June 29, 2009

THE FEDERAL RESPONSE TO A TRAGIC TEEN SUICIDE: THE STRETCHING OF A STATUTE TO PUNISH CYBER-HARASSMENT, THE GROUNDBREAKING TRIAL, IMPLICATIONS FOR EVERYONE, AND SUGGESTIONS FOR THE FUTURE.

John M Ivancie

THE FEDERAL RESPONSE TO A TRAGIC TEEN SUICIDE: THE STRETCHING OF A STATUTE TO PUNISH CYBER-HARASSMENT, THE GROUNDBREAKING TRIAL, IMPLICATIONS FOR EVERYONE, AND SUGGESTIONS FOR THE FUTURE.

J. MICHAEL IVANCIE JR.

SUBMITTED APRIL 21, 2009

FACULTY ADVISOR: PROFESSOR DAVID MARCUS

TABLE OF CONTENTS

I. INTRODUCTION

This article addresses the legal implications of using an anti-hacking statute, the Computer Fraud and Abuse Act ("CFAA"), in an unprecedented manner – to prosecute cyber-harassment. Lori Drew, a middle-aged woman from Missouri, along with her teenage daughter and another young woman, created a fake MySpace account to harass an on-and-off friend of Drew's daughter. The trio proceeded to harass their target through the MySpace account. This harassment led to the eventual suicide of their target. The public was outraged upon discovering what Drew had done; however, there were no state criminal statutes in Missouri which criminalized Drew's actions. In response to this, federal prosecutors indicted Drew in California for violating the CFAA, a statute which, since its inception, has been used to prevent hacking and unauthorized access of computer systems, *not* cyber-harassment. This paper will argue that the extension of the CFAA as articulated in the Drew case is beyond the bounds of the intent of those who drafted it, and that such an extension ignores the way the CFAA has been used by prosecutors and applied by judges. Additionally, such an extension of the CFAA would make the statute constitutionally questionable in application and create dire implications for internet use.

Section I of this paper discusses the factual background of the Drew case and outlines the unique legal issues it presents. Section II discusses the statutory history of the Computer Fraud and Abuse Act, how it is typically used, and the competing interpretations of the CFAA among various circuits. After laying out the original intent for the CFAA and its typical use, Section II will close by arguing that the extension of law articulated in the Drew case is entirely unsupported. Section III will explore the

implications of using the CFAA as the prosecutors have in the Drew case – specifically, how it may chill internet use and give prosecutors unprecedented discretion to choose among the millions of "violations" occurring daily. Additionally, the unreasonable legal results of extending the CFAA as advanced in the Drew case will be evidenced by specific examples of internet usage and how each would be criminalized under the Drew precedent. Further, Section III will address four specific reasons why the CFAA's expansion is a mistake: 1) it uses contracts of adhesion to create criminal violations; 2) it privatizes criminal statute writing; 3) it allows terms of service agreements to dictate the scope of the CFAA, making it void for vagueness; and 4) it is necessarily overbroad in application. Section IV will address legislative responses to the Drew case and suggest limits and guidelines for a more focused approach to controlling cyber-harassment. The conclusion, Section V, will reiterate that the CFAA is an inappropriate statute to police cyber-harassment, and argue that a more tailored statute is necessary.

A. FACTUAL BACKGROUND

Around September 2006, Lori Drew, her high-school-aged daughter Sara Drew and family friend Ashley Grills created a fictitious account on MySpace.com under the name of "Josh Evans," a 16-year-old male.[1] These three residents of suburban St. Louis, Missouri created this account to communicate with Sara Drew's on-and-off friend, 13-year-old Megan Meier.[2] Grills claimed the original intent of the account was to

[1] Associated Press, *Key Events in the Megan Meier Case*, http://www.usatoday.com/tech/products/2008-05-15-1838288037_x.htm.

[2] Associated Press, *Mom Indicted in MySpace Suicide Case*, http://www.msnbc.msn.com/id/24652422.

determine if Megan was gossiping about Sara.[3] The trio also contemplated setting up a meeting between Megan and the fake boy at a mall to humiliate Megan.[4] Megan and the fictitious Josh Evans messaged each other regularly and had a flirtatious relationship through MySpace.com's messaging service.[5] Allegedly, Lori, Sara and Ashley all participated in writing messages to Megan.[6]

On October 15, 2006 the fictitious Josh Evans sent Megan a message saying that he no longer wanted to be her friend.[7] The next day, "Josh" sent Megan another message telling her that the world would be a better place without her.[8] Megan responded to Josh with "[y]ou are the kind of boy a girl would kill herself over."[9] Megan called her mother, upset about the hurtful messages sent from the Josh Evans account.[10] Upon arriving home and reviewing the content of the messages, Megan's mother was disturbed by the vulgarity used in them.[11] After arguing with her mother, Megan ran upstairs to her bedroom.[12] Twenty minutes later, Megan's parents discovered that Megan had hung

---

[3] Kim Zetter, *Government's Star Witness Stumbles: MySpace Hoax Was Her Idea, Not Drew's*, http://blog.wired.com/27bstroke6/2008/11/lori-drew-pla-3.html.

[4] *Id.*

[5] Kim Zetter, *Experts Say MySpace Suicide Indictment Sets 'Scary' Legal Precedent*, http://blog.wired.com/27bstroke6/2008/05/myspace-indictm.html; Indictment of Defendant at 7, United States v. Drew, No. CR-08-0582-GW (alleging that Drew, writing as Josh Evans, invited Megan to touch his "snake," called her "sexi" and induced Megan to write "aww sexi josh ur so sweet if u moved back u could see me up close and personal lol"); *id.* at 8 (alleging that Drew, writing as Josh Evans told Megan "Heyy babe!! Call me sometime…I love you so much.").

[6] Zetter, *supra* note 3.

[7] Associated Press, *supra* note 1.

[8] Associated Press, *supra* note 1; Indictment, *supra* note 5, at 8.

[9] Zetter, *supra* note 3.

[10] Associated Press, *Mom: MySpace Hoax Led to Daughter's Suicide*, http://www.foxnews.com/story/0,2933,312018,00.html.

[11] *Id.*

[12] *Id.*

herself in her closet.[13] Megan Meier died in a hospital the following day on October 17, 2006.[14]

After Megan's suicide, a neighbor informed her parents that the Josh Evans account was a fictitious creation of Lori Drew and others.[15] The following year, media coverage surrounding Lori Drew's role in Megan Meier's suicide grew, creating a flurry of attention and public outrage.[16] On Dec. 3, 2007, the St. Charles County, Missouri prosecutor stated that after reviewing the criminal code, he could find no way to file charges against Drew.[17] On May 15, 2008, a Los Angeles grand jury indicted Drew in the district court for the Central District of California.[18] The indictment specified a charge for conspiracy pursuant to 18 U.S.C. § 371 (1994), and three charges for unauthorized access of a computer used in interstate commerce in furtherance of a tortuous act, namely, the intentional infliction of emotion distress on Megan Meier, pursuant to the CFAA, 18 U.S.C. § 1030(a)(2)(C).[19] Ashley Grills, the woman who sent the last message from the Josh Evans's account, agreed to testify at Lori Drew's trial in exchange for immunity.[20]

---

[13] *Id.*

[14] *Id.*

[15] Associated Press, *supra* note 1.

