php?ref=pf (last accessed Mar. 10, 2009).
As a matter of intuition, most people would say “no.” But for Lori Drew, the Missouri woman accused of creating a fake MySpace profile in order to “cyberbully” her daughter’s former friend, the answer is “yes.” Drew - 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 – killed herself, and federal prosecutors charged Lori Drew under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq.

If the story is true, then there is certainly nothing noble about Lori Drew’s conduct. Anonymously harassing an emotionally vulnerable young girl is the epitome of depraved cowardice. Yet the Drew 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 Note 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, instead arguing 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. MySpace

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.\(^4\) Once a member has established a profile – which typically includes a
picture and a list of personal interests - 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.\(^5\) Social networks like MySpace are a relatively recent phenomenon,
yet they have proliferated with amazing speed.\(^6\) MySpace, which was launched in 2003,\(^7\) has
quickly become the largest, with a current (and constantly expanding) membership of more than
246 million users.\(^8\) The site’s persistent appeal with young people,\(^9\) as well as its consistently

---

\(^4\) See Zenyep Tufecki, *Grooming, Gossip, and MySpace*, 11 INFORMATION, COMMUNICATION &
SOCIETY 544, 545 (2008) (defining a social network site as “a category of websites with profiles,
semi-persistent public commentary on the profile, and a traversable publicly articulated social
network displayed in relation to the profile.”).

\(^5\) *Doe v. MySpace, Inc.*, 528 F.3d 413, 415 (5th Cir. 2008).

\(^6\) Tufecki, supra note 4, at 545.


a user registers a new account, MySpace co-founder Tom Anderson automatically becomes her
“first” friend. Sellers, supra note 7. Anderson’s “friend” count is therefore a reasonably
accurate running total of current membership on MySpace.
high web traffic rates, has made MySpace a valuable window into the milieus of politics and pop culture. MySpace is, in short, “simply a place to hang out and express yourself” – a purpose that surely appealed to Megan Meier when she created her MySpace account in 2006.

B. The Facts of the Lori Drew Case

From the outset, it should be noted that the events leading up to Megan Meier’s suicide are “deeply in dispute.” But here is what has been put in the public record: 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.” Megan and Lori Drew’s daughter would go on “jags

---

9 See Tufecki, supra note 4, at 545 (noting that between 80 and 90 percent of college students operate a profile on a social networking site).
12 In 2004, the rock band R.E.M. debuted its album “Around the Sun” on MySpace before it was available anywhere else. Sellers, supra note 7.
13 Id.
16 Id.
of companionship,” but eventually ended their friendship.\textsuperscript{17} In September 2006, Megan’s parents allowed her to sign up for a MySpace account,\textsuperscript{18} despite the fact that, at age 13, she was technically too young to have one.\textsuperscript{19} 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.\textsuperscript{20}

What Megan did not know when she readily accepted Josh’s friend request was that he was a fictional character.\textsuperscript{21} Nonetheless, the pair was soon communicating back and forth. Drew’s pre-trial motions go out of their way to note that the profile of Josh Evans was open for only 29 days, and for 28 of those 29 days “nothing negative was communicated.”\textsuperscript{22} The government’s indictment reveals some PG language of the sort one might expect flirtatious

\textsuperscript{17} Id.
\textsuperscript{18} Id.
\textsuperscript{20} Collins, supra note 15.
\textsuperscript{21} 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. She also testified that the purpose of the fake MySpace profile arose as a way for Drew and her daughter to ascertain whether Megan Meier had been spreading malicious rumors about Drew’s daughter. Id. Media reports have also indicated that Drew and her daughter, as well as Ashley Grills, had access to the “Josh Evans” account. Collins, supra note 15. In any case, “Josh Evans” appeared closely tailored to draw Megan in: “His answer to the section “Goal you would like to achieve this year” was ‘meet a great girl.’ The girl he was looking for happened to have long brown hair, like Megan. As for weight, Josh answered, ‘DONT [sic] REALLY MATTER.’” Collins, supra note 15.
\textsuperscript{22} Motion to Dismiss, supra note 14, at 3, n. 2.
eighth-graders to talk about: Josh allegedly sent a message telling Megan that she was “sexi” [sic], as well as a separate invitation to touch his “snake.”

However, the relationship between Megan and Josh deteriorated rapidly on October 16, 2005, when an “insult war” broke out between the two. The conversation ended “in substance, that the world would be a better place without [Megan] in it.” Shortly after that argument, Megan committed suicide. The government alleged in its indictment that Lori Drew learned of Megan Meier’s suicide that same day, immediately deleted the Josh Evans account, and told one of her alleged co-conspirators to “keep her mouth shut” about it.

C. 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. After the state closed its investigation, the Meiers told their story in November 2007 to a local newspaper columnist, and the case soon spread quickly beyond the confines of Dardenne Prairie. Many news sources framed the Drew

---

24 Collins, supra note 15.
25 Drew Indictment, supra note 23, at 8. 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 15.
26 Drew Indictment, supra note 23, at 8.
27 Currier and Hunn, supra note 14, at A1. Jack Banas, the prosecutor for St. Charles County, Missouri, summed up the futility of his case to The New Yorker: “‘Are you going to hug this lady, say she did something great? No. She made a huge, fatal mistake . . . . But there are disputed facts and undisputed facts, and even if you believe all of them they still don’t give you a criminal fact pattern in the state of Missouri.’” Collins, supra note 15.
28 Collins, supra note 15.
case in terms of a meddlesome, vindictive mother bent on revenge, which sparked outrage and, in some cases, outward hostility toward the Drew family.\textsuperscript{29}

Despite the lack of state charges, federal prosecutors in Los Angeles, California\textsuperscript{30} breathed new life into the Drew saga, and indeed, perhaps into cybercrime law, by charging Lori Drew in May 2008 with one felony count of conspiracy under 18 U.S.C. § 371\textsuperscript{31} and 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)\textsuperscript{32} of the Computer Fraud and Abuse Act (“CFAA”).\textsuperscript{33} The precise details of count one – the conspiracy charge under 18 U.S.C. § 371 - are beyond the scope of this Note, but it was undoubtedly brought in light of the difficulty in sorting out who among Lori Drew, Drew’s daughter, and Ashley Grills took the physical step of registering the phony MySpace profile and communicating with Megan Meier on a day-to-day basis.\textsuperscript{34} The object of the conspiracy, the government alleged, was to obtain information from

\textsuperscript{29} See, e.g., Barbara Shelly, \textit{Online Avengers Perpetrate Problem}, \textit{TULSA WORLD}, Dec. 16, 2007, at G4 (noting that online harassers had published Lori Drew’s address, phone number, and business contact information, causing the Drews to leave their home, separate from their teenage daughter, and close their home-based advertising business).

