JENNIFER STISA GRANICK (California Bar No. 168423)
jennifer@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Fax: (415) 436-9993 (fax)

PHILLIP R. MALONE (California Bar No. 163969)
pmalone@cyber.law.harvard.edu
CYBERLAW CLINIC
BERKMAN CENTER FOR INTERNET AND SOCIETY
HARVARD LAW SCHOOL
23 Everett Street
Cambridge, MA 02138
Telephone: (617) 384-9134

Amici Curiae

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES, Plaintiff, v. LORI DREW Defendant.	Case No. CR-08-0582-GW **BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ET AL., IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS INDICTMENT FOR FAILURE TO STATE AN OFFENSE AND FOR VAGUENESS** Date: September 4, 2008 Time:. 8:30 AM Honorable Judge George H. Wu

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

LEGISLATIVE MATERIALS

INTERNET SOURCES

STATEMENT OF INTEREST OF *AMICI CURIAE*

Amici are three organizations, the Electronic Frontier Foundation, the Center for Democracy and Technology and Public Citizen, and the 14 individual faculty members listed in Appendix A who research, teach and write scholarly articles and books about internet law, cybercrime, criminal law and related topics at law schools nationwide. None received any compensation for participating in this brief. *Amici's* sole interest in this case is in the evolution of sound and principled interpretation and application of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C). *Amici* believe that this brief will assist the Court in its consideration of the proper interpretation and application of the CFAA in this case.

Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights. As part of that mission, EFF has served as counsel or *amicus* in key cases addressing privacy issues and rights as applied to the Internet and other new technologies. With more than 13,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

Center for Democracy & Technology ("CDT") is a non-profit public interest and Internet policy organization. CDT represents the public's interest in an open,

decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. In particular, CDT works to protect online free speech, including the right to speak anonymously and to engage in robust communication and debate without inappropriate threats of criminal sanctions.

Public Citizen is a non-profit, public interest organization that has defended the rights of citizens and consumers since its founding in 1971. Public Citizen has stood against the enforceability of abusive terms in one-sided contracts of adhesion and strongly rejects the proposition that criminal liability should attach to violations of contractual fine print. Since 1999, Public Citizen has also defended the First Amendment right of citizens to communicate anonymously in online forums without the threat of unjustified liability.

FACTS AND SUMMARY OF THE ARGUMENT

Defendant Lori Drew is a Missouri resident charged in the Central District of California with violating the Computer Fraud and Abuse Act ("CFAA"). The Government alleges that in the fall of 2006, Defendant created a MySpace account under the name of "Josh Evans." Indictment, *United States v. Drew*, No. 08-00582, 6 (C.D. Cal. May 15, 2008). Through the "Josh Evans" account, Defendant communicated and developed an online relationship with Megan Meier, a 13-year-old girl also living in Missouri. Indictment at 6. At some point during their communications "Josh Evans" said hurtful things to Miss Meier. *Id*. at 7-8. Tragically, Miss Meier took her own life.

There are state and federal statutes that regulate harassing and otherwise harmful speech, carefully identifying speech that falls outside of First Amendment protection. *See, e.g.,* 47 U.S.C. § 223(a)(1)(C); R.S.Mo. 565.090 (former).[1] Neither of those statutes appears to criminalize the communications from "Josh Evans" to Miss Meier here. In the absence of applicable First Amendment-compliant criminal statutes, the Government has chosen to indict Defendant for violating the CFAA, 18 U.S.C. § 1030(a)(2)(C), and for conspiring to violate it. The Government theory is that Defendant's use of a fictitious name and registration information and her hurtful speech violated the MySpace terms of service (TOS). *See Terms and Conditions – MySpace.com,* http://www.myspace.com/index.cfm?fuseaction=misc.terms (last modified Feb. 28, 2008). Defendant allegedly failed to provide truthful and accurate registration information; failed to refrain from using any information obtained from MySpace services to harass, abuse, or harm other people; failed to refrain from soliciting personal information from anyone under 18; failed to refrain from

[1] The Missouri legislature amended the statute following this case in recognition that the laws in effect at the time would not prohibit the conduct alleged here. The new statute, which requires proof of intent to do harm to another (as the First Amendment requires), may or may not criminalize Defendant's alleged conduct.

promoting information that she knew was false or misleading; and failed to refrain from posting photographs of other people without their consent, all in violation of the terms of use. Indictment at 6-7. On the Government's view, account holders who use their MySpace accounts in violation of the TOS are accessing the company servers "without authorization" or "in excess of authorization." In this way, Defendant victimized MySpace when "Josh Evans" did not follow its terms of service.

The Government's novel and unprecedented response to what everyone recognizes as a tragic situation would create a reading of the CFAA that has dangerous ramifications far beyond the facts here. Terms of service include prohibitions both trivial and profound. As detailed in examples below, the Government's theory would attach criminal penalties to minors under the age of 18 who use the Google search engine, as well as to many individuals who legitimately exercise their First Amendment rights to speak anonymously online. This effort to stretch the computer crime law in order to punish Defendant Drew for Miss Meier's death would convert the millions of internet-using Americans who disregard the terms of service associated with online services into federal criminals. Indeed, survey evidence shows that the majority of teenage MySpace users have entered at least some false information into MySpace, and would thus be subject to prosecution under the Government's theory. Pew Internet & American Life Project, *Teens, Privacy and Online Social Networks: How teens manage their online identities and personal information in the age of MySpace*, 23-24, http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (Apr. 18, 2007). In fact, child safety advocates like the Child Exploitation and Online Protection Centre of the British government specifically encourage children to protect themselves by providing misleading identifying information instead of real names on social networking sites. *See* Child Exploitation and Online Protection Centre, *Thinkuknow: Social Networking,*

http://www.thinkuknow.co.uk/(X(1)S(z4uckb3yrpokhbemgzsglhm2))/8_10/control/social.aspx (last visited July 31, 2008) ("It's a good idea to use a nickname rather than your real name."). To the best of amici's knowledge, never before in the 22-year history of the CFAA has a criminal prosecution been based on such a theory.

The case is reminiscent of *United States v. LaMacchia*, 871 F.Supp. 535 (D. Mass. 1994), where the district court rejected a Government attempt to stretch the scope of the federal wire fraud statute, 18 U.S.C. § 1343, to cover the unauthorized, non-commercial distribution of copyrighted software products over the internet by an MIT student. At the time, copyright law did not contain criminal provisions against non-commercial infringement. Noting that the key question was whether, metaphorically, "new wine can be poured into an old bottle," *id*. at 536, the court recognized that:

> [w]hat the Government is seeking to do is to punish conduct that reasonable people might agree deserves the sanctions of the criminal law. . . . While the Government's objective is a laudable one, particularly when the facts alleged in this case are considered, its interpretation of the wire fraud statute would serve to criminalize the conduct of not only persons like LaMacchia, but also the myriad of home computer users who succumb to the temptation to copy even a single software program for private use.