[16] *Id.*; Kim Vetter, *Cyberbullying Suicide Stokes the Internet Fury Machine*, http://www.wired.com/politics/onlinerights/news/2007/11/vigilante_justice (blogger tracked down Lori Drew's identity and address, then published that information on her blog).

[17] Associated Press, *supra* note 1.

[18] *Id.*

[19] Indictment, *supra* note 5, at 9.

[20] Joann Brady, *Exclusive: Teen Talks About Her Role in Web Hoax That Led to Suicide*, http://abcnews.go.com/GMA/story?id=4560582&page=1.

B. THE PROSECUTORS' THEORY OF THE CASE

The theory the government relied on for the charges against Drew has led to controversy.[21] The Computer Fraud and Abuse Act, found at 18 U.S.C. § 1030, was originally created to combat hacking and other computer-based criminal activity. Specifically, a violation of the CFAA occurs when someone has "knowingly accessed a computer without authorization or exceed[ed] authorized access."[22] In the Drew case, the government is applying the CFAA in a novel way. The government's theory of the case is that by violating the MySpace.com terms of service (signing up under a fake name, etc.), Drew and her co-conspirators were not authorized users of MySpace.com and thus were accessing information on MySpace.com servers either without authorization or in excess of authorized access and were therefore in violation the CFAA.[23] The stretch, and what has many concerned, is that this makes private contracts, namely a website's Terms of Service agreement ("TOS") criminally enforceable. Thus, if a website's Terms of Service was to stipulate that only left-handed people with red hair could access their website, and a right-handed person with blonde hair accessed that website, he or she would be an unauthorized user susceptible to federal criminal charges under the CFAA.[24]

---

[21] *See, e.g.*, Jacqui Cheng, *EFF: MySpace Suicide Charges a Threat to Free Speech*, Aug. 4, 2008, http://arstechnica.com/news.ars/post/20080804-eff-myspace-suicide-charges-a-threat-to-free-speech.html; Zetter, *supra* note 5 ("if successfully prosecuted the case could set a bad precedent for turning breach-of-contract civil cases into criminal ones").

[22] 18 U.S.C. § 1030(a)(1) (2008).

[23] *Id.*

[24] *Id.* § 1030(a)(2)(c) ("(a)Whoever-- . . . (2)intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-- . . . (C)information from any protected computer" is in violation and under subsection (c)(2)(B)(ii) susceptible to fine and up to 5 years in prison).

C. THE TRIAL

Drew's jury trial began on November 11, 2008 and lasted one week.[25] The jury returned a verdict of guilty for the lesser included misdemeanor violations of the CFAA, but not for felony violations.[26] The jurors felt they were not given enough evidence to find felony violations, which would have required not only the conclusion that Drew accessed information on MySpace.com servers without authorization, which they concluded she did, but also that she accessed those servers with the express intent to inflict emotional distress upon Megan Meier.[27]

After the jury returned their verdict, the forewoman of the jury, Valentina Kunasz, spoke out about the trial.[28] Kunasz stated that "[t]rust me, I was so for this woman going away for 20 years," but Kunasz found it difficult to convict Drew on the felony charges based on the evidence presented at trial.[29] Kunasz also admitted that the jurors never considered whether the use of the statute was appropriate in this case.[30] Interestingly, Kunasz entirely rejected the argument by Drew's attorney that no one reads TOS agreements, stating, "I always read the terms of service . . . [i]f you choose to be lazy and not go through that entire agreement or contract of agreement, then absolutely you should

---

[25] United States v. Drew, Criminal Docket For Case #: 2:08-cr-00582-GW (filed May 15, 2008).

[26] Scott Glover, *Jury Delivers Mixed Verdict in MySpace Bullying Trial*, L.A. TIMES, *available at* http://articles.latimes.com/2008/nov/27/local/me-myspace-trial-verdict27.

[27] Kim Zetter, *Jurors Wanted to Convict Lori Drew of Felonies, But Lacked Evidence*, http://blog.wired.com/27bstroke6/2008/12/jurors-wanted-t.html.

[28] *Id.*

[29] *Id.*

[30] *Id.*

be held liable."[31] Kunasz also commented on the emotional gravity of the trial, stating that "[t]his was a very serious subject for every single one of us. We wanted to make sure that we came to the right decision and that there was no question on anything." The jurors were likely moved by the very tragic facts, which is shown by Kunasz's want to convict Lori Drew of the highest possible crimes.

The judge in the case, Judge George H. Wu, is currently reviewing a Rule 29 motion for acquittal and has taken it under submission, with a decision pending.[32] Drew was set to be sentenced on April 30, 2009; however, sentencing has been pushed back to May 18th, thus, giving Judge Wu more time to consider the pending acquittal motion as well.[33] Ms. Drew faces up to three years of incarceration, but it is possible she will only receive probation for her convictions.[34]

If Judge Wu does not grant the defense counsel Rule 29 motion, the defense will almost certainly appeal.[35] However, the Drew case presents such a novel question of law that either side will likely appeal if the outcome is unfavorable to them. It is unlikely that the judge will upset the jury's verdict by granting the motion, thus making a defense appeal highly likely.[36] An appeal would bring the case before the Ninth Circuit. Many argue that the Ninth Circuit would set aside Drew's convictions based on the

---

[31] *Id.*

[32] United States v. Drew, *supra* note 25.

[33] *Id.*; Suburban Journal, *NEW: Sentencing Date for Drew Pushed to May 18*, http://suburbanjournals.stltoday.com/articles/2009/04/01/stcharles/crime/doc49d393684bc35156320724.txt.

[34] Glover, *supra* note 26.

[35] Kim Zetter, *Can Lori Drew Verdict Survive the 9th Circuit Court?*, http://blog.wired.com/27bstroke6/2008/12/can-lori-drew-v.html.

[36] *Id.*

misapplication of the CFAA in her case.[37] The Ninth Circuit has not squarely addressed the issue before and despite predictions either way, there is law supporting a broad application of the CFAA and a more limited approach present in district court opinions within the Ninth Circuit.[38] The differing interpretations of the CFAA will be discussed in Section II below.

While legally, the Drew case has serious precedential implications for all internet users, at its core the case is about a want of justice for what many feel was a series of despicable acts that led to the tragic loss of a young life. The Drew case is not the first example of cyber-harassment; however, it serves as a poignant example of the gravity of harm that can come from it and the need to tailor a statute that can more appropriately address such a social ill. The Drew case highlights the need to confront cyber-harassment, but also shows that the CFAA may not be the proper tool.