\textsuperscript{30} MySpace’s central servers – which Lori Drew “accessed” by registering a MySpace account – are located in Beverly Hills, California.

\textsuperscript{31} “If two or more persons conspire either to commit any offense against the United States, or . . . or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”

\textsuperscript{32} “Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer. . . [is subject] to a fine . . . or imprisonment for not more than 5 years . . . [if] the offense was committed in furtherance of any criminal or tortious act . . . .”


\textsuperscript{34} See note 21, \textit{supra}, and accompanying text (indicating that Lori Drew herself did not register the MySpace profile but approved of it); Currier and Hunn, \textit{supra} note 15 (noting that it was initially unclear who registered the profile). Jack Banas, the prosecutor for St. Charles County,
Megan Meier and then use it against her for a tortious purpose: intentional infliction of emotional distress.\(^{35}\)

The crux of counts two through four – accessing a protected computer without authorization under the CFAA – constitutes the root of the prosecution’s theory of Drew’s liability. Essentially, it is this: Section 1030(a)(2)(C) prohibits obtaining information from a “protected computer” by means of intentional, unauthorized access.\(^{36}\) Use of the MySpace website is governed by its Terms of Use, which constitute a contract between MySpace and its users.\(^{37}\) 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.”\(^{38}\) Because Lori Drew’s conduct was in express

---

\(^{35}\) *Drew Indictment*, *supra* note 23, at 5. An action for the common law tort of “intentional infliction of emotional distress” will lie “where the defendant intentionally engaged in some conduct toward the plaintiff . . . with the purpose of inflicting emotional distress, or . . . where any reasonable person would have known that such would result; and his actions are of such a nature as to be considered outrageous and intolerable in that they offend against the generally accepted standards of decency and morality.” *Samms v. Eccles*, 358 P.2d 344, 346-47 (Utah 1961); *see also* Restatement 2d Torts § 46 (“One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.”).

\(^{36}\) *18 U.S.C. § 1030(a)(2)(C) (2008)* (“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.”)

\(^{37}\) *MySpace Terms, supra* note 20 (“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.”).

violation of 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. Unauthorized access under §1030(a)(2)(C) is a misdemeanor unless committed in furtherance of an intentional tortious act, in which case the charge becomes a felony.

On November 26, 2008, a jury in Los Angeles convicted Lori Drew of three misdemeanor counts of computer fraud under the CFAA. Though the jury rejected the prosecution’s theory that Drew intended to harm Megan Meier through her conduct – 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.

[As of this writing, Drew is currently awaiting sentencing.]

D. The Computer Fraud and Abuse Act

Prohibited (“Prohibited activity includes . . . using any information obtained from MySpace services to harass, harm, or abuse another person . . . “). 39 Drew Indictment, supra note 23, at 9-10.

40 Id. at 6; S. Rep. 104-357, at *8 (1996).


42 Id. This raises an important point with regard to the scope of this Note: Though the prosecution initially charged Drew with two separate violations of MySpace’s Terms of Use (using false information to register an account and using the account to “harm, harass or abuse another person.”), the jury convicted Drew of only one of those violations. In other words, Drew’s alleged cyberbullying conduct is no longer at issue – the sole issue is whether violation of a website’s terms of service constitutes “unauthorized access” under the CFAA. In her post-trial briefs, Drew argued that her false registration information nonetheless did not vitiate MySpace’s consent to access the site by raising the rather tricky dichotomy between “fraud in the inducement” and “fraud in the factum.” See Supplement to Rule 29 Motion, United States v. Drew, No. CR-08-582-GW (C.D. Cal. Dec. 15, 2008) (“Rule 29 Motion”). That defense is beyond the scope of this paper, but for a detailed discussion of the legal concepts involved, see Orin S. Kerr, Cyberspace’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes, 78 N.Y.U. L. REV. 1596, 1652-54 (2003).
1. Structure of the Law

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. 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.

The Act 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; 2) compromises the confidentiality of data by obtaining information from a protected computer; 3) intentionally trespasses in a government or federal interest computer; 4) knowingly accesses a protected computer with intent to defraud and thereby obtains something of value; 5) causes damage to a computer, either by the knowing transmission of code or by intentional trespass; 6) knowingly, and with intent to defraud, trafficks in computer

---

passwords;\textsuperscript{50} 7) with intent to extort money or something else of value, threatens to damage a protected computer.\textsuperscript{51} 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.\textsuperscript{52}

Though this Note will primarily focus on § 1030(a)(2)(C), the CFAA provision under which Lori Drew was charged, it will at times discuss the Act’s other provisions not only to draw out broad themes that run throughout the CFAA, but also to analyze how courts have interpreted statutory language common to all CFAA criminal provisions.

2. Origins of the CFAA

The goals and current structure of the CFAA cannot be fully understood without a short history lesson on why the statute was passed. Congress enacted the CFAA’s predecessor, the Counterfeit Access Device and Computer Fraud and Abuse Act, in 1984.\textsuperscript{53} At that time, computers had already become an integral part of the national defense and finance sectors.\textsuperscript{54} Hackers, naturally interested in the information banks and governments kept behind their new computerized walls, quickly found surreptitious ways to satisfy their curiosity.\textsuperscript{55}

\textsuperscript{54} The statute applied only to certain non-public computers - those that contained private financial data or national security information, or those that were under government operation. Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. REV. 2164, 2255 (2004).
But the legislative history of the 1984 Act reveals 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. But more fundamental was the attitudinal problem - most people viewed hacking conduct as harmless “intellectual pranksterism” rather than conduct that had potentially serious economic and national security ramifications. Therefore, a major goal of the original CFAA was to provide clear notice that Congress intended to proscribe – and indeed, criminalize – certain forms of computer activity. The solution was therefore a new federal statute that lowered the bar for felony prosecution of hacking conduct.