Id. at 544.[2]

The case is also reminiscent of *United States v. McDanel*, prosecuted by this same United States Attorney's office under a different provision of the CFAA before

[2] *Accord United States v. Czubinski*, 106 F.3d 1069, 1079 (1st Cir. 1997) (reversing CFAA and fraud convictions for browsing through IRS files but not sending or obtaining any information, the court added "a cautionary note. The broad language of the mail and wire fraud statutes are both their blessing and their curse. They can address new forms of serious crime that fail to fall within more specific legislation. . . . On the other hand, they might be used 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. The case at bar falls within the latter category.")

the Government admitted error on appeal and moved to overturn the defendant's conviction. *See United States v. McDanel*, Government Brief, attached as Exhibit A, at 6, 8. In *McDanel*, the Government stretched the definition of "harm to the integrity" of a computer system to cover truthful reports about a security vulnerability that could endanger a customer's private communications.

The Government's proposed interpretation of the CFAA in this case is a similar stretch, one that is unsupported by case law or Congressional intent, is overbroad and unconstitutionally vague, and would punish constitutionally protected activities. This Court should reject the unwarranted expansion of the CFAA and dismiss the indictment.

I. THIS COURT SHOULD DISMISS THE COMPUTER FRAUD AND ABUSE ACT CHARGES AGAINST DEFENDANT DREW BECAUSE HER ALLEGED VIOLATION OF THE MYSPACE TERMS OF USE DOES NOT CONSTITUTE "UNAUTHORIZED ACCESS" OR "EXCEEDING AUTHORIZED ACCESS" UNDER THE STATUTE

A MySpace account holder does not gain unauthorized access or exceed authorized access to MySpace servers by disregarding conditions set forth in that service's terms of service (TOS). The CFAA criminalizes unauthorized access to a computer system or to information on the system. Both the plain language of the statute and the legislative history show that the statute is meant to punish trespassers and "hackers," not users who ignore or violate sites' contracts or customers who misuse the service.

A. By Its Plain Terms, The Computer Fraud And Abuse Act Prohibits Trespass And Theft, Not Mere Contractual Violations Of Terms Of Use

The fundamental question in this case is when access to a highly popular, everyday web site is "without authorization" or in excess of authorized access.[3] The

[3] Another issue is whether the Government must plead and prove that Defendant intended that her access be unauthorized, or merely that she intended to access, and the access also happened to be unauthorized. Criminalizing unintentional computer

plain language of the CFAA does not criminalize an account holder's use of a computer in violation of TOS, but rather a trespasser's access to computer systems or areas of computer networks without permission. In other words, the statute prohibits trespass and theft, not improper motive or use. Every exercise of statutory interpretation begins with an examination of the plain language of the statute. *Christensen v. C.I.R.,* 523 F.3d 957, 962 (9th Cir. 2008) (Courts look to the plain language of a statute, and to legislative history). The Government charged Defendant with 18 U.S.C. 1030 (a)(2)(C), which states:

> (a) Whoever-- …(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--…(C) information from any protected computer if the conduct involved an interstate or foreign communication; …shall be punished as provided in subsection (c) of this section.

Although Congress did not define the phrase "without authorization," it did so for the phrase "exceeds authorized access". The term "exceeds authorized access" means: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2008).

The plain language of the statute prohibits trespass, either by outsiders who have no rights to the computer system, or by "insiders" who have some rights to access the computer system, but have limited rights to access or alter information on that same system. The Indictment in this case does not allege whether the defendant's access to the MySpace service was "without authorization" or "in excess of authorized access" or both. Regardless, both prongs of 1030(a)(2)(C) are straightforward prohibitions against computer trespass. The first covers outsiders who have no rights to the computer system, and the second covers "insiders" who have some rights to access the computer system, but do not have rights to access or alter certain files or information on that same system. If the computer owner gives

---

trespass raises serious due process problems, but *amici* do not take up that issue here.

the user the ability to access to particular information, then the user does not exceed his authorization by accessing that information, regardless of the purpose or manner of such access. *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, *5 (M.D. Fla. Aug. 1, 2006) (plain reading of "exceeds authorized access" means "those [who go] *above* [their] authorization, meaning those that go beyond the permitted access granted to them – typically insiders exceeding whatever access is permitted to them"). The plain language of Section 1030(a)(2) targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Shamrock Foods v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (citing *Brett Senior & Assocs., P.C. v. Fitzgerald,* 2007 WL 2043377 (E.D. Pa. July 13, 2007)).

B. The Legislative History Supports The View That The CFAA Prohibits Trespass And Theft, Not Improper Motive Or Use.

The legislative history confirms that Congress intended the CFAA to criminalize intruders who trespassed on computers and computer networks. *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 495-96 (D.Md 2005) (citing S. Rep. No. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482 (explaining that the CFAA "is a consensus bill aimed at deterring and punishing certain 'high-tech' crimes")). The CFAA was originally called the Counterfeit Access Device and Computer Fraud and Abuse Act and was enacted in 1984. Counterfeit Access Device and Computer Fraud and Abuse Act, Pub. L. No. 98-473, Title II, § 2102(a), 98 Stat. 1937 (1984) (prior to 1986 amendment). The 1984 House Committee emphasized that "section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense." H.R. Rep. No. 98-894 at 20 (1984) *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706. Consequently, the committee report emphasized concerns about "hackers" who "trespass into" computers and the inability of "password codes" to protect against this threat. *Id. at*

10-11, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695-97. The 1984 version of the law criminalized actions of one who gains "unauthorized access" or who "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."

In 1986, Congress deleted the part of the statute that prohibited those with authorization from using the system for unauthorized purposes and substituted the phrase "exceeds authorized access." *Werner-Masuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (quoting S. Rep. No. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486). As the court in *Werner-Masuda* explains:

> By enacting this amendment, and providing an express definition for "exceeds authorized access," the intent was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,'" thereby "removing from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.

Id. at 499 n.12 (quoting S. Rep. No. 99-432, at 21, 1986 U.S.C.C.A.N. 2479, 2494-95) (alterations in original). Congress used the "exceeds authorized access" language to avoid extending criminal liability to employees where administrative sanctions were more appropriate. *Id.*

This intention is further supported by the fact that, when discussing the CFAA, and specifically section (a)(2)(C), legislators often referred to "hackers" and the need to protect sensitive information from theft. *See, e.g.,* 142 Cong. Rec. E1621-03 (daily ed. Sept. 17, 1996) (statement of Rep. Goodlatte); *see also* 141 Cong. Rec. S9423 (daily ed. June 29, 1995) (statement of Sen. Leahy). The modern, conventional usage of "hacker" is usually someone who gains unauthorized access to a computer typically to obtain information of value he or she is not entitled to obtain, or to cause damage. *See, e.g., Oxford English Dictionary*, Oxford Univ. Press (defining, *inter alia*, a hacker as "a person who uses his skill with computers to try to gain unauthorized access to computer files or networks"); *see also United States v.*

Riggs, 739 F. Supp. 414, 423-24 (N.D. Ill. 1990) (citing approvingly to sources that define hackers as those using computer skills to gain unauthorized access to a computer system). The legislative history makes no mention of unauthorized or excessive access obtained through ignorance or disregard of private terms of service.