II. THE CFAA: ITS HISTORY, PURPOSE, AND USE.

This section will discuss how the CFAA has typically been used prior to the Drew case. Subsection A will discuss the legislative history of the CFAA and the acts its drafters intended to criminalize under the statute. Subsection B analyzes the Department of Justice's handbook on prosecuting computer crimes, and its message about how the CFAA should be used. Subsection C will show under what factual situations the CFAA is traditionally used, and how it is interpreted by judges. Within that section, differing

[37] *E.g. Id.*

[38] *Compare* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008), *with* Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

interpretations of the CFAA will be explored, along with the legal issues those differing interpretations create, which interpretations are more grounded in legislative history and produce a proper result, and how they may relate to the ultimate outcome in the Drew case.

The CFAA was created contemporaneously with advancements in technology to criminalize computer hacking. The CFAA has since been used, both civilly and criminally, to punish those who, without authorization, access or hack into computer systems. A typical CFAA case involves a defendant who, without authorization, accesses a computer system to attain information to sell or use it for personal gain. The Drew case presents a drastic factual departure from that of other CFAA cases. The use of the CFAA in the Drew case, when viewed in light of its legislative history, judicial interpretations, and historic use by federal prosecutors, shows that the legal extension argued for is not grounded in the intent of the statute, nor in the consistent interpretations since its enactment. Thus, the CFAA was not intended, nor is it properly equipped to handle, cyber-harassment or other cases factually similar to the Drew case.

A. STATUTORY BACKGROUND

The CFAA was originally called the Counterfeit Access Device and Computer Fraud and Abuse Act, and was passed into law in 1984.[39] It was created to protect against hacking and other unauthorized access of computer systems.[40] This view is

[39] Counterfeit Access Device And Computer Fraud And Abuse Act of 1984, 98 Pub. L. No. 473, 98 Stat. 1837, amended and renamed the Computer Fraud And Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (Oct. 16, 1986).

[40] 132 CONG. REC. H9260-02 ("Today, we will consider a very important bill-one aimed at reducing the amount of computer crime. Mr. Speaker, 'hacking' presents a tremendous danger to all of us.").

supported by the legislative history, the language of the statute, and debates surrounding the bill.[41] The 1984 House Committee made clear 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."[42] Specifically, hacking and unauthorized access were ills contemplated by legislators working on the bill.[43] The CFAA focuses on whether a user is authorized to access the information in question; if the user is, then no 'breaking or entering' or trespass has occurred. What the congressional record lacks is any mention of using the CFAA to combat the use of computers for harassing or bullying behavior. It is likely such a harm was not even contemplated by the drafters of the CFAA or Congress; however, the tresspatory hacking foundation of CFAA violations makes its use for cyber harassment untenable. The CFAA represents the congressional response to the modern development of computer-based criminality in the form of hacking and unauthorized access to protected information.

---

[41] S. REP. NO. 99-432 (Sept. 3, 1986) (recognizing importance of combating computer crime and unauthorized access and "deter[ring] would-be computer criminals."); H.R. REP. No. 98-1159 (Stating CFAA "creates a federal offense to wrongfully access a computer and obtain information concerning national defense or foreign relations" and "creates a federal offense to wrongfully access a computer and obtain data protected under the right to financial privacy act or the fair credit reporting act." and "creates a federal offense to wrongfully access to computer and use, modify, destroy or disclose information without authorization, in a government computer, or prevent authorized use of a government computer. attempts and conspiracies to commit these three offenses are also prohibited."); Christensen v. C.I.R., 523 F.3d 957, 962 (9th Cir. 2008) (when interpreting a statute, courts look to the plain language of the statute, and to legislative history).

[42] H.R. REP. NO. 98-894, at 20 (1984).

[43] CONG. REC., *supra* note 40 (mentioning "hacking" as the danger the CFAA is addressing); S. REP. 104-357 (Aug. 27, 1996) (discussing problems CFAA is meant to remedy and listing examples of instances when hackers have attained information when not authorized).

Originally, the CFAA was drafted to protect specific industries or certain classes of information, such as governmental or financial institutions, and medical and financial information.[44] The CFAA, however, has evolved and expanded. It now casts a much wider net over computer-based crime.[45] To this effect, the CFAA has been amended multiple times in reaction to new forms of computer-based criminality.[46] The CFAA's development has been largely reactionary in nature. Indeed, as Tom Leahy explained regarding amendment in 1990, "[t]his bill catches up with some problems already out of hand, by strengthening laws against computer abuse, [and] deterring malicious computer hacking."[47] One amendment in particular will be relevant to later analysis in Section II. The 1986 amendment to the CFAA substituted the phrase "exceeds authorized access" for "or having accessed a computer with authorization, uses the opportunity such access provides for *purposes to which such authorization does not extend*."[48] This change was made to take focus away from the *purpose* of the access to solely whether the access was

---

[44] S. REP., *supra* note 41 (recommending passage of CFAA and discussing a security breach that occurred in a cancer centers radiology patient computer database, and serious harm that could have resulted had hackers adjusted radiation treatment levels for patients, also recognizing growing role computers play in financial institutions with more than $100 trillion of electronic transfers occurring in 1983).

[45] See, *e.g.*, 18 U.S.C. § 1030(a)(2)(C) (amended 1996) (protecting information on computers used in interstate commerce).

[46] *See, e.g.*, 104 P.L. 294, Title II, 201, Title VI, 604(b)(36), 110 Stat. 3488 (broadening scope of Act, adding "the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State"); 110 P.L. 326 Title II, 203, 204(a), 205-08, 122 Stat. 3560 (Sept. 6, 2008) (amending CFAA to address "malicious spyware, hacking and keyloggers" and increasing its jurisdiction); CONG. REC., *supra* note 25, ("Mr. Speaker, as the gentleman knows, computer crime is a rapidly developing crime. We really have no idea just the dimensions of the problem. I am sure this is not going to be the last word on computer crime, but it certainly is a major step."); *see also* Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 285 (1997); Charlotte Decker, *Cyber Crime 2.0: An Argument To Update The United States Criminal Code To Reflect The Changing Nature Of Cyber Crime*, 81 S. CAL. L. REV. 959 (2008).

[47] 136 CONG. REC. 4614, (Apr. 19, 1990).

[48] S. REP .NO. 99-432, at 21 (emphasis added).

authorized or not.[49] Here, it is noteworthy that Congress has not amended the CFAA to specifically address cyber harassment or bullying (crimes focused on purpose), implying that the statute is not intended for such use. While the CFAA is continually evolving to cope with advances in technology and associated criminal activity, Congress has not modified the CFAA to address cyber harassment, and courts should be reluctant to extend it judicially. The fact that technology may grow faster than the law is able to predict or respond to criminal behavior serves as an important theme under which to view the Drew case.