---

56 See id. 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 prosecution in the Federal trial courts.”).

57 Id. at 3696. The Senate Judiciary Committee put it this way: “There 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.

58 Id. at 3695-97. In fact, the legislative history of the 1984 specifically cites to the movie War Games as a realistic depiction of the ability of hackers to cause widespread damage simply by gaining unauthorized access to secure networks. Id. at 3696. In War Games, Matthew Broderick plays a high-school student who uses a 1970s-vintage computer and modem to unwittingly hack into a top-secret military supercomputer, nearly starting a war with the Soviet Union. War Games (Metro-Goldwyn-Mayer 1983).

59 Pub. L. No. 98-473, 98 Stat. 2190, reprinted in 1984 U.S.C.C.A.N. 3689, 3692 (“[T]he 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. 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.”).
In sum, the history of the 1984 Act is important because it illustrates a realization by legislators that if they were going to criminalize conduct that many people did not perceive to be illegal, they had to do so via new legislation rather than by shoehorning instances of computer crime into existing wire and mail fraud statutes. A new piece of legislation, appropriately tailored to the crime Congress sought to prevent, would put the public on notice that hacking was wrong and would be punished.\(^{60}\) As noted in part IV, infra, we are presented with a similar attitudinal problem today. Though the 1984 Act has faded into the background, the lessons it teaches about applying old law to a new crime have not.

3. \textit{Section §1030(a)(2)(C) of the CFAA}

At bottom, § 1030(a)(2)(C) is a theft provision – it punishes people who steal private and confidential data. 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. . . .”\(^{61}\) Therefore, the “crux of the offense” is “abuse of the computer to obtain [intangible] information.”\(^{62}\)

\(^{60}\) See S. Rep. 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 computers to the law enforcement community, those who own and operate computers and those tempted to commit crimes by unauthorized access to computers. Rather than having to ‘boot-strap’ enforcement efforts against computer crime by relying on statutory restrictions designed for other offenses, the [CFAA] set forth in a single statute computer related offenses.”).


\(^{62}\) Id. at *7-*8.
Therefore, 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 exceeded authorized access), and 3) that the defendant obtained information from a protected computer. At first, this subsection seems to encompass a wide range of computer use. “Protected computer” has essentially been construed to mean any computer at all, 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.

In addition, §1030(a)(2)(C) is a subsection of §1030(a)(2), and therefore must be read within the context of that section. Congress has noted that “the premise of [1030(a)(2)] is privacy protection.” Indeed, the whole point of adding (a)(2)(C) to the CFAA in 1996 was to

---

63 E.g., United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007).
64 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 54, at 2166 (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. Former Vice President Protection Act, Pub. L. 110-326, 112 Stat. 3560, Title II, § 203 (2008).
65 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 (E.D. Pa. July 13, 2007), at *3) (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. 99-432 at *6 (1986), reprinted in 1986 U.S.S.C.A.N. 2479, 2484.
66 S. Rep. 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.”
“increase protection for the privacy and confidentiality of computer information.”67 This focus on privacy is 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.”68 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 transport the data off the protected computer.69 Congress noted that this rationale was “critically important because, in an electronic environment, information can be stolen without asportation.”70

There are two things to note about this idea of “privacy protection” under the CFAA for purposes of the Lori Drew prosecution: First, it explains the presence of the terms “without authorization” and “exceeds authorized access” in the Act: 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.

E. 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 public computer networks. Rudimentary examples existed outside of the governmental and financial sectors, but

68 Id.
69 Id.
70 Id. at *8 (emphasis added).
they were confined to academia and other private institutions.\textsuperscript{71} The World Wide Web (the foundational basis for the Internet) was not established until 1991, and did not kick into high gear until the mid-1990s, when providers such as AOL, Prodigy, and CompuServe began offering Internet service to members of the public.\textsuperscript{72}

However, unlike the private networks from which the Internet originated, this new concept of “cyberspace” was thought to be very public – the “modern equivalent of the Western Frontier,” where users could roam freely without limitations or consequence.\textsuperscript{73} But as in the West, computer users soon settled down and began to stake claims to cyber-territory, essentially reinvigorating the idea of online private space.\textsuperscript{74} The question, then, is twofold: First, in what ways can computer users protect the information they store on their computer networks and websites from public access? And which ways should the law recognize as legitimate? Several legal scholars have suggested that there are two different ways in which a computer owner may protect the information she stores on it: code-based protections and contract-based protections.

\textsuperscript{71} 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’s Internet Learning Center, A Brief History of the Internet, khttp://www.walthowe.com/navnet/history.html (last visited Mar. 12, 2009).
\textsuperscript{72} Id.
\textsuperscript{74} Hunter, \textit{supra} note 73, at 443.
1. **Code v. Contract-Based Protection**

Code-based protection is essentially technical barriers to access that the computer owner programs by code into the computer software. Typical code-based “gatekeepers” include password protection, or a routing system that directs every would-be user to a main login page. Code-based protection would also certainly include internal networks such as company intranets. The purpose of code-based protection is 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). 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. The key point is that technical code-based protection measures “actually have to control access to some degree,” as opposed to simply indicating the permissible limits of access to a computer or website. 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.

By contrast, a computer owner may control access by contract. Essentially, she posts terms and conditions to which a user must agree before he is “permitted” to use the computer or the website. Common examples would be 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

---

75 Kerr, *supra* note 42, at 1644; Bellia, *supra* note 54, at 2212.
76 Bellia, *supra* note 54, at 2212.
77 *See* Kerr, *supra* note 42, 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 . . . ”).
78 Bellia, *supra* note 54, at 2212.
user must affirmatively agree before she is granted access.\textsuperscript{80} The key difference, however, is that unlike code-based protection, contract-based protection is not coded into the computer system by any technical means. Instead, contract-based protection works “on the honor system, or perhaps more accurately, the honor system backed by contract law remedies.”\textsuperscript{81}

Because of these distinctions, some commentators view code-based measures (such as encryption of e-mail, for example), as a “strong” version of protection of information on computers – one that may even trigger Fourth Amendment protection.\textsuperscript{82} The reasoning is 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.”\textsuperscript{83} Either way, an unauthorized user must take extraordinary, and often illegitimate, measures to gain access to a code-based site, giving the site’s owner reasonable assurance that her private contents will remain safe from prying eyes.