The legislative history supports the conclusion that the CFAA criminalizes trespasses in which the user gains access to computer services or information to which he is not entitled, not those in which an authorized individual uses the services or information in an impermissible manner. Defendant Drew had an account on MySpace, a free interactive internet-based social network open to anyone who signs up for the service. There are no fees, no vetting, no checks on who may use the service. Usernames and passwords are deployed, not to keep people off MySpace, but to give users control over their own account profiles and keep such profiles separate. Defendant Drew allegedly used her account to access MySpace services and information. She had no special skill with computers and did not circumvent any security measures, technological or otherwise. As is any member of the public who signs up and holds an account, she was authorized to use the service and to access the system, including information stored there. The way she used her account, if the allegations are true, was reprehensible. But unless her hateful speech rises to the level of harassment or stalking, it is not criminal and cannot be punished; attempting instead to punish that speech under the CFAA merely because it took place on the internet in contravention to a private terms of service is improper.

C. Courts Are Justifiably Wary Even Of Civil Enforcement Of Website Terms Of Service

Adopting the erroneous view of the CFAA propounded by the prosecution in this case would criminalize the actions of internet users or web service account holders who violate a mere contractual promise to use a computer in a certain way or who ignore or disregard terms of service hidden behind a "legal notices" hyperlink at the bottom of a webpage. As detailed in Section III.A, *infra*, many, perhaps most,

internet users do not even read or understand these documents, which are often long, riddled with legalese, and poorly organized and formatted or typically are written at a level of difficulty that exceeds the ability of most consumers to understand. *Accord* Robert W. Gomulkiewicz, *Getting Serious About User-Friendly Mass Market Licensing for Software*, 12 Geo. Mason L. Rev. 687, 692-94, 701-02 (2004); Alan M. White & Cathy Lesser Mansfield, *Literacy and Contract*, 13 Stan. L. & Pol'y Rev. 233, 235-42 (2002). Significantly, the Government in this case has not alleged that the Defendant or co-conspirators ever read or even looked at the MySpace terms, but only that the terms "were readily *available*" to users "who *could* click on a link titled 'Terms of Service' or 'Terms' to be directed to a web page where [they] *could* review those rules." Indictment at 4 (emphasis added).[4]

Indeed, the current prosecution would impose criminal liability for merely ignoring or violating terms of service at a time that courts and academics continue to debate the extent to which and under what circumstances such documents should be enforced as a matter of regular civil contract law. *See, e.g.,* Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 462-63, 475-76 (2006) (citing cases and noting differences in enforceability between corporate-entity defendants and individuals). Among the thorny issues that are presented by such cases are whether the user receives adequate actual or constructive notice of the terms, whether the user effectively consents and whether the terms are unconscionable. Whatever the merits of recognizing private, civil contract obligations and remedies in such situations, however, the imposition of serious criminal liability in light of these problems would be fundamentally unfair.

[4] This failure to allege that Defendant had any actual notice or awareness of the terms of service, her violation of which allegedly constitutes the sole basis for "unauthorized" use and criminal CFAA liability, would appear to undermine the sufficiency of the indictment, given Section 1030 (a)(2)(C)'s requirement that one "intentionally" access a computer without authorization or exceed authorized access, However, *amici* do not focus further on this issue.

D. Imposing Criminal Liability For Ignoring Or Violating Terms Of Service Would Be An Unprecedented, Extraordinary And Dangerous Extension Of Federal Criminal Law

George Washington University Law Professor Orin Kerr has argued thoughtfully and persuasively that "unauthorized access" should not include access to a computer in violation of a contract or terms of service. Doing so would:

> threaten a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace. Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers, broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web.

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1599 (2003). Consider the remarkable and disturbing results that a contract-based approach to authorized access can create under the CFAA:

> Imagine that a website owner announces that only right-handed people can view his website, or perhaps only friendly people. Under the contract-based approach, a visit to the site by a left-handed or surly person is an unauthorized access that may trigger state and federal criminal laws. A computer owner could 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. By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner.

Id. at 1650-51.

Professor Kerr's concerns are not merely hypothetical. There are many surprising terms of service provisions that, if violated, would convert authorized users into federal criminals. Take for example, two of the internet's most popular websites' terms of service:

- "You may not use the Services and may not accept the Terms if (a) you are not of legal age to form a binding contract with Google," *Google Terms of Service*, § 2.3, http://www.google.com/accounts/TOS (last modified Apr. 16, 2007).

- "[Y]ou agree to . . . provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ("Registration Data") . . . [and] maintain and promptly update the Registration Data, and any other information you provide to Company, to keep it accurate, current and complete . . . ." *Facebook Terms of Use,* http://www.facebook.com/terms.php (last modified June 7, 2008).

On the Government's view, a user who is under the age of majority violates the CFAA every time she enters a search query on the Google.com webpage and obtains information. Under Facebook's terms of use, if a user changes jobs or addresses or even her thoughts on what her favorite movie is, she would need to immediately tell Facebook, as this is information she has provided to the company, or run the risk that her continued use of the site could lead to criminal sanctions.[5]

In another example, the Electronic Frontier Foundation reports that terms of service for the popular dating site Match.com require users of either the website or the dating service to be single or separated from their spouses. *See, e.g., Match.com Terms of Use Agreement,* http://www.match.com/registration/membagr.aspx ("You must be at least eighteen (18) years of age and single or separated from your spouse to register as a member of Match.com or use the Website.") (last visited July 30, 2008). The brief's author has not been able to visit the site to confirm the report; because she remains happily married, doing so would be a violation of the site's terms, potentially a criminal act under the interpretation of the CFAA advanced by the Government here.

---

[5] It is of no import that the Government might not bring these cases. The inability to distinguish in a meaningful and principled way between the terms of service violations of the Defendant here and the myriad other similar violations of terms like those of MySpace or Facebook that occur every day starkly reveals the unconstitutional vagueness and potential for arbitrary enforcement the statute would suffer under the Government's interpretation. *See* Section III, *infra*. Moreover, because the CFAA provides for a civil cause of action, the Government's interpretation would enable Google and Facebook and any other affected web site owner to bring suit.

E. The Better View, Supported By More Recent Cases, Rejects CFAA Liability For Authorized Users Acting Outside the Terms and Conditions of That Authorization

Professor Kerr's concern about applying the CFAA to contract violations followed holdings by several courts in civil cases that a disloyal employee's use of a computer or a competitor's automated searching of a system for commercial purposes could violate the statute. However, the more recent and better view, consistent with Kerr's well-reasoned analysis, rejects the idea that authorized access becomes unauthorized, and thus criminal, when the user acts with his own purposes, rather than those of the computer owner, in mind. *See, e.g.*, *Werner-Masuda*, 390 F. Supp. 2d at 495-96; *Brett Senior & Assocs.*, 2007 WL 2043377; *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); *Lockheed Martin Corp.*, 2006 WL 2683058. This better view rejects CFAA liability even where the defendant is a former employee violating a negotiated employment contract or confidentiality agreement by transferring confidential information to a rival company for the employee's own economic benefit and to the detriment of the computer owner. The instant case is a far easier one: all that is alleged here is that the defendant violated the standard MySpace service terms of use, and did so without any purpose to gather trade secrets or commercial or proprietary data, or to gain any economic advantage.

1. More Recent, Better-Reasoned Cases Adopt A Narrower View Of "Exceeding Authorized Access"

The better-reasoned cases hold that if a user is authorized to access a computer and information stored there, then doing so is not criminal, even if that access is in violation of a contractual agreement or non-negotiated terms of use. For example, in *Werner-Masuda* the plaintiff argued that the defendant, a union officer, exceeded her authorization to use the union computer when she accessed a membership list to send to a rival union, and not for legitimate union business. The defendant had signed an agreement promising that she would not access union computers "contrary to the

policies and procedures of the [union] Constitution". *Werner-Masuda,* 390 F. Supp. 2d at 495 (D. Md. 2005). The District Court rejected this argument, holding that even if the defendant breached a contract, that breach of a promise not to use information stored on union computers in a particular way did not mean her access to that information was unauthorized or criminal.

> Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the [Stored Communications Act] or the CFAA. . . . Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it. . . . Nor do [the] terms [of the Stored Communications Act and the CFAA] proscribe authorized access for unauthorized or illegitimate purposes. (citations omitted)

Id. at 499.

Here, too, the gravamen of the Government's complaint is not that Defendant improperly obtained information to which she was not entitled on the MySpace servers, but rather that she used the MySpace service for an unauthorized or illegitimate purpose. The CFAA does not proscribe authorized access for unauthorized or illegitimate purposes. Thus, to the extent that Defendant may have breached the Terms of Service by using a MySpace account contrary to the policies established by the company, it does not follow that she was not authorized to access the MySpace servers in violation of the CFAA.

Subsequent cases have followed the reasoning of *Werner-Masuda* based on either plain language or legislative history. In *Lockheed Martin Corp.* the court found no CFAA violation under the plain language of the statute. "Exceeds authorized access," the opinion states, refers to those employees "that go beyond the permitted access granted to them – typically insiders exceeding whatever access is permitted to them." *Lockheed Martin Corp.,* 2006 WL 2683058, at *5.

In *Diamond Power Int'l, Inc. v. Davidson*, the District Court similarly rejected

a CFAA claim against an employee who violated an employment agreement by using his access to his employer computer system to steal data for a competitor. The defendant transferred information from password-protected computer drives to his new employer while still employed with the former company in violation of a confidentiality agreement. *Davidson*, 540 F. Supp. 2d at 1327-31. Correctly identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view," the court held that "a violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." *Id.* at 1343.

In *Brett Senior & Assocs.*, an employer alleged that its former employee misused confidential information at his new employer in violation of the CFAA. While still working with his former employer, the employee interviewed with a rival company and showed it a list of his employer's clients and those the details of those clients' business with the company. Before leaving to join the new firm, the employee then contacted 20 of his clients and convinced 15 of them to come with him to the new firm. *Brett Senior & Assocs., P.C.*, 2007 WL 2043377 at *1. The court relied on the legislative history to reject the former employer's CFAA claim. The employee defendant had full access to information contained in the computer system until his departure, and the court concluded that a CFAA violation is a trespass offense, not a misuse of services offense. *Id.* at *3.

In *Shamrock Foods v. Gast,* under similar facts, the District Court relied on *Davidson* and *Werner-Masuda* to hold that the defendant did not access the information at issue "without authorization" or in a manner that "exceed[ed] authorized access." *Shamrock Foods*, 535 F. Supp. 2d at 968. The defendant had an employee account on the computer he used at his employer Shamrock and was permitted to view the specific files he allegedly emailed to himself. The CFAA did not apply, even though the emailing was for the improper purpose of benefiting

himself and a rival company in violation of the defendant's Confidentiality Agreement.[6] *See Werner-Masuda,* 390 F.Supp.2d at 496 (interpreting the same language "prohibit[ing] only unauthorized access and not the misappropriation or disclosure of information" in the Stored Communications Act (SCA), 18 U.S.C. § 2701(a) to mean that "there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access." (quoting *Educ'al Testing Service v. Stanley H. Kaplan, Educ'al Ctr., Ltd.,* 965 F. Supp. 731, 740 (D. Md. 1997) ("[I]t appears evident that the sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way."))).

2. Older Cases Wrongly Adopted A Broader View Of "Exceeding Authorized Access"

The cases discussed above contrast with and reject earlier decisions, most importantly *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), which introduced an agency theory of authorization under the CFAA that several courts have followed. *Shurgard* follows neither the plain language nor the legislative intent of the CFAA and would lead to a variety of troubling and potentially unconstitutional results. *See id*. The reasoning in *Werner-Masuda* is both persuasive and correct and, to the extent that *Shurgard* takes a different approach, this Court should reject it.

In *Shurgard*, the District Court denied a motion to dismiss a CFAA claim brought by an employee that took employer information from the computer system

[6] Of course, a plaintiff may be able to bring a valid claim under state law for misappropriation of trade secrets. That claim would be subject to the safeguards built into the trade secret liability rules, including allowances for reverse engineering and for disclosure of information that is not, in fact, secret. The CFAA violation has no safeguards; under the Government's view in this case it would put all the power in the hands of the corporation drafting the terms of use.

with him to his next job. *Id.* at 1129. The court relied on the Restatement (Second) of Agency, §112 (1958), to hold that when the plaintiff's former employees accepted new jobs with the defendant, the employees "lost their authorization and were 'without authorization' [under the CFAA] when they allegedly obtained and sent [the plaintiff's] proprietary information to the defendant via e-mail"). *Shurgard,* 119 F. Supp. 2d at 1125. The court examined the Senate report accompanying Congress's *1996* amendments to the CFAA, and concluded that Congress intended the statute to have "broad meaning" that was intended to cover the situation under dispute. *Id.* at 1129. But the 1996 amendments were of little relevance to the authorization issues in *Shurgard* or here, as those amendments replaced the term "federal interest computer" with "protected computer." 18 U.S.C. § 1030(a)(2)(C) (2008). In contrast the district court in *Werner-Masuda* relied heavily on the *1986* Senate report accompanying the CFAA. *Werner-Masuda,* 390 F. Supp. 2d at 497-499. The 1986 amendments are the relevant ones because those are the amendments that added the term "exceeds authorized access." 18 U.S.C. § 1030(a)(2)(C) (2008). This is the term at issue here because it is the part of the statute that reaches insiders who are allowed access for some purposes, but not for others. For this reason, *Werner-Masuda*'s take on the legislative history of the CFAA is far more persuasive than that of the court in *Shurgard* on the critical issue of whether Defendant Drew gained unauthorized access or exceeding authorized access.

A few cases find that, in the civil employment context, the principles of agency mean that an employee accesses a computer "without authorization" if, without knowledge of the employer, the employee uses the employers computer system in a manner adverse to the employer's interests. *See, e.g.*, *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-421 (7th Cir. 2006); *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006). Several earlier cases also found a CFAA violation for non-employees, but only after clear and repeated warnings that the user's conduct was not authorized, and only under circumstances where the user

either had a fiduciary duty to the computer owner or where the access was for competitive commercial gain, facts significantly absent in this case. *See EF Cultural Travel BV v. Zefer Corp.* 318 F.3d 58 (1st Cir. 2003), (rejecting a CFAA claim based on a "reasonable expectations" test but stating in dicta that "a lack of authorization could be established by an explicit statement on the website restricting access"); *EF Cultural Travel BV v. Explorica Inc.,* 274 F.3d 577 (1st Cir. 2001) (finding CFAA liability where the defendant poached an ex-EF employee, who in turn revealed confidential information about his former employer which improved the competitor's use of automated tools to search and "systematically glean company's prices from [competitor's] website"); *Southwest Airlines Co. v. FareChase Inc.,* 318 F. Supp. 2d 435 (N.D. Tex. 2004) (defendant created an automated tool that "scraped" web site information and allowed corporate travelers to search online for airline fares, including Southwest's. despite the plaintiff's "repeated warnings and requests" to cease); *Register.com, Inc. v. Verio, Inc.,* 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (court enjoined automatic searching of the registrant contact information contained in domain registry database after lawyers specifically objected to the defendant's use and sent out a terms of use letter to the defendant), *aff'd in part as modified by Register.com, Inc. v. Verio, Inc.,* 356 F.3d 393 (2d Cir. 2004) (reversing the trial court's CFAA finding on the basis that there was insufficient likelihood of showing the $5,000 damage threshold necessary for private claims, but upholding a trespass to chattels claim); *America Online Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998) ("*AOL*"), (the defendant transmitted more than 92 million unsolicited and bulk e-mail messages advertising their pornographic Web sites to AOL members in violation of AOL's email policies and terms of use).