Section 1030(a)(2)(C) of the CFAA, which Lori Drew was indicted under, in part specifies that a violation occurs when someone "intentionally access a computer without authorization or exceeds authorized access."[50] Exceeding authorized access is defined within the statute as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[51] The statute does not define "without authorization"; however, the language is unambiguous. The plain meaning of the words in the statute, coupled with the legislative intent surrounding the CFAA, leaves little doubt that incidents of trespass or hacking[52] are synonymous with the unauthorized access, which the CFAA criminalizes. The essential takeaway of the legislative history of the CFAA is that

---

[49] *Id.* ("removing from the sweep of the statute one of the murkier grounds of liability, under which a [someone'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.").

[50] 18 U.S.C. § 1030(a)(2)(C).

[51] 18 U.S.C. § 1030(e)(6).

[52] At this point, it is worth noting that the definition of hacking is "to gain access to a computer illegally", http://www.merriam-webster.com/dictionary/hacking, and "[[t]o use one's skill in computer programming to gain illegal or unauthorized access to a file or network: hacked into the company's intranet." http://dictionary.reference.com/browse/hacking.

"breaking and entering" into computer networks was a violation of federal law. The legislature intended to prevent trespass into protected computer networks by unauthorized users and nothing more.

B. DEPARTMENT OF JUSTICE INTERPRETATION

The Department of Justice's manual[53] for prosecuting computer crimes provides a good framework for how the CFAA is utilized and understood institutionally.[54] It is especially noteworthy that the Department of Justice characterizes § 1030(a)(2) offenses as crimes "Compromising the *Confidentiality* of a Computer."[55] When discussing the "obtaining information" part of section (a)(2)(C), the manual defines the violation as an "expansive one which includes merely viewing information online without downloading or copying it."[56] The DOJ takes the view that the "crux of the offense under subsection 1030(a)(2)(C) . . . is the abuse of a computer to obtain the information."[57] The

[53] Office of Legal Education Executive Office for United States Attorneys, *Prosecuting Computer Crimes*, http://www.usdoj.gov/criminal/cybercrime/ccmanual/ccmanual.pdf ("The contents of this book provide internal suggestions to Department of Justice attorneys.") (hereinafter "DOJ Manual").

[54] While this manual may be instructive on institutional use, it is not likely to be of persuasive value under the Supreme Court's *Chevron* agency deference standard because Congress has not left a gap in the CFAA for the DOJ to specifically fill. Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984) (when Congress has "explicitly left a gap for an agency to fill, there is an express delegation of authority to the agency to elucidate a specific provision of the statute by regulation").

[55] DOJ Manual, *supra* note 53, at 2, 15 (emphasis added).

[56] DOJ Manual, *supra* note 53, at 16 (citing S. REP. NO. 99-432, at 6; America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

[57] *Id.*

information need not be tangible in nature; intangible property, such as a proprietary computer program, is protected as well.[58]

The Department of Justice's interpretation of protected information is at odds with the prosecutors' view of the law in the Drew case. Namely, because the information at issue in the Drew case belonged to MySpace.com, the victim under the government's theory is MySpace.com, not Megan Meier. However, this information possessed no real value to MySpace.com, which also makes it unclear if the injury is really traceable to MySpace.com. Had Drew used any talents or cunning to sneak into MySpace servers and access proprietary software or download mass amounts of user information, then a true violation of the CFAA would have occurred and MySpace would clearly have been victimized. The facts here, however, do not support such criminal liability.

The Department of Justice's manual also discusses the jurisdictional and venue issues in CFAA cases.[59] The manual suggests the prosecutor focus on where the crime was committed.[60] The manual also recognizes that determining where a crime was committed can be difficult, but looking to where the crime was *initiated, continued, or completed* can provide likely locations for venue.[61] The manual suggests that, regarding § 1030(a)(2)(C) violations, "it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access and where the information is obtained."[62] The above quotation implies that venue should exist where the crime is

---

[58] *Id.*

[59] *Id.* at 93-98.

[60] *Id.* at 96.

[61] *Id.* (Multidistrict offenses "may be ... prosecuted in any district in which such offense was begun, continued, or completed." (citing 18 U.S.C. § 3237(a))) (emphasis added).

[62] *Id.*

initiated, but the DOJ also implies that venue can exist anywhere along the chain of access, which can be prejudicial to defendants. Thus, appropriate venue is extremely broad and unclear at best.

This broad approach to venue for the CFAA makes sense when a user is "victimizing" computers as he hacks through a network. However, the reasonableness of venue and jurisdiction fades when cyber-harassment is at issue. For example, in the Drew case, the "criminal" activity was initiated in Missouri, and the harm was felt in Missouri. Nevertheless, the case was prosecuted in California – where MySpace.com, the putative victim in the case, keeps its servers. This odd result highlights again why the CFAA is being used inappropriately. Under the prosecutors' theory, in this case the victim is MySpace.com, hence venue where their servers are; however, this case was brought *solely* because of what happened to Megan Meier, the true victim in this case. Yet, the case was not brought in Missouri where the real harm was felt. This could set a precedent for the future, where cyber-harassment cases will not be tried where the harm really occurred or was initiated, but at a distant server where the harassing information traveled through.

Practically, such venue results do not make sense, and would serve only to make defending oneself more difficult. In the Drew case, the venue was possibly to Ms. Drew's benefit. Had she been tried in Missouri, the likelihood of finding impartial jurors would have been even slimmer. The beneficial venue result in the Drew case should not distract the reader, however, from the important point that facing criminal charges far from one's normal residence, and where the majority of the criminal activity occurred, could cause great hardship and prejudice to the defendant.

C. How Federal Courts Apply the CFAA

A typical CFAA case[63] involves the defendant accessing information without authorization.[64] The plain language of Section 1030(a)(2), which Drew was charged under, targets "the unauthorized procurement or alteration of information, not its misuse or misappropriation."[65]

It is noteworthy that the United States Supreme Court has not squarely addressed any CFAA cases, and has only mentioned 18 U.S.C. § 1030 in passing to make general points regarding statutory construction.[66] Due to a lack of high-court treatment, there are differences in the interpretation of the CFAA among the various circuits. The two key applicable issues that have arisen in CFAA litigation include what sort of intent a defendant must have to violate the statute, and whether the breach of access-contracts can give rise to criminal liability. Additionally, the practical differences between unauthorized access to private secured servers and public websites will be addressed in the context of judicial interpretations of the CFAA.

---

[63] Many CFAA cases are not criminal, but are instead prosecuted civilly. The CFAA makes civil claims available for certain violations falling within the CFAA. A civil CFAA cause of action must also include one of the five sub-factors present in 1030(c)(4)(A)(i). Included in these sub-factors is a loss of over $5000, which is used in many cases to meet the requirement. Civil cases are more common than the criminal cases and they provide a majority of the precedent. However, looking to these cases, it is important to consider the differences in standards of proof and the lack of procedural protections that may be present in a criminal case like lenity and Fifth and Sixth amendment rights. Civil cases, however, still provide a body of law which judges rely on when disposing of all CFAA cases, criminal or civil.

[64] *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 368-69 (D. Conn. 2001) (Ivanov hacked computer system, threatened to destroy it and tried to extract a consulting fee out of company to help secure their network); United States v. Czubinski, 106 F.3d 1069, 1078-79 (1st Cir. 1997) (person convicted for hacking into and browsing through IRS files, but not sending or downloading that information).