No such affirmative protection exists with regulation of websites by contract. A user may explicitly disagree with a term of use that says, “this site is private, and access is conditioned

\textsuperscript{80} Kerr, \textit{supra} note 42, at 1645.
\textsuperscript{81} Id. at 1646.
\textsuperscript{82} See, e.g., Michael Froomkin, \textit{The Metaphor is the Key: Cryptography, the Clipper Chip, and the 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). \textit{But see} Orin S. Kerr, \textit{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 Note 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.” \textit{Id.} at 529.
\textsuperscript{83} Kerr, \textit{supra} note 82, at 504.
upon your agreement to not reveal any information contained herein,” and still be granted access to the website if she clicks “I agree.” The point that is salient to the Lori Drew prosecution is that code-based measures are far more effective at protecting private information than regulation by contract, and Lori Drew was charged under § 1030(a)(2)(C) – the provision of the CFAA that protects 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. For example, 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. 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 simply 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.

---

practical effect of such a system is that anybody at all – Lori Drew, “Josh Evans,” or Grendel, 
the monster from Beowulf\textsuperscript{85} - can establish a MySpace profile.

In fact, MySpace explicitly acknowledges that the content on its site is \textit{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).”\textsuperscript{86} In other words, protecting personal information is up to the 
user, not MySpace.\textsuperscript{87} Such a system is simply not code-based protection.\textsuperscript{88} 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] . . . .”\textsuperscript{89} Lori Drew may have lied to 
gain access to MySpace, but the system is “technically configured” to allow her use - as well as 
the use of 246 million others.

\textsuperscript{85} MySpace Profile of Grendel, 
http://profile.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=5272436 (last 
visited Mar. 12, 2009).

\textsuperscript{86} MySpace Safety Tips and Settings, General Tips, 
(last accessed Mar. 12, 2009).

\textsuperscript{87} 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), \textit{aff’d} by Doe v. MySpace, 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).

\textsuperscript{88} Kerr, supra note 42, 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.”). \textit{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).

\textsuperscript{89} Bellia, supra note 54, at 2248.
With this code-based versus contract-based dichotomy in mind, this Note 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

Assume that Lori Drew, before she registered her MySpace account, read the Terms of Use that govern use of the website – including the provisions cautioning against misrepresenting one’s identity and harassing other MySpace users – realized that her scheme would violate those terms, and clicked “I agree” anyway. Having established intent, the question now becomes whether her continued access of the MySpace server is “without authorization” or “in excess of authorization.”

90 This is a considerable assumption given the stated facts of the Drew case. As noted above, §1030(a)(2)(C) requires intent to access a computer without authorization – that is, it must have been Lori Drew’s conscious object to violate MySpace’s Terms of Service. See note 65, supra (noting that Congress intended to proscribe only intentional acts of unauthorized access). Yet Ashley Grills testified that though Lori Drew was present when Grills registered the MySpace account and agreed to the terms of use, neither woman read them. Scott Glover, Mother Saw MySpace Plan as Clever, Witness Says, L.A. TIMES, Nov. 21, 2008, at B4. It is therefore an uphill battle to impute specific intent to of MySpace’s prohibitions about misrepresenting one’s identity to Lori Drew. However, a few courts have imputed knowledge of website terms of service – at least for purposes of a forum selection clause – to computer users based principles of agency. See, e.g., Abramson v. Am. Online, Inc, 393 F. Supp. 2d 438, 440 (N.D. Tex. 2005) (using apparent authority and ratification to impute knowledge of a forum selection clause in AOL’s Terms of Service to woman whose son had established an AOL account on her behalf). Cf. Motise v. Am. Online, Inc., 343 F.Supp.2d 563, 566 (S.D.N.Y. 2004) (man who used his stepfather’s AOL account was held to be a “sub-licensee” of that account and therefore bound by forum selection clause in AOL’s Terms of Service).
This Note will argue that the government’s prosecution of Lori Drew never should have taken place at the federal level. It will argue that, for purposes of criminal prosecutions under § 1030(a)(2)(C) of the CFAA, a user is “without authorization” only if she circumvents data protection measures that are regulated by computer code, rather than terms of use posted on a website. This interpretation of “without authorization” is consistent with caselaw interpreting the criminal provisions of the CFAA. Further, criminalizing a violation of website’s terms of service would have the disturbing effect of criminalizing the conduct of many everyday users of the Internet – a result that Congress surely did not contemplate in passing the CFAA.

A. “Unauthorized Access” 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,’” 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.” 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 obtain or alter.” It is also clear that the CFAA contemplates a distinction between “insiders” and outsiders: Specifically, outsiders are those to

91 Bellia, supra note 54, at 2234.
92 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n. 10 (1st Cir. 2001)
access a computer “without authorization,” and insiders are those who have some authorized access to a computer but then “exceed” it in some way.94

Yet courts and commentators alike have had a hard time keeping the terms “without authorization” and “exceeds authorized access” separate.95 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.96 The post-verdict fight boiled down to the question of whether Drew’s access to the MySpace servers was “unauthorized,” and therefore the focus of this Note going forward will be to examine how courts have defined “without authorization” in the absence of Congressional guidance.97

B. Judicial interpretations of “without authorization”

Given the lack of statutory guidance on the meaning of “without authorization,” courts have defined the term in various ways. Many of them simply apply the plain meaning of the

95 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.”). See also Kerr, supra note 42, at 1630 (2003) (“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.”).
96 See Drew Indictment, supra note 23 (using the phrase “without authorization and in excess of authorized access” consistently throughout).
97 In any case, proving the greater proves the lesser. Because “without authorization” ostensibly encompasses the conduct of users who have no authority whatsoever to use a protected computer, proving that someone has accessed “without authorization” necessarily also proves access “in excess” of authorized use.
word “authorization,” turning to dictionaries for reference. Second, some courts cite to the Second Circuit’s holding in *United States v. Morris,* which essentially posits 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. Later courts have explained that the scope of a user’s authorization under this “intended function” test turns on “the nature of the relationship established by the computer owner and the user.”