These civil cases are readily distinguished from the criminal prosecution of Defendant Drew here because all but *AOL* involve actual prior notice to the defendant that their computer access was unauthorized, rather than the mere posting of terms of service on a website which could be ignored or violated by a user. These

cases also all involve use of the plaintiff's computer service for the defendant's commercial advantage to the detriment of the computer system owner. *See* Lemley, 91 Minn. L. Rev. at 476-77 (noting a greater willingness of some courts to enforce terms against businesses than against consumers). Here, Defendant Drew allegedly failed to provide truthful and accurate registration information; failed to refrain from using any information obtained from MySpace services to harass, abuse, or harm other people; failed to refrain from soliciting personal information from anyone under 18; failed to refrain from promoting information that she knew was false or misleading; and failed to refrain from posting photographs of other people without their consent. The indictment does not allege even that Defendant had seen or knew of these terms in the MySpace TOS, but she certainly did not receive any direct warnings to stop. Nor was she acting for commercial advantage in a way that could be seen as unfairly competing with or harming MySpace's business, factors important to the decisions in virtually all the above cases.

Apart from these important factual distinctions, for the reasons stated, these cases were wrongly decided, in light of the plain language and the legislative history of the CFAA.

F. The Rule Of Lenity Requires The Narrower Interpretation Of The CFAA's "Access" Language

The rule of lenity should guide the construction of section 1030 (a)(2)(C) in this case because the CFAA is first and foremost a criminal statute. *See Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8 (2004); *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 (1992). The rule of lenity "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." *Shamrock Foods*, 535 F. Supp. 2d at 965-67 (plain language of the statute, legislative history and rule of lenity support a narrow view of the CFAA); *see Pasquantino v. United States*, 544 U.S. 349, 383 (2005); *McNally v. United States*, 483 U.S. 350, 359-60

(1987).

Here, because Congress has not proactively specified that the CFAA's "access" provisions criminalize mere violations of terms of service, the rule of lenity requires that courts adopt the "less harsh" interpretation. *See, e.g., United States v. Miranda-Lopez*, 2008 WL 2762392 at *5 (9th Cir. July 17, 2008) ("the 'longstanding' rule of lenity requires us to resolve any ambiguity in the scope of a criminal statute in favor of the defendant" (citations omitted)). This is the approach taken by the court in *Shamrock Foods Co.* in adopting the narrower interpretation of "accesses . . . without authorization or exceeds authorized access." The court there used the rule of lenity to reject imposition of CFAA liability on a disloyal former employee, concluding "[t]he approach advanced by Shamrock would sweep broadly within the criminal statute breaches of contract involving a computer. . . . *The Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA*." *Shamrock Foods* at 967 (emphasis added). *United States v. LaMacchia* reached a similar result as the rule of lenity would require. Because Congress had failed to criminalize non-commercial distribution of copyrighted materials, the Government was not entitled to stretch a broader statute regulating a different kind of conduct to punish admittedly bad conduct. *LaMacchia,* 871 F. Supp. 535 (D. Mass. 1994). If Congress wanted to criminalize the conduct at issue here, it could have. If Congress wanted to give the force of law to terms of service agreements, it can. But it did not, and the rule of lenity does not permit the Government to use the CFAA to reach that result.

G. The Government's Previous Attempt In This District To Expand Civil Cases Interpreting the CFAA into the Criminal Context Led To The Wrongful Conviction And Incarceration Of An Individual For Constitutionally Protected Activities

In a disturbingly similar expansion of civil CFAA cases to support a criminal prosecution under a different section of the CFAA, 18 U.S.C. § 1030(a)(5)(A), the United States Attorney's Office in this district from 2001 to 2003 prosecuted

computer programmer Bret McDanel, *United States v. McDanel,* Ninth Circuit Case No. 03-50135, Central District of California Case No. CR-01-638-LGB. McDanel worked for a Tornado, a Los Angeles firm that provided Web-based email and voice mail services. While employed there, he discovered a serious security flaw in the company's email system, which intruders could exploit to read customers' private messages. He brought the flaw to the company's attention, but it wasn't fixed. After he left Tornado, McDanel sent an anonymous email to Tornado customers, describing the security flaw, and directing customers to a website McDanel had set up providing more information. The Government indicted McDanel for violating the CFAA, alleging that because he *sent emails* to customers' Tornado.com email addresses, and these emails gave customers information that the company did not want its users to have, McDanel intentionally caused damage to the integrity of Tornado's email server. The Government relied heavily on *Shurgard*'s agency law theory, arguing that McDanel acted without the best interests of Tornado in mind, so his emails were improper. McDanel was convicted and sentenced to 16 months in prison.

On appeal to the Ninth Circuit,[7] the Government reversed its position, "confess[ed] error," and moved to dismiss the charges against McDanel. (See *United States v. McDanel*, Government Brief, attached as Exhibit A, at 6, 8). While McDanel sent information to Tornado's servers, and while that information caused harm to Tornado's business (by reducing customer confidence in the privacy and security of their messages), the Government admitted that that type of harm could not be a CFAA violation unless it was intended to help someone illegally access the system or change data there. *Id.* at 8. The flaw in the current prosecution and that of McDanel is the same. The Government seeks to extend the reasoning of disfavored civil law cases from the employment or commercial context to argue that any use of

[7] Jennifer Granick, Civil Liberties Director with *amicus* Electronic Frontier Foundation, represented Mr. McDanel on appeal.

a computer server in a manner contrary to the interests of the server owner is a crime. As with the prosecution of Mr. McDanel, this prosecution is in error.

II. APPLYING THE CFAA TO DEFENDANT'S CONDUCT IN THIS CASE WOULD CONSTITUTE A SERIOUS ENCROACHMENT ON FUNDAMENTAL CIVIL LIBERTIES, INCLUDING FREEDOM OF SPEECH

A. The First Amendment Assures The Right To Speak Anonymously Online

Individuals have the qualified right to speak anonymously, including on the internet, so criminal prosecution for failing to supply accurate identifying information to an online communications service endangers First Amendment rights. Yet one of the alleged violations of the MySpace terms of service on which the Government bases this Indictment is Defendant's use of a fictitious name in registering for an account. *See* Indictment at 6.