[65] 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)).

[66] *See* Jones v. Bock, 549 U.S. 199, 220 (2007); TRW Inc. v. Andrews, 534 U.S. 19, 38 (2001).

1. INTENT

There is a competing view among some circuits as to whether the intent of the accessor determines if the access is authorized or not. Typically, this scenario involves an employee of a company accessing company records while authorized as a current employee, but with the intent to take privileged information with him or herself to a competing employer.[67] Some courts hold, based on an agency theory, that even when fully authorized, if the employee has the intent to access the records for an unapproved purpose, then he or she is violating the CFAA.[68] Essentially, the cases diverge on statutory interpretation, and the better reasoned cases look to the strict wording of the statute, which turns on whether the access is authorized and not the specific use the attained information is going to be put to. Thus, if the access is authorized, how the information is eventually used is irrelevant. So, if the access was authorized the CFAA analysis ends, and there is no violation. While here, the intent issue is really a sub-part of the larger contractual, TOS-based theory used by the Drew prosecutors, intent alone could be a way in which a CFAA violation can be fabricated despite a user meeting all

[67] *See, e.g.*, Othentec Ltd. v. Phelan, 526 F.3d 135 (4th Cir. 2008) (claim against former employee for violation of CFAA); Patriot Homes, Inc. v. Forest River Housing, Inc., 512 F.3d 412, 413 (7th Cir. 2008) (plaintiff home builder sued four former employees for copying from plaintiff's computers their proprietary home designs and using them in new venture); Fiber Systems Intern. Inc. v. Roehrs, 470 F.3d 1150, 1155 (5th Cir. 2006) (suit against former corporate officers who were bought out and then took companies' trade secrets and other propriety information with them without authorization).

[68] *Compare* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (finding agency theory of authorization), and International Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (recognizing agency theory), *with* Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005) (rejecting agency theory); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933-36 (W.D. Tenn. 2008) (rejecting agency theory); Lockheed Martin Corp. v. Speed, 2006 U.S. Dist. LEXIS 53108, 2006 WL 2683058 at * 4 (M.D. Fla. 2006) (rejecting agency theory based on plain meaning of CFAA and finding that employees were authorized to access the company computer).

terms laid out by a website. Hence, it is worthwhile to analyze whether the intent-based approach is tenable and should be used by courts to determine if a CFAA violation has occurred.

For example, in *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc*., the district court for the Western District of Washington held that based on the Restatement (Second) of Agency, once employees accessed their current employer's computers for the purpose of attaining information to transfer to their future employer, they were acting without authorization because authorization terminated when they allegedly became agents of the competitor during the act.[69] Therefore, according to *Shurgard,* when a user is fully authorized – even under contract – but accesses information the purpose of taking it to a new employer or to commit fraud, his or her access is withdrawn.[70] This analysis ignores the plain wording of the CFAA, which focuses solely on whether authorization exists, and is not persuasive. The defendants in *Shurgard* were authorized, and the court mistakenly focused on their intent to find a CFAA violation. The focus should instead be on authorization, and while in *Shurgard*, the plaintiff's CFAA claim would fail because the access was authorized, plaintiffs in similar factual situations would still have other viable claims like misappropriation of trade secrets, conversion, and unfair competition (which were also pursued in the *Shurgard* case). Again, *Shurgard* is not persuasive because it takes the focus away from whether the access at the time was factually authorized and instead looks to the intent of use which, as Congress has made clear, is irrelevant.[71]

---

[69] *Shurgard,* 119 F. Supp. 2d at 1124-25.

[70] *Id.*

[71] *See supra* Section II A.

The district court for the District of Maryland presented a better reasoned view in *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, following the plain wording of the CFAA.[72] The *Werner-Masuda* court refused to use intent or purpose to determine whether the access was authorized. Instead the court looked at whether the user in question was authorized at the time of access.[73] In following the clear wording of the statute, the *Werner-Masuda* court made a clear distinction: "the CFAA, however, do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do [its] terms proscribe authorized access for unauthorized or illegitimate purposes."[74] Further, the court supported this conclusion by referring to the legislative history surrounding the 1986 amendment to the CFAA, which specifically intended to prohibit only unauthorized access, shifting the focus away from the purpose for the access which was a "murky ground for liability."[75]

Courts have since noted that accepting an agency theory like *Shurgard*'s would "inappropriately expand federal jurisdiction by broadly sweeping in conduct in which a defendant accesses a company computer with 'adverse interests.'"[76] Intent serves no relevant role when determining whether access was authorized or not.[77] Were the CFAA

---

[72] *Werner-Masuda,* 390 F. Supp. 2d at 498-99.

[73] *Id.* ("It is undisputed Werner-Masuda was authorized to access VLodge, and to use such access to obtain the information on the membership list. Thus, under the plain language of the statute, she did not exceed her authorized access by accessing and/or obtaining Plaintiff's membership information.").

[74] *Id.* at 499.

[75] *Id.* at 499 n.12 (citing S. REP. NO. 99-432, at 21).

[76] US Bioservices Corp. v. Lugo, --- F.Supp.2d ----, 2009 U.S. Dist. LEXIS 4101, *11 (D. Kan. 2009) (citing Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008)).

[77] *Shamrock*, 535 F.Supp.2d at 966 ("the legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information.")

to specifically limit *the use of* legitimately attained information, then intent might be relevant; however, it does not.

Thus, under the *Shurgard* intent framework, Drew would be liable because her access and use of the MySpace servers was for an illegitimate purpose. That result, however, is erroneous and ignores the question of whether the access at its core was authorized. Additionally, the harm in the Drew case does not factually stem from the access Drew had to the MySpace servers, but what she did with that information once she had attained it – using it to inflict emotional distress on Megan Meier. The plain meaning of the CFAA and the reasoning adopted in *Werner-Masuda* should control, and authorization should not turn on use or purpose. Intent is an improper framework under which to use the CFAA, which focuses on authorization and not intent. Thus, once authorization is given, the CFAA is out of play. Focusing on intent ignores the original purpose of the CFAA: to prevent hacking or unauthorized access. A violation occurs when a hacker gains unauthorized access to a system, and whether the hacker has the intent to use the obtained information for good or bad is irrelevant. It is the unauthorized access itself which is the violation.

While Drew may have accessed MySpace.com servers with the intent to harass Megan Meier, such intent is irrelevant under the correct application of the CFAA. The CFAA criminalizes hacking, or unauthorized access. The intent to harass Megan Meier does not in itself make access unauthorized. The question for CFAA cases is solely whether the defendant was authorized to access the servers. Specifically, for the theory behind the Drew case, this turns on whether contracts can act as a de facto criminal statute outlining what conduct can lead to a violation of the CFAA.