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 “intended function” test in a criminal context, none have extended the contract theory of liability

---

98 *See, e.g., Healthcare Advocates v. Harding, Earley, Follmer, & Frailey, 497 F.Supp.2d 627, 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). The judge in the Lori Drew trial instructed the jury that “access without authorization” means “to access a computer without the approval, permission, or sanction of the computer’s owner.”

99 928 F.2d 504 (2d Cir. 1991).

100 *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 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 Mar. 12, 2009).

to criminal defendants. And equally importantly, all criminal prosecutions under §1030(a)(2)(C) have involved circumvention of code-based protective measures.

1. Contractual Theory of “Unauthorized Access” – Civil Cases

In its brief, the government emphasizes the “great weight of circuit authority holding that contractual terms can identify what is ‘unauthorized’ . . . within the meaning of Section 1030.”\(^{102}\) The “great weight” language aside, the prosecution is certainly correct that growing number of courts have found a user’s access to a computer or website to be “without authorization” for purposes of the CFAA’s civil provisions based on a violation of contract terms.

To understand this broad application of the statute, however, it is first important to understand that the idea of terms of use as binding contracts originated in the world of online contracting.\(^{103}\) 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.\(^{104}\) Generally, courts have found such “clickwrap” agreements can constitute binding contracts.\(^{105}\)

---

\(^{102}\) *Government Response*, *supra* note 98, at 10.


\(^{104}\) See 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 Note.

\(^{105}\) 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).
However, while courts have been willing to enforce online terms of use against entities or companies (often ones who are competitors of the company that runs the website in question), they have been very reluctant to enforce online terms of use against individuals who use the site, often finding that such agreements do not give adequate notice or inquiry notice of significant provisions contained within them.\(^{106}\) That is an important point, considering that the Drew prosecution involves not only an individual who is accused of violating a website’s terms of service, but who also faces criminal liability for it.

In any case, the question of whether terms of service and clickwrap agreements are enforceable as a contract is a separate question from whether violation of them can constitute unauthorized access under the CFAA. Assuming such online contracts are binding upon users, the prosecution is correct that a good number of courts interpreting the CFAA’s civil provisions have held that violation of contract can constitute unauthorized access. However, the bulk of these cases involve anti-competitive behavior between businesses and their employees. For example, a rival company may use some sort of program or code to mine a competitor’s website

\(^{106}\) Lemley, *supra* note 108, at 476 (“One plausible reading of the cases is that courts in browsewrap cases show greater solicitude to consumers than to businesses, and will enforce browsewraps primarily in business-to-business (b2b) rather than business-to-consumer (b2c) transactions.”) See also *iParadigms*, 544 F.Supp.2d at 485 (no knowledge imputed to defendant users of website where plaintiff sought to enforce usage policy that was not part of clickwrap agreement to which defendants agreed, and site did not direct defendants to view usage policy or otherwise indicate it was part of the clickwrap agreement); *Specht*, 306 F.3d at 32 (no knowledge of binding arbitration clause imputed to users who downloaded software from website, because licensing terms were listed at the bottom of webpage, below the download button for the software, and users received no direction or otherwise had reason to scroll to bottom of webpage before or after downloading software). Cf. Campbell v. Gen. Dynamics Gov’t Sys. Corp., 407 F.3d 546, 557 (1st Cir. 2005) (refusing to uphold company’s mandatory arbitration policy against former employee because notice of the change in policy, which was sent via a companywide email that provided an embedded link to the policy on the company’s intranet, did not “state directly that the Policy contained an arbitration agreement” nor “contain anything to put the recipient on inquiry notice of that possibility by conveying the Policy’s contractual significance”).
for valuable data, in violation of a confidentiality agreement or express prohibition not to do so.\textsuperscript{107} Or an employee might quit his job at company A but takes proprietary company information along with him to company B in violation of a confidentiality or non-compete agreement.\textsuperscript{108}

However, the Lori Drew case presents a narrower question: Outside the realm of competing business entities, does violation of a website’s terms of service constitute “unauthorized access”? A few courts have expressly held that violation of a public website’s terms of service can constitute “unauthorized access” under the CFAA. Once such example is \textit{America Online, Inc. v. LCGM, Inc.}:\textsuperscript{109} 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

\textsuperscript{107} \textit{See}, \textit{e.g.}, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001) (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).

\textsuperscript{108} \textit{See}, \textit{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.”). \textit{Citrin} is an example of how some courts have addressed CFAA civil claims against former employees who collect proprietary business information from computers which they are authorized to access, but then provide that information to a competing business. \textit{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 \textit{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 instant he began acting as an agent for the competing entity). This theory of “unauthorized access” has been expressly rejected by some courts as too broad an application of the CFAA. \textit{See, e.g.}, Condux Int’l Inc. v. Haugum, 2008 U.S. Dist. LEXIS 100949 at *12 - *15) (D. Minn. Dec. 15, 2008) (collecting cases rejecting the \textit{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).

thousands of AOL members and transmitted to them nearly 100 million spam emails advertising pornographic websites. 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.”

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, or have dodged the question altogether. 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, the defendants, in the course of intellectual property

110 Id. at 448.
111 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., 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).
112 See Am. Online, Inc. v. National Health Care Discount, 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 noted 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 v. Boardfirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 (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).
113 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 they objected to use of the scraper)
litigation, used the Internet Archive’s Wayback Machine\textsuperscript{115} to view archived copies of Healthcare Advocates’ public website.\textsuperscript{116} 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 to the images.\textsuperscript{117} 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.\textsuperscript{118} 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. . . . The Harding firm accessed the Internet Archive’s website with only an ordinary web browser [and] they did not employ any special tools. . . . 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 [sic] something more than merely using a public website in the manner it was intended to be liable under the CFAA.\textsuperscript{119}

The \textit{Healthcare Advocates} decision is important for two reasons: First, the court recognized that simply 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

\textsuperscript{115} The Wayback Machine is a public, online library of 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. \textit{Id.} at 631.