Average internet users may have numerous valid reasons for wanting to keep their identities secret. Individuals may want to protect themselves from unwanted attention or from unwanted advertising, even while the service providers hope to sell customer's personally indentifying information or send advertising. They may wish to avoid having their views stereotyped according to their racial, ethnic or class characteristics, or their gender. They may be associated with an organization but want to express an opinion of their own, without running the risk that readers will assume that the group feels the same way. They may want to say or imply things about themselves that they are unwilling to disclose otherwise. And they may wish to present provocative ideas that they fear could subject them to retaliation. Not surprisingly, in a recent survey, almost one-third of social network users admitted to providing false information to protect their identities. Antony Savvas, *Social Network Users Hide Identities*, Computer Weekly, Sept. 25, 2007.

The Supreme Court has consistently upheld the right to anonymous speech in a variety of contexts, noting that "[a]nonymity is a shield from the tyranny of the majority . . . [that] exemplifies the purpose [of the First Amendment] to protect

unpopular individuals from retaliation … at the hand of an intolerant society." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995); *see also id*. at 342 ("an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."); *Gibson v. Fla. Legislative Investigative Comm.*, 372 U.S. 539, 544 (1963) ("[I]t is ... clear that [free speech guarantees] ... encompass[] protection of privacy association …"); *Talley v. California*, 362 U.S. 60, 64 (1960) (finding a municipal ordinance requiring identification on hand-bills unconstitutional, and noting that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.").

The First Amendment applies fully to internet communications, including email and the World Wide Web. *Reno v. ACLU*, 521 U.S. 844, 870 (1997) (there is "no basis for qualifying the level of First Amendment protection that should be applied to" the internet). Numerous courts have specifically upheld the right to communicate anonymously on the internet. *See, e.g., Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) ("The right to speak anonymously extends to speech via the internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas."); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998); *ACLU of Ga. v. Miller*, 977 F. Supp. 1228, 1230 (N.D. Ga. 1997); see also *ApolloMEDIA Corp. v. Reno*, 526 U.S. 1061 (1999), *aff'd* 19 F. Supp. 2d 1081, 1085 n.5 (C.D. Cal. 1998) (protecting anonymous denizens of a web site at www.annoy.com, a site "created and designed to annoy" legislators through anonymous communications); *Global Telemedia Int'l v. Does*, 132 F. Supp. 2d 1261, 1267 (C.D. Cal. 2001) (striking complaint based on anonymous postings on Yahoo! message board based on California's anti-SLAPP statute).

It is true that the constitutional privilege to remain anonymous is not absolute. Plaintiffs may properly seek information necessary to pursue reasonable and meritorious litigation. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578

(N.D. Cal. 1999) (First Amendment does not protect anonymous internet users from liability for tortious acts such as defamation); *Doe v. Cahill*, 884 A.2d 451, 456 (Del. 2005) ("Certain classes of speech, including defamatory and libelous speech, are entitled to no constitutional protection."). Also, individuals can choose to waive their free speech rights, and courts may enforce confidentiality agreements over a First Amendment defense. *See Snepp v. United States*, 444 U.S. 507, 510 (1980) (*per curiam*). However, the law does not presume a waiver of constitutional rights in contract so courts give heightened scrutiny to the enforceability of such agreements. *Ohio Bell Tel. Co. v. Public Utilities Comm'n*, 301 U.S. 292, 307 (1937). To enforce such a contract, the waiver must not undermine the relevant public interest. *See D. H. Overmyer Co. v. Frick Co.,* 405 U.S. 174, 187-88 (1972).

In this case, even assuming, *arguendo*, that the MySpace TOS is privately enforceable in spite of its contractual infirmities and restrictions on protected anonymous speech, monetary damages, not criminal convictions and prison sentences, "are always the default remedy for breach of contract." *United States v. Winstar Corp.,* 518 U.S. 839, 885 (1996) (plurality opinion). "Our system of contract remedies rejects, for the most part, compulsion of the promisor as a goal. It does not impose criminal penalties on one who refuses to perform his promise, nor does it generally require him to pay punitive damages." *Canada Dry Corp. v. Nehi Beverage Co.*, 723 F.2d 512, 526 (7th Cir. 1983). Yet the Government's construction of "without authorization or exceeds authorized access" in this case, based in part on Defendant Drew's alleged failure to supply "truthful and accurate registration information," Indictment at 5, 7, would make the assertion of protected anonymity the basis for criminal liability. While "[t]he Government may violate [the First Amendment] in many ways, . . . imposing criminal penalties on protected speech is a stark example of speech suppression." *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 244 (2002).

The First Amendment problems begin with, but do not end with, the right to

speak anonymously. Under the Government's construction of the CFAA, speech that violates any terms of service would be unauthorized or in excess of authorization and potentially criminal. If the comment policy of a web site specified "no comments favorable to Democrats" or "no comments that are off-topic" or "no bad stuff" those expressions too would be swept into the reach of the CFAA.

B. Constitutional Avoidance Dictates A Narrow Reading Of "Access" Under The CFAA

This Court need not decide whether enforcing the CFAA would violate the First Amendment in this case. The mere fact that the question arises, however, requires this Court to interpret "exceeds authorized access" narrowly, so as to avoid a potentially unconstitutional application. "'[I]t is a cardinal principle' of statutory interpretation . . . that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.'" *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (quoting *Crowell v. Benson*, 285 U.S. 22, 62 (1932)). A narrow construction of "unauthorized access" and "exceeds authorized access" – one which does not punish the failure to use truthful identification information when using online services that indicate an interest in collecting this data in their terms of use – is both possible and otherwise compelled by the statutory language and history of the CFAA.

III. APPLICATION OF THE CFAA WHEN A USER IGNORES OR VIOLATES WEBSITE TERMS OF SERVICE WOULD VIOLATE DUE PROCESS AND RENDER THE STATUTE VOID FOR VAGUENESS AND LACK OF FAIR NOTICE

Grounding criminal liability under section 1030(a)(2)(C), as the Government seeks to do here, on an interpretation of "access without authorization" and/or "exceeds authorized access" that is based entirely on whether a person has fully complied with the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service would strip the statute of adequate notice to citizens of what conduct is criminally prohibited and render it hopelessly and

unconstitutionally vague. If the Government's proposed construction of 18 U.S.C. 1030(a)(2)(C) in this case is correct, not only the defendant but also potentially millions of otherwise innocent internet users would be committing frequent criminal violations of the CFAA through ordinary, indeed routine, online behavior which they have been given no reason to believe would make them felons. The lack of notice under the Government's interpretation is stark; counsel for *amici* are not aware of a *single* criminal prosecution or conviction in the entire 22 years of the CFAA's existence that has attempted to base criminal liability on disregard for the contractual terms of service on a website.

The Supreme Court has stated that,

> "[i]t is a fundamental tenet of due process that '[n]o one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes.' *Lanzetta v. New Jersey*, 306 U.S. 451, 453 (1939). A criminal statute is therefore invalid if it 'fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden.' *United States v. Harriss*, 347 U.S. 612, 617 (1954)."

United States v. Batchelder, 442 U.S. 114, 123 (1979); s*ee also Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972). A plurality of the Supreme Court has further specified that "[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion).