2. CONTRACT

Another crucial legal issue in the Drew case is the effect of contracts in determining whether access is authorized or not. Some CFAA cases discuss theories claiming that confidentiality or do-not-compete contracts between employers and their breaching employees create evidence of unauthorized access.[78] In rejecting this same argument, the district court for the Eastern District of Pennsylvania Court stated in *Brett Senior & Associates, P.C. v. Fitzgerald* that:

> [I]n looking to the use to which an employee is permitted to put information, the cases often make the existence of a confidentiality or non-compete agreement dispositive of liability under the CFAA. It is unlikely that Congress, given its concern "about the appropriate scope of Federal jurisdiction" in the area of computer crime, intended essentially to criminalize state-law breaches of contract.[79]

There, the court refused to find a CFAA violation, notwithstanding the fact that the defendant had signed a confidentiality agreement and then had procured and given information attained from his former employer to a competitor.

Some courts, however, have recognized that terms of service violations can lead to a CFAA violation.[80] Those cases, however, are consistently different

---

[78] *See, e.g.*, *Werner-Matsuda,* 390 F. Supp. 2d at 498-99 (rejecting contention that registration agreement created liability under the CFAA); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1335 (N.D. Ga. 2007) (rejecting use of confidentiality agreement to show violation of CFAA); Brett Senior & Associates, P.C. v. Fitzgerald, 2007 WL 2043377 (E.D. Pa. 2007) (refusing to construe violation of confidentiality agreements as violation of CFAA).

[79] *Fitzgerald*, 2007 WL 2043377 at *4 (citing S. REP. 99-432, at 3 (1986)).

[80] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) (noting that "[a] lack of authorization could be established by an explicit statement on the website restricting access," giving rise to a CFAA violation if a website user thereafter violated the terms of use); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-82 (1st Cir. 2001) (finding that defendant's use of a computerized "scraper" to glean information from plaintiff's website likely exceeded authorized access where such use at least implicitly violated a confidentiality agreement);

from the Drew case. These cases are generally older, and all deal with civil claims between large corporations. Therefore, the loss of personal liberty via criminal charges was not contemplated by the court in accepting such a broad application of the CFAA.[81] Additionally many of cases involved prior notice of a violation of the TOS and only after repeated offenses was a CFAA claim pursued. All of these cases are extremely distinct from the Drew case. A contract-based approach has been viewed as contrary to legislative intent and unwise, and the problems are only compounded when enforcement is sought against individuals criminally.[82]

The conclusion that breaches of contract should not rise to the level of CFAA violations is grounded in legislative history, and is precisely on point for the Drew case. In the Drew case, the prosecutors argued that a contract (the MySpace.com terms of service) is what set the parameters for authorized access. However, based on legislative

---

Southwest Airlines v. Farechase, Inc., 318 F. Supp. 2d 435, 439-40 (N.D. Tex. 2004) (finding that Southwest sufficiently stated CFAA claim where Southwest had directly informed the defendant that its scraping of southwest.com was unauthorized); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000) (finding that plaintiff successfully established that defendant's use of its website was unauthorized within the meaning of the CFAA simply by virtue of the fact that plaintiff objected to the defendant's use); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (concluding that defendants' use of AOL membership to harvest e-mail addresses of AOL users was unauthorized because such actions violated AOL's terms of service).

[81] Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 476 (noting that "the division the courts seem to be creating between enforceability against businesses and enforceability against individuals" makes enforcement less likely as to individuals); *see also* Canada Dry Corp. v. Nehi Beverage Co., 723 F.2d 512, 526 (7th Cir. 1983) ("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.").

[82] *See, e.g.*, *Werner-Matsuda,* 390 F. Supp. 2d at 498-99; Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 368 (2004); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1600 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 528 (2003).

history, judicial interpretation, and a logical reading of the statute, relying on contracts to establish violations is misplaced – especially in the context of criminal penalties.

The goal of the CFAA is to protect against unauthorized access. It was not intended to act as means of criminalizing private contracts. The refusal by courts to recognize confidentiality or employment agreements as an avenue to show a CFAA violation illustrate that. And while a confidentiality or employment contract may operate as a precursor to gaining employment and access to computer systems needed to work, a violation of the agreement does not then make the employee an unauthorized user. Similarly, a violation of the terms of service, while a precursor to use, should not be used to create criminal liability.

If courts are willing to reject confidentiality and non-compete agreements when deciding the scope of authorized access, then courts should not consider an adhesive, non-bargained terms of service agreement for a public website as defining the scope of authorized access. Allowing contracts of adhesion to create a *criminal* violation under the CFAA, but similarly refusing to use employment contracts of more equal bargaining as a basis for *civil* violations of the CFAA is an absurd result. The issues of adhesion contracts and unequal bargaining will be further addressed in Section III A below; however, the Drew case serves as a clear example of why private contracts should not be capable of creating criminal liability. Lori Drew is facing charges for failing to follow the MySpace terms of service, a contract she may have never seen or read, yet could lead to her incarceration.

3. PRACTICAL DIFFERENCES BETWEEN PRIVATE, SECURED SERVERS AND PUBLIC WEBSITES

MySpace.com is the sixth most popular website in the world[83] and has more than 106 million accounts.[84] It is not within MySpace's business model to exclude users; this is evidenced by its daily traffic and membership alone. Therefore, MySpace does not limit access, and anyone can create an account—its servers are effectively open to all. What MySpace does do is provide rules and guidelines for use to protect MySpace.com legally and provide a better user environment for its customers. MySpace.com is very different and much more accessible than the protected banking and healthcare computer systems that the CFAA was originally created to protect.

To that point, there is a very logical distinction between protecting a private secured computer from hackers, and limiting access from undesired users on public websites. This theory was discussed by the district court for the Northern District of Texas in *Southwest Airlines Co. v. BoardFirst, L.L.C.* There, the court denied the plaintiff's motion for summary judgment as to its CFAA claims.[85] Further, the court discussed a shift in CFAA interpretation and whether terms of service for websites really act as a precursor for access. The court recognized that the CFAA does not forbid the use of a protected computer for any purpose; rather, that it just prevents access without authorization. And to that effect, the court noted that Southwest Airlines' website, which was the focus of the case, "is a publicly available website the access to which is not

[83] Global Top Sites, http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none.

[84] Faultline, *MySpace Music Deal Poses Multiple Threats*, http://www.theregister.co.uk/2006/09/08/myspace_threatens_record_labels/.

[85] Southwest Airlines Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 (N.D. Tex. Sept. 12, 2007).

protected by any sort of code or password."[86] This discussion illustrates the very distinct circumstance of where a hacker gains access to a protected and private computer system and when the user of a fully available public website violates its terms of use. The two scenarios are clearly distinct, and as the court in *BoardFirst* hinted at, that is why it would be unreasonable to extend the CFAA from the former to the latter. As a practical matter, protecting the integrity of private contracts was not the intent of the CFAA. Instead, its goal was to protect secured information. Private contracts should not be criminalized, especially when those contracts are adhesive and may be open to judicial scrutiny, which will be discussed in greater detail in Section III below.