\textsuperscript{116} \textit{Id.} at 632.

\textsuperscript{117} \textit{Id.} The Wayback Machine allows owners of public websites to opt out of its archiving process, which Healthcare Advocates elected to do. \textit{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. \textit{Id.}

\textsuperscript{118} \textit{Id.} at 646.

\textsuperscript{119} \textit{Id.} at 648-49.
has been given permission to enter – even if the owner of the content did 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 to combat unfair competition or bulk e-mail spamming. And Healthcare Advocates indicates a general reluctance to use § 1030(a)(2)(C) against computer users who are granted free access to a public website. 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 explicitly held that violation of a contract constitutes “unauthorized access” for purposes of the CFAA’s criminal provisions.

2. Contractual Theory of “Unauthorized access” - Criminal Cases

Two circuits – the First and the Fifth – have analyzed CFAA criminal prosecutions in which some sort of user contract was involved. In both cases the contract itself did not ultimately determine the issue of the defendant’s liability. But this gets us right to the very heart of the question in the Lori Drew case – whether violation of a website’s terms of service can trigger criminal liability under the CFAA – so it is worth examining both of these cases in some detail.

The First Circuit, in United States v. Czubinski,\(^{120}\) took on 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”

\(^{120}\) 106 F.3d 1069 (1st Cir. 1997).
duties. Nonetheless, Czubinski knowingly disregarded those rules by browsing the tax returns of various people, including Boston city officials and a former girlfriend. 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.”

On appeal, Czubinski argued that his browsing of tax returns was simply an act of “idle curiosity,” and that the government failed to prove that in doing so he obtained anything “of value.” The First Circuit agreed and reversed Czubinski’s conviction. 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.” The court elaborated no further on this proposition, but it appears that the court was doing more than simply 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 accessor is not entitled so to obtain . . . .” Czubinski 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.

---

121 Id. at 1071, n. 1.
122 Id. at 1071-72.
123 Id. at 1078.
124 Id.
125 Id.
126 Id.
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,\(^{128}\) making its interpretation of “unauthorized access” merely dicta. Second, the IRS database which Czubinski accessed was not accessible to the general public – instead, it was a government computer that contained sensitive personal data. This is a critical point. In many respects, the facts of *Czubinski* are precisely what Congress had in mind when it pictured “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.”\(^{129}\) Put simply, *Czubinski* does not involve a publicly accessible website regulated only by contract, and therefore must be distinguished from the Drew case.\(^{130}\)

The Fifth Circuit also had a chance to address squarely the issue of liability based on contract terms in *United States v. Phillips*,\(^{131}\) but ultimately declined to do so. When Andrew Phillips matriculated at the University of Texas at Austin (UT) in 2001, he signed the

---

\(^{128}\) *Czubinski*, 106 F.3d at 1079. 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.


\(^{130}\) 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 108, *supra*. Professor Kerr argues that *Czubinski’s* brief dicta about exceeding authorized access suggest, as per *Shurgard*, “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 42, at 1634.

\(^{131}\) 477 F.3d 215 (5th Cir. 2007).
University’s standard computer use agreement, which banned, *inter alia*, port scans and other hacking activity. 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. 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.

When the excitement of port scanning had run its course, Phillips then used the information he had collected to launch a “brute force attack” on a secure UT website (“TXClass”) 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. 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. UT spent nearly $200,000 cleaning up the mess and then contacted the Secret Service, whose investigation led to Phillips. Phillips was convicted under § 1030(a)(5) of the CFAA, which makes it a crime to “knowingly [cause] the transmission of a program . . . or command, and as a

---

132 The *Phillips* court described port scanning as the sending of codes or other programs to various computers and networks to detect potential vulnerabilities in those computers - often a prelude to a full-scale hacking attack. *Id.* at 217, n. 1.
133 *Id.* at 217.
134 *Id.*
135 *Id.*
136 Essentially, a hacker launches a “brute-force attack” by collecting thousands of random password 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.
137 *Id.*
138 *Id.*
139 *Id.*
result of such conduct, intentionally causes damage without authorization, to a protected computer.”

Phillips’s primary argument to the Fifth Circuit Court of Appeals was that the Government failed to prove at trial that he had accessed the secure TXClass website “without authorization.” The Phillips court, however, used the Morris “intended function” test to hold that “Phillips’s brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to … data that he was not permitted to view or use.”

Yet that wasn’t the end of the story. Phillips made yet another argument: He claimed 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). However, the Fifth Circuit rejected this argument too, 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, obtain such authorization from UT

\[140\] Id.; §1030(A)(5)(A)(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.”)

\[141\] Id. at 219.

\[142\] Id. at 220.

\[143\] Id. Recall that unlike §1030(A)(2)(C), §1030(a)(5) does not include the language “exceeds authorized access.”
merely by viewing a login page, or clicking a hypertext link.\textsuperscript{144} 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.

Naturally, the prosecution in the Drew case pounced 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.”\textsuperscript{145} But that interpretation is missing a very important caveat: The court’s language in \textit{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 \textit{only} out of a contractual or agency relationship would be absurdly untrue: It ignores the millions of Internet users who are freely “authorized” to peruse public websites with \textit{no} restrictions whatsoever – contractual, code-based, or otherwise. The \textit{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.

And on that note, no court has ever held under the CFAA that obtaining information from a public website with no code-based protection is a crime. The few criminal prosecutions that have been brought under §1030(a)(2)(C) have involved defendants who have stolen proprietary

\textsuperscript{144} \textit{Id.} at 220.
\textsuperscript{145} Government Response, supra note 98, at 7.
In fact, the theme of obtaining information from private databases (as opposed to computer databases or websites open to the general public) persists uniformly throughout all criminal prosecutions under CFAA provisions that have “unauthorized access” as an element – most notably §1030(a)(4) and §1030(a)(5).