In the Ninth Circuit, "[t]o survive vagueness review, a statute must '(1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner.'" *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (quoting *Nunez v. City of San Diego*, 114 F.3d 935, 940 (9th Cir. 1997). "Vague statutes are invalidated for three reasons: '(1) to avoid punishing people for behavior that they could not have known was illegal; (2) to avoid

subjective enforcement of laws based on 'arbitrary and discriminatory enforcement' by government officers; and (3) to avoid any chilling effect on the exercise of First Amendment freedoms.'" *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122, 1133 (9th Cir. 2007) (quoting *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998)).[8]

Nothing in § 1030(a)(2)(C), its legislative history, or the case law interpreting it provides any sort of "fair notice" to citizens, including the defendant here, that such everyday behavior could constitute a federal crime. For at least the following four reasons the interpretation advanced by the Government would fall short of providing required notice and avoiding vagueness. Given that courts should adopt a narrow construction of a statute to avoid vagueness and other unconstitutional infirmities, s*ee Zadvydas v. Davis*, 533 U.S. at 689, the Government's proposed view of the CFAA must be rejected.

A. Web Site Terms of Service are Routinely Ignored or Not Fully Read or Understood

The fallacy of any notion that internet users are on "fair notice" that disregarding the terms of service of the many web sites and web services they visit puts them at risk of serious criminal liability is revealed by the widespread (and widely accepted) understanding that large numbers of users never read these terms, or read and understand only limited portions of them.

First, terms are often poorly accessible. Many web sites or web-based services post their terms behind a "legal notices" or "terms of service" hyperlink which users can only access by scrolling to the bottom of the page and clicking on the link. To access the MySpace terms of use, for example, one must scroll down to find a hyperlink labeled "terms". *See MySpace.com Home Page*, http://www.myspace.com/

[8] *See also United States v. Wunsch*, 84 F.3d 1110, 1119 (9th Cir. 1996) (finding that requirement in state bar statute incorporated in local rule to "abstain from all offensive personality" was unconstitutionally vague in the context of district court sanction of attorney).

(last visited July 28, 2008). Nothing about the link indicates that it is exceptionally important, much less that failure to click on it and read the underlying terms could subject the user to criminal penalties.

Second, the terms of service presented by many web sites and other online services are lengthy and impenetrable. In one particularly daunting example, Network Solutions, the domain name registrar, has a TOS that takes up 115 pages when pasted into a single spaced, 12-point font Microsoft Word document. *See Network Solutions Terms of Service*, http://www.networksolutions.com/legal/static-service-agreement.jsp (last visited July 28, 2008). The MySpace terms at issue here contain over 60 separate paragraphs or subparagraphs and takes up roughly ten pages when pasted into a Word document. *See Terms and Conditions—MySpace.com,* http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited July 28, 2008).

Not surprisingly, then, many commentators recognize that few consumers actually take the time to read and understand digital terms of service (or similar software download agreements) before saying they agree to them. *See* Restatement (Second) of Contracts § 211, cmt. b (1981) ("Customers do not . . . ordinarily understand or even read the standard terms."); Robert L. Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 Hous. L. Rev. 1041, 1051 (2005) ("Clickwrap licenses are ubiquitous today, and most people click to accept without reading the text."); Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. Rev. 429, 429-31 (2002) ("with increasing alacrity, people agree to terms [in clickwrap contracts] by clicking away at electronic standard forms on web sites and while installing software"); Michael I. Meyerson*, The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. Miami L. Rev. 1263, 1269 & nn.28-29 (1993) (citing cases recognizing the failure of most consumers to read form

contracts).[9] In one notable example, public disregard for license terms was graphically illustrated by a software company that surreptitiously inserted into its license agreement an offer to pay $1000 to the first person to send an email to a particular address. It took four months and more than 3000 installations before someone noticed the offer and claimed the prize. Jeff Gelles, *Internet Privacy Issues Extend to Adware*, Newark Star-Ledger, July 31, 2005, at 5. *See also Ting v. AT & T*, 182 F. Supp. 2d 902, 930 (N.D. Cal. 2002) (holding a customer service agreement procedurally unconscionable because lack of notice contributed to surprise, the court acknowledged that "AT & T's own research found that only 30% of its customers would actually read the entire CSA [consumer service agreement] and 10% of its customers would not read it at all").

Similarly, empirical research confirms that, in the online context, a majority of users ignored the EULA entirely when installing such popular software as Google Toolbar on their home computers. Nathaniel Good et al., Commentary, *User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware*, 2 I/S: J.L. & Pol'y for Info. Soc'y 283, 321 (2006). Furthermore, even the few people who do read the terms of service are unlikely to take notice of more than a handful of the provisions. Due to human cognitive limitations, even rational consumers will be ignorant of non-salient terms in form contracts. Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 Stan. L. Rev. 211, 244 (1995).

Moreover, as noted earlier, most website terms, like other form contracts, are long, written in impenetrable legalese and poorly organized. *See* Robert W. Gomulkiewicz, *Getting Serious About User-Friendly Mass Market Licensing for*

[9] In fact, research has shown that even participants in sophisticated business transactions routinely fail to read the terms of form contracts. Andrew Robertson, *The Limits of Voluntariness in Contract*, 29 Melbourne L. Rev. 179, 188 (April 2005) (surveying empirical research).

Software, 12 Geo. Mason L. Rev. 687, 692-94, 701-02 (2004). Such contracts often written at a level of difficulty that exceeds the ability of most consumers to understand. *See* Alan M. White & Cathy Lesser Mansfield, *Literacy and Contract*, 13 Stan. L. Rev. 233, 235-42 (2002). Drafters of these agreements give little attention to readability, instead relying heavily on legal boilerplate and including restrictive terms primarily designed to limit the company's exposure to liability. *See* Gomulkiewicz, *supra*, at 692-94, 701-02; Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. Chi. L. Rev. 1203 (2003). Given the difficulty of comprehending form contracts, and the typically low-dollar amount of the transactions to which they apply, a consumers' decision to forego reading a website's terms of use is not only common, but entirely rational. Eisenberg, 47 Stan. L. Rev. at 240-44; Meyerson, 47 U. Miami L. Rev. at 1269-70. Thus, even persons who are conscientious about reading the terms of service may be unaware of some of the provisions. Under these circumstances, whatever the validity of holding such contracts enforceable for purposes of contract law, the transformation of their terms into the defining criteria for serious criminal violations creates serious risks of criminal sanctions for unwitting violations that cannot pass vagueness and notice review.[10]

B. Web Site Terms Are Frequently And Arbitrarily Changed By Site Owners With Little Or No Likelihood Of Actual Notice To Users

Many terms of service contain clauses which state that the website owner can unilaterally change the terms at any time, and that continued use of the website implies acceptance of the new terms. For example, the MySpace terms at issue here, even if actually read and understood by a user when he or she visits or signs up for

[10] *See* Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 465, 475-76 (2006) (observing that in civil cases "in today's electronic environment, the requirement of assent has withered to the point where a majority of courts now reject any requirement that a party take any action at all demonstrating agreement to *or even awareness of terms* in order to be bound by those terms.") (emphasis added). A similar lax view simply cannot provide "fair notice" in the criminal context.

an account, expressly state that they can be changed without further notice to the user merely by updating the agreement on the MySpace website – the user is then presumably obligated to review the entire terms for changes *every time* he or she visits. *See Terms and Conditions—MySpace.com,* http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited July 28, 2008) ("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. It is therefore important that you review this Agreement regularly to ensure you are updated as to any changes.")[11] Under the Government's expansive view of the CFAA, a person's access to MySpace would be unauthorized or would exceed their authorization if that person used MySpace and inadvertently violated a newly added or updated provision of the terms that had been inserted since the last visit. However challenging such a view of notice to a contract's terms may be for civil contract law, it fundamentally cannot be said to constitute adequate "fair notice" for due process vagueness purposes. *See Douglas v. U.S. Dist. Court for Cent. Dist. Calif.*, 495 F.3d 1062, 1066 & n.1 (9th Cir. 2007) (holding that website users are not required to continually monitor a site's terms of use for possible changes).