Looking at CFAA cases, it becomes clear that hacking and unauthorized use was the conduct that the statute was trying to deter and criminalize. In fact, out of all the U.S.C. 1030(a)(2)(c) criminal cases the writer could find, *all* dealt with accessing information using hacking skills or other tresspatory means.[87] At their roots, none of the violations were caused by attaining access by violating and ignoring the terms of service agreements. Strictly viewed, if complying with the terms of service are a necessary step in being an authorized user then, yes, those who violate the terms of service to access a website could be in violation of the CFAA. However, this interpretation flies in the face of legislative intent and the track record of CFAA criminal cases, where the criminal

[86] *Id.* at *44 (citing America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000) (questioning whether an AOL member's violation of the membership agreement would make them an unauthorized user).

[87] *See, e.g., Ivanov*, 175 F. Supp. 2d at 367 (Russian citizen hacked a U.S. corporation's servers and attained control over its entire network, then attempted to extort money from them); United States v. Willis, 476 F.3d 1121 (10th Cir. 2007) (aiding and abetting by providing passwords to someone who did not have access); United States v. Dearman, 218 F. App'x 800 (10th Cir. 2007) (challenging validity of conviction for obtaining information to perpetrate bank theft). It is additionally noteworthy that of the sixty-one cases that mention subsection (a)(2)(c) only eight are criminal cases(two of which recognize in a footnote that the CFAA claim was voluntarily dismissed) and the rest are civil actions.

activity did not spring from a contractual obligation, but instead was the result of unauthorized access to a computer on the part of the accused.

The legislative history surrounding the CFAA makes its target clear: tresspatory hacking. The CFAA was never intended to handle situations of cyber-harassment. Using a statute designed to deter and punish hacking to address an entirely different social ill is misguided at best. The result of such a stretch will be further illustrated in Section III below, but hacking and cyber-harassment are clearly different offenses, requiring entirely different actions to further each act. The focus of hacking is on unauthorized access, whereas cyber-harassment involves interaction between individuals, not specific invasions of, and transmissions between servers. The Drew case not only struggles to fit within the pre-existing legal framework of the CFAA, but the articulated extension also serves to create a number of undesirable practical and legal issues.

III. THE POLICY IMPLICATIONS OF 18 U.S.C. § 1030 AS APPLIED IN THE DREW CASE

This section discusses what the practical effects will be if the extension in the Drew case is recognized to be sound law. Subsection A will demonstrate that many of the contracts and Terms of Service agreements that federal prosecutors would use to create criminal liability are contracts of adhesion and therefore should not be used as a basis for criminal liability. Subsection B will highlight that the extension of the CFAA as articulated in the Drew case would effectively privatize the writing of criminal statutes. Subsection C will show that a contract-based extension of the CFAA would make it void for vagueness. Subsection D will show that the extension of the CFAA is necessarily overbroad and would criminalize such a wide range of activity that the extension is

unsustainable. Finally, subsection E will close with further examples of how the Drew case's extension of the CFAA would lead to more unwanted results.

The prosecutors in the Drew case argue that Drew and her conspirators became unauthorized users by violating the MySpace.com terms of service.[88] The relevant portions of the MySpace.com terms of service, as stated by the prosecutors, require that users:

> a. provide truthful and accurate registration information;
> b. refrain from using any information obtained from MySpace services to harass, abuse or harm other people;
> c. Refrain from soliciting personal information from anyone under 18;
> d. Refrain from promoting information that they knew was false or misleading;
> e. Refrain from promoting conduct that was abusive threatening, obscene, defamatory or libelous; and
> f. Refrain from posting photographs of other people without their consent.[89]

Ms. Drew violated these terms, according to the indictment, by creating a MySpace account "under a fictitious name", obtaining "information from a juvenile MySpace member", and "using Myspace to torment, harass, humiliate, and embarrass the juvenile Myspace member."[90]

The Drew prosecutors' reliance on MySpace.com's terms of service makes clear that *but for* those terms, the prosecutors would be unable to charge Drew. Essentially, Drew's activity is only criminalized when referenced in light of the terms of service. This contract-based approach to prosecuting CFAA cases has serious implications for all internet users.

---

[88] Indictment, *supra* note 5, at 4-5; MySpace.com, *Terms & Conditions*, http://www.MySpace.com/index.cfm?fuseaction=misc.terms.

[89] Indictment, *supra* note 5, at 4-5.

[90] *Id.* at 5.

A. ADHESION

Terms of service ("TOS") agreements can come in multiple forms. For some websites, one must have a user account to access the essential functions of the website. MySpace.com is an example of this. Other websites do not require a user account to use core functions. The difference between the two is relevant for TOS agreements because typically, when a person creates a user account at a website, he or she is generally required to confirm that he or she has read and agreed to the site's TOS by clicking a button or checking a box.[91] Websites that do not require a user account or clear assent to a TOS agreement normally just post a link to the TOS somewhere on their home page and leave it to the user to find and decipher the terms on which he or she can use the website.[92] In the latter case, a user's continued presence on a website and use of the website's services is generally claimed to be assent to the terms.[93] The degree of involvement by users is an important consideration in all contracts, including web-based

[91] *See, e.g.*, MySpace.com, *Signing up For MySpace, Now with Free Music*, http://signups.MySpace.com/index.cfm?fuseaction=signup (requiring entry of account information and then providing a box to check which states "[b]y checking the box, you confirm that: You agree to the MySpace Terms of Service and Privacy Policy."); Yahoo.com, *Yahoo! Registration*, www.yahoo.com (visit website and click signup) (requiring entry of personal information and that the user check a box certifying that "I have read and agree to the Yahoo! Terms of Service and Yahoo! Privacy Policy").

[92] *See, e.g.*, Google.com, *Terms of Service*, http://www.google.com/intl/en/privacy_terms.html; youtube.com, *Terms of Service*, http://www.youtube.com/t/terms; Live.com, *Microsoft Service Agreement Last Updated: September 2008*, http://help.live.com/help.aspx?project=searchtou&market=en-us.

[93] *See* Google.com, *supra* note 92 ("You can accept the Terms by … actually using the Services. In this case, you understand and agree that Google will treat your use of the Services as acceptance of the Terms from that point onwards.").

TOS agreements.[94] Thus, whether TOS agreements have been seen or ratified by the user should be a factor in determining enforceability.[95]

TOS agreements are authored either by the individual webmasters, or, when the websites are more sophisticated, by an attorney or legal department. This is noteworthy, because the logical tendency of those writing the contract is to make the terms as beneficial to themselves or the party that they are creating the contract for.[96] Thus, website TOS agreements, like many click-wrap, mass-market contracts, tend to favor the drafter of the contract.[97]

There is a strong, and reasonable, belief that mass-market contracts are rarely read by the people they bind.[98] TOS agreements on websites are no exception to this, and in fact may tend be ignored to a greater degree than other contracts that are in the form of a printed purchase or warranty agreement, or even the typical click-wrap contract which requires scrolling through of the document and confirming that it was "read."[99] Courts are

---

[94] RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. b (1981) ("Customers do not . . . ordinarily understand or even read the standard terms."); Alan M. White & Cathy Lesser Mansfield, *Literacy And Contract*, 13 STAN. L. & POL'Y REV. 233 (2002) (many consumers do not read or understand contracts they regularly enter into).