See, e.g., United States v. Willis, 476 F.3d 1121, 1123 (10th Cir. 2007) (defendant helped a third party obtain names, addresses, birthdates, and social security numbers from a protected database at a credit collection agency in order to further identify theft scheme); United States v. Johnson, 58 Fed.Appx. 926, 927 (3d Cir. 2003) (defendant accessed Pennsylvania State Police computer system in order to provide fraudulent drivers licenses); United States v. Galietti, 2007 U.S. Dist. LEXIS 80492 at *4 (D. Conn. 2007) (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) (defendant hacked into corporation’s internal network and demanded $10,000 to make the system secure again).

See, e.g., United States v. Green, 428 F.3d 1131, 1132 (8th Cir. 2005) (defendant paid SBC Communications employees to steal the names and social security numbers of SBC customers, which he then used to buy flat-screen TVs on credit); United States v. Soo Young Bae, 250 F.3d 774, 775 (D.C. Cir. 2001) (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) (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) (defendant 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) (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) (unauthorized use of a stolen ATM card and PIN); United States v. Morris, 928 F.2d 504, 505-06 (2d. Cir. 1991) (defendant released a virus onto secure network); United States v. Grooters, 2008 U.S. Dist. LEXIS 48222 at *7 (W.D. Mich. June 24, 2008) (defendant used a non-public database at a federal public defender’s office to obtain personal addresses and social security numbers).

See, e.g., United States v. Heckencamp, 482 F.3d 1142, 1143-45 (9th Cir. 2007) (defendant used 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) (fired employee used home computer to remotely hack into former employer’s internal network and disable the server); Phillips, 477 F.3d at 217 (defendant launched brute-force password attack on secure university website); United States v. Shea, 493 F.3d 1110, 1113-14 (9th Cir. 2007) (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) (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) (former employee retained network access card and used it to
Put another way, the overwhelming bulk of criminal caselaw under the CFAA involves defendants who have circumvented code-based measures on private websites. In the next section, I argue that such an interpretation is consistent with Congressional intent, canons of statutory interpretation, and basic constitutional protections.

IV. Resolution and Recommendation

A. Code-Based Interpretation of Unauthorized Access

When analyzing criminal charges under § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, courts must draw a line in the sand between code-based protection and contract-based protection, and they must stop blurring the line between “without authorization” and “exceeds authorized access.” Furthermore, the idea of websites and public networks is confusing courts. The CFAA was enacted when the Internet was a system of private networks secured by code-based protection. Though the Act has consistently been expanded, Congress has not adequately addressed the public/private dichotomy of the Internet. Therefore, a court analyzing a § access his former employer’s internal computer network system); United States v. Schuster, 467 F.3d 614, 615 (7th Cir. 2006) (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) (defendant used remote radio transmitter to jam computer-controlled emergency response system); United States v. Lloyd, 269 F.3d 228, 231 (3d Cir. 2001) (defendant planted 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) (terminated employee used his retained e-mail account and “switch user” program to gain administrative user access to company’s internal network); United States v. O’Brien, 435 F.3d 36, 37-38 (1st Cir. 1996) (former employee used remote computer to hack into tour company’s internal database and cancel customer reservations); United States v. Sablan, 92 F.3d 865, 866-67 (9th Cir. 1996) (former bank employee, using password she had retained after being fired, accessed bank’s mainframe computer and damaged files therein).
1030(a)(2)(C) criminal charge in which a user has accessed a website to “obtain information” needs to ask a series of questions:

First, is the website private or public? The answer is as simple as the mode of protection: a website – or perhaps more accurately, the part of a website a defendant tried to access - should be defined as “private” if the website owner has erected strong code-based protection measures that affirmatively regulate and control public use of that part of the site. If he has simply stipulated terms of use, or allows free access to his website, 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.149

If the website is private – in other words, if the website’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 website owner. If the computer owner has granted the user at least some right to use the website 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 website owner, or the website owner could have a network administrator responsible for registering authorized users.

149 This does not mean that the CFAA can never apply to public websites. For example, if a hacker uses a remote virus to commandeer control of the New York Times’ online webpage and defiles it with Swastikas and other hate propaganda, he has certainly “accessed” a public website, 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 causing the transmission of a program . . . and, as a result of such conduct, causes damage without authorization, to a protected computer.”
Given a right of access, courts must then determine if the user nonetheless used her authorized access to “obtain or alter information” on the website 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 website owner and the user – taking into consideration things like employee use contracts if necessary.

Finally, if a private website’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 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 Access “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. First, when Congress

---

150 The leading commentators who have proposed a code-based interpretation of the CFAA’s “unauthorized access” provisions have considered this issue but have not hit upon it squarely. Professor Kerr, *supra* note 42, at 1657-63, discusses the implications using a code-based standard of “unauthorized access” under §1030(a)(2)(C), but he does not address whether that
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. 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 a 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].

This fact 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.” Again, the point is that code-based controls on computers drove the entire construction of the CFAA.

interpretation is consistent with Congressional intent. Professor Bellia, supra note 54, at 2255-58, discusses Congress’s intent in passing the CFAA but within the context of her argument of a broad definition of the term “access.”

See Bellia, supra note 57, 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 . . . .”).


The Senate Judiciary Committee gave another example in the 1986 Amendments to the CFAA: “[A government] employee who uses his department’s computer and, without
But even in the CFAA amendments that have been passed since Internet use has become widespread, Congress has never suggested that the Act applies to computers and websites not regulated by code – though it has had ample opportunity to do so. For example, in the 2002 revisions, Congress expressed its concern over “zombie attacks”\(^{154}\) 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.\(^{155}\) And in 2008, Congress strengthened the CFAA to combat the surreptitious placement of spyware on private computers.\(^{156}\) 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.”\(^{157}\) Certainly, one way of doing that is to provide criminal penalties for serious computer crime violations, but

---


\(^{155}\) See H. Rep. 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).


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 security protection measures. Reading a violation of a website’s terms of service as “unauthorized access” arguably discoutrages website owners to use more costly and detailed code-based measures to protect their data.

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 shown its intent to “ensure that the [CFAA] is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime,” and this language has led some courts to conclude that the Act’s provisions should be interpreted broadly. 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.