[11] *See, also e.g., West Terms of Use,* http://west.thomson.com/about/terms-of-use/default.aspx?promcode=571404 (last visited July 28, 2008) ("By accessing, browsing, or using this website, you acknowledge that you have read, understood, and agree to be bound by these Terms. We may update these Terms at any time, without notice to you. Each time you access this website, you agree to be bound by the Terms then in effect."); *AOL Terms of Use,* http://about.aol.com/aolnetwork/aolcom_terms (last visited July 28, 2008) ("You are responsible for checking these terms periodically for changes. If you continue to use AOL.COM after we post changes to these Terms of Use, you are signifying your acceptance of the new terms.")

C. Web Site Terms May Themselves Be Arbitrary, Vague, or Frivolous And Are Created by Private Site Owners for a Myriad of Business or Personal Reasons Having Nothing To Do With Regulating "Access" for CFAA Purposes

Many web site terms contain conditions that are themselves vague, arbitrary or even fanciful. They are not written by their private drafters with the precision and care that would be expected – indeed required – of operative provisions in a criminal statute. Yet operative criminal provisions are precisely what routine business terms would be transformed into under the Government's interpretation of § 1030(a)(2)(C). This fact multiplies the likelihood that such an interpretation cannot satisfy the due process requirement that a statute not "fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits," *Morales*, 527 U.S. at 56, since the statute will itself in turn rely for its essential meaning on the existence and clarity of separate contractual terms.

Web site owners and internet businesses draft specific web site and web service terms of use provisions for a variety of reasons that have nothing to do with regulating "access" to their sites, and certainly nothing to do with preventing the sort of unauthorized hacking or trespass or theft of private data with which the CFAA is properly concerned. Google, for example, presumably included the terms of use provision described earlier – barring use of its services by minors -- to protect itself against liability and to try to ensure its terms were binding in the event of a litigated dispute. Surely it did not mean – or imagine – that tens of millions of minors in fact would never use its services to obtain information or would do so at the risk of criminal liability. In another example, YouTube's Community Guidelines, expressly incorporated into the site's terms of use, prohibit "bad stuff." *YouTube Community Guidelines,* http://www.youtube.com/t/community_guidelines (last visit July 28, 2008). Uploading "bad stuff" would violate YouTube's terms which, under the Government's theory here, would constitute unauthorized access or exceeding authorized access to the site. Surely YouTube did not draft the "bad stuff"

prohibition with CFAA access control in mind. The meaning of "bad stuff" is the essence of vagueness, and it is not even clear whose determination – YouTube's? A jury's? – would be required. To make sense and to avoid fatal vagueness problems, the terms "without authorized access" and "exceeds authorized access" in the CFAA must be limited to clear, proper purposes consistent with the statute's goals, and not whatever commercial or personal purpose motivates a site owner to draft a provision in a terms of service document.

D. Basing Criminal Liability On Private Contract Terms Inevitably Will Lead To Arbitrary And Discriminatory Enforcement

Allowing the provisions of privately created, sometimes arbitrary or even frivolous web site terms of use to prescribe the legally critical CFAA standard for when a person has gained unauthorized access or exceeded authorized access to computers can only lead to arbitrary and discriminatory enforcement of the CFAA. Statutes that create the likelihood of such arbitrary and discriminatory enforcement are invalid. *See, e.g., Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971) (law disallowing three people to congregate if it is annoying to others was unconstitutionally vague, "not in the sense that it requires person to conform his conduct to an imprecise but comprehensible normative standard, but rather in the sense that no standard of conduct is specified at all").

Choosing, as the Government has here, to prosecute under the CFAA a single, isolated instance of violating terms or service out of literally millions of similar, ongoing violations illustrates the dangers of arbitrary enforcement. In a world where each violation or neglect of a web site's terms could constitute unauthorized or excessive access and be the basis for criminal prosecution, there simply is no limiting principle that would restrain the exercise of this enforcement discretion and prevent arbitrary or discriminatory application of the law.

CONCLUSION

Megan Meier's death was a terrible tragedy, and there is an understandable desire to hold the Defendant somehow accountable for it, if Defendant's conduct was as alleged. But a dangerously overbroad construction of the CFAA would criminalize the everyday conduct of millions of internet users. The novel -- indeed, unprecedented in the history of the CFAA -- interpretation of § 1030(a)(2)(C) advanced in the indictment cannot be squared with the plain language of the statute, its legislative history, and the constitutional requirements that criminal statutes provide citizens fair notice, avoid vagueness and comport with the First Amendment. Consequently, amici urge the Court to dismiss the Indictment.

DATED: August 1, 2008

By _____

Jennifer Stisa Granick (California Bar No. 168423)

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x102
Facsimile: (415) 436-9993

Certificate of Compliance with Circuit Rule 32-1

Pursuant to Rules 29(c)(5) and 32(a)(7)(C) of the Federal Rules of Appellate Procedure and Ninth Circuit Rule 32-1, I hereby certify that the foregoing brief uses 14-point Times New Roman spaced type; the text is double-spaced; and footnotes are single-spaced. This brief complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(d) and 32(a)(7)(B) because there are no limits on the length of party briefs in support of motions to dismiss in criminal cases under Rule 12. This brief contains approximately 11,000 words.

DATED: August 1, 2008

By _____
Jennifer Stisa Granick
For *Amici Curiae* Electronic Frontier Foundation

APPENDIX A

LAW FACULTY *AMICI CURIAE*

Amici file this brief in their individual capacities, and not as representatives of the institutions with which they are affiliated. Institutional affiliations are listed for identification purposes only.

Susan Brenner
NCR Distinguished Professor of Law and Technology
University of Dayton School of Law

Lauren Gelman
Executive Director
Center for Internet and Society
Stanford Law School

Llewellyn Joseph Gibbons
Associate Professor
University of Toledo College of Law

Eric Goldman
Assistant Professor of Law
Director, High Tech Law Institute
Santa Clara University School of Law

Mark A. Lemley
William H. Neukom Professor of Law
Stanford Law School
Director, Stanford Program in Law, Science and Technology

Phillip R. Malone
23 Everett Street
Cambridge, MA

Paul K. Ohm
Associate Professor of Law
University of Colorado Law School

Malla Pollack
Professor of Law
Barkley School of Law
Paducah, Kentucky

Michael Risch
Associate Professor of Law
Project Director - Entrepreneurship, Innovation and Law Program
West Virginia University College of Law

Jason Schultz
Acting Director
Samuelson, Law, Technology & Public Policy Clinic
UC Berkeley School of Law

Brian G. Slocum
Associate Professor of Law
University of the Pacific
McGeorge School of Law

Daniel J. Solove
Professor of Law
George Washington University Law School

William McGeveran
Associate Professor
University of Minnesota Law School

Robert Weisberg
Edwin E. Huddleson, Jr. Professor of Law
Director, Stanford Criminal Justice Center
Stanford Law School