160 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) (“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.”).
Recognizing that states were free to pass their own computer laws, Congress instead evinced intent to take federal jurisdiction only over computer crimes in which there is a “compelling federal interest.”\textsuperscript{162} As the subsequent expansion of the CFAA’s criminal provisions makes clear, the idea of “compelling federal interest” contemplates either conduct that poses a threat to either national security or the economy, or conduct that violates a user’s privacy interest in data stored on a computer.\textsuperscript{163} The legislative history is rife with examples of malicious computer access that threatens national security or economic interests,\textsuperscript{164} jeopardizes sensitive private financial or personal identifying data,\textsuperscript{165} or has the potential to cause serious physical harm.\textsuperscript{166} By itself, violating a website’s terms of service does none of those things.


\textsuperscript{163} See Reid Skibell, \textit{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.”).

\textsuperscript{164} See, e.g., S. Rep. 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. S23,783 (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”).

Further, courts have consistently warned against interpreting statutes in a manner that criminalizes a broad range of conduct, yet that is precisely what the government’s interpretation of “unauthorized access” in this case threatens to do. As one commentator has pointed out, 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.”

166 See S. Rep. 99-432 at 2-3 (1986), 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); H. Rep. 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).

167 See, e.g., Dowling v. United States, 473 U.S. 207, 228 (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); 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 “while the government’s objective is a laudable one . . . its interpretation of the wire fraud statute would serve to criminalize the conduct of . . . 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.”).

168 Kerr, supra note 42, at 1650-51. This notion is also the basis for Drew’s pre-trial motion to dismiss on grounds of improper prosecutorial delegation. Citing a line of U.S. Supreme Court Commerce Clause cases (Carter v. Carter Coal Co., 298 U.S. 238 (1938); A.L.A. Schechter Poultry Co. v. United States, 295 U.S. 495 (1935); Panama Refining Co. v. Ryan, 293 U.S. 388 (1935)) for the proposition that broad, standardless grants of governmental enforcement power to agencies can violate the Constitution, Drew argued that the government’s read of §1030 had the effect of delegating prosecutorial power to private citizens. Mot. to Dismiss Indictment for Vagueness at 6, United States v. Drew, CR-08-582-GW (C.D. Cal. July 23, 2008), available at http://burningbird.net/docs/drewvague.pdf. In particular, Drew argued that “like the [Commerce Clause cases], there are no standards for computer owners when setting up TOS’s. At the same time, however, these owners now have the power to set guidelines, rules and terms that can, if violated, cause criminal liability. Such power, by the government’s interpretation of §1030, is now in the hands of . . . anyone . . . [who] can get on the Internet and set up a rudimentary Website.” Id. at 6-7.
In enacting the CFAA, Congress simply 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

Finally, two fundamental principles of statutory construction cut strongly against the government’s interpretation of §1030(a)(2)(C) in the Drew case. One was raised by Drew herself in a pre-trial motion: If the government’s read of “unauthorized access” is correct, then the statute is void on vagueness grounds because it fails to provide clear notice to ordinary people of precisely the conduct it prohibits.\(^\text{169}\) 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,\(^\text{170}\) which ostensibly makes it difficult for a user to know whether she is in compliance with all terms at all times.

\(^{169}\) Id. at 6; City of Chicago v. Morales, 527 U.S. 41, 55 (1999). See also 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”);

\(^{170}\) See, e.g., MySpace Terms, supra note 19 (“MySpace may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace on the MySpace Website. Your continued use of the MySpace Services after MySpace posts a revised Agreement signifies your acceptance of the revised Agreement.”).
With regard to the issue of vagueness, it is critically important to remember why the CFAA was passed in the first place. Recall that Congress was fundamentally concerned about two things: First, the inability of the existing wire and mail fraud statutes to directly capture nascent hacking activity, and – just as importantly – the public misperception at the time that computer hacking was simply harmless pranksterism.\textsuperscript{171} In what is perhaps the definitive reason for enacting a new computer crime law, the 1984 Act’s legislative history states: “The [Senate Judiciary] 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.”\textsuperscript{172}

Today, as in 1984, we are faced with a “tremendous attitudinal problem.”\textsuperscript{173} In our current online world, self-sharing, voyeurism, and deception are often the norm in public social networking communities like MySpace,\textsuperscript{174} 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.”\textsuperscript{175} 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. Therefore, absent plain and unmistakable Congressional intent to impute criminal

\begin{itemize}
  \item \textsuperscript{171} See note 60, supra, and accompanying text (noting Congress’s concern with the rather cavalier public attitude towards computer crimes).
  \item \textsuperscript{173} Id. at 3697.
  \item \textsuperscript{174} 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.”).
  \item \textsuperscript{175} See, e.g., Mattathias Schwartz, The Trolls Among Us, THE NEW YORK 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).
\end{itemize}
liability to computer users who violate a website’s terms of service, courts should refrain from interpreting the CFAA in such an expansive manner.176

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 defendants177 - a proposition that some courts interpreting “without authorization” under the CFAA have rightly heeded.178 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 . . . . The fact that this Court now addresses the CFAA in a civil context does not withdraw the necessity of applying the rule of lenity.”179

V. CONCLUSION

176 E.g., United States v. Wiltberger, 5 Wheat. 76, 95 (1820) (“It is the legislature, not the court which is to define a crime, and ordain its punishment”); 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.”).

177 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. . . . 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).

178 See, e.g., Condux Intl. Inc. v. Haugum, 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 statute, it is required to construe the statute in favor of the defendant.”); Shamrock Foods v. Gast, 535 F.Supp.2d 962, 967 (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).

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.\footnote{See Joel Currier, Gov. Blunt Signs Law Against Cyber-Bullying, ST. LOUIS POST-DISPATCH, July 1, 2008, at D3.} 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].”\footnote{MO. REV. STAT. § 565.090 (2008).} Other states have quickly followed Missouri’s lead in passing similar anti-cyberbullying statutes.\footnote{See usatoday.com, State Action on Cyberbullying, \url{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).}

Courts, however, must resist the urge to vastly expand the reach of the CFAA 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

\footnote{Even more notably (and perhaps as 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 (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, \url{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.”183 Millions upon millions of Internet users are counting on it.

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