[95] White & Lesser, *supra* note 94; Jennifer Femminella, *Online Terms And Conditions Agreements: Bound By The Web*, 17 ST. JOHN'S J. LEGAL COMMENT. 87, 101-06 (2003) (arguing web-wrap agreements do not satisfy the contract principle of mutual assent); Drew Block, *Caveat Surfer: Recent Developments in the Law Surrounding Browse-Wrap Agreements, and the Future of Consumer Interaction with Websites*, 14 LOY. CONSUMER L. REV. 227, 232 (2002) ("There is a clear difficulty in fitting browse-wrap agreements into the traditional context of contract law.").

[96] William J. Condon, Jr., *Comments And Notes: Electronic Assent To Online Contracts: Do Courts Consistently Enforce Clickwrap Agreements?* 16 REGENT U.L. REV. 433, 437 ("Contracts of adhesion tend to be one-sided, favoring the drafter.").

[97] *Id.*; Christina L. Kunz & John E. Ottaviani, *Browse-Wrap Agreements: Validity Of Implied Assent In Electronic Form Agreements*, 59 BUS. LAW. 279, 289 (2003) (recognizing competition between business could make terms more favorable for consumers).

[98] *See, e.g.*, White, *supra* note 94, at 234.

[99] Femminella, *supra* note 95.

weary of click-wrap or other adhesive contracts when they are substantively unfair or lack adequate notice.[100] In some instances, courts have refused to bind users to the terms of such contracts.[101] Additionally, courts have recognized that browsewrap contracts can be unenforceable when the website "fails to provide adequate notice of the terms, and there is no showing of actual or constructive knowledge."[102] The reluctance of courts to bind users to click-wrap or browsewrap contracts shows how absurd it would be to allow civilly unenforceable contracts to lead to *criminal* liability.[103]

---

[100] Kaustuv M. Das, Ph.D., Note & Comment, *Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the "Reasonably Communicated" Test*, 77 WASH. L. REV. 481, 491 ("In examining forum-selection clauses in adhesion contracts, courts have looked to the adequacy of notice"); Condon, *supra* note 95 at 437 ("Consequently, courts under the doctrine of unconscionability require substantive fairness in such contracts.")

[101] *See, e.g.*, Carnival Cruise Lines, Inc. v. Superior Court, 234 Cal. App. 3d 1019 (1991) (holding that "that the forum-selection clause is unenforceable as to any particular plaintiff if the court determines that such plaintiff did not have sufficient notice of the forum-selection clause prior to entering into the contract for passage"); Berman v. Cunard Line, Ltd., 771 F. Supp. 1175, 1177-78 (S.D. Fla. 1991) (refusing defendant's motion to transfer to contract-based forum because defendant had not controverted plaintiff's claim that she was unaware of the forum-selection clause in the ticket); Das, *supra* note 100, at 492 ("courts have interpreted [the Supreme Court's] *Shute* [decision] to imply that notice is required for enforcement of forum-selection clauses contained in adhesion contracts.")

[102] Southwest Airlines Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *16 (N.D. Tex. Sept. 12, 2007); *see also* Specht v. Netscape Communications Corp., 306 F.3d 17, 32 (2d Cir. 2002) (holding that, because Netscape's terms were not readily available, plaintiffs "were not placed even on constructive notice of the existence of such terms, and thus were not bound by them."); Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. LEXIS 4553, 2000 WL 525390, at *3 (C.D. Cal. March 27, 2000) (dismissing Ticketmaster's breach of contract claim where the terms and conditions were situated at the bottom of the home page in "small print").

[103] Tarra Zynda, *Ticketmaster Corp. v. Tickets.Com, Inc.: Preserving Minimum Requirements of Contract on the Internet*, 19 BERKELEY TECH. L.J. 495 (2004) ("The differences between shrinkwrap and browsewrap licenses warrant a separate analysis of browsewrap licenses"); *cf.* Susan Randall, *Judicial Attitudes Toward Arbitration and the Resurgence of Unconscionability*, 52 BUFF. L. REV. 185, 186 (2004) (stating that judges find "arbitration agreements unconscionable at twice the rate of nonarbitration agreements).

B. PRIVATIZATION

Because TOS agreements are left entirely to the devices of website owners, the result of using the CFAA to criminalize TOS agreements essentially delegates the creation of criminal laws to individuals and corporations that run websites and write TOS agreements. In fact, Ms. Drew's attorneys unsuccessfully argued in a motion to dismiss that extending the CFAA to enforce TOS agreements would "delegate the responsibility of deciding what conduct will be criminal to private parties."[104] The theory rested on three Supreme Court cases that rejected the delegation of power to governmental agencies contrary to the delegation of power set by the Constitution.[105] Not only is this extension of the CFAA a delegation of prosecutorial power as argued by the Drew defense, but it also seems that a strong argument can be made that the prosecutors are essentially delegating the legislative function of lawmaking to ordinary citizens and corporations who manage websites and author TOS agreements.[106]

Such an extension would allow a website operator, for example, to set limits on public discussion of religion on the website's forum. If anyone did discuss religion on the website, a record of their action could be forwarded on to prosecutors for a violation of the CFAA. Any activity could be criminalized. Such a result puts criminal law in the

---

[104] United States v. Drew, Notice of Motion; Motion To Dismiss Indictment-Unconstitutional Delegation Of Prosecutorial Power; Points And Authorities, Case No. CR-08-582-GW, Sept. 4, 2008.

[105] Carter v. Carter Coal Co., 298 U.S. 238 (1936); A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935); Panama Refining Co. v. Ryan, 293 U.S. 388 (1935).

[106] Clinton v. City of New York, 524 U.S. 417, 478 (1998) ("The legislature cannot delegate its power to make a law; but it can make a law to delegate a power.") (citation omitted); Loving v. United States, 517 U.S. 748, 772 (1996) ("Congress may not delegate the power to make laws and so may delegate no more than the authority to make policies and rules that implement its statutes.").

hands of the public to wield, without any check or wisdom required by the traditional law-making process.

C. VOID FOR VAGUENESS

The range of activity which could be criminalized under the contract theory of authorization—which is virtually unlimited—could render the CFAA void under vagueness because the statute would "fail to provide the kind of notice that [would] enable ordinary people to understand what conduct it prohibits."[107] In fact, the CFAA under a contract-based theory would not only be vague, but it would be completely unpredictable.[108] The scope of prohibited conduct would only be limited by the imagination of webmasters authoring terms of service agreements.

D. OVERBROAD

A contract based approach to the CFAA would increase its reach exponentially. Additionally it would give prosecutors the power to selectively prosecute among the numerous violations. This broad power would necessarily chill Internet use. It is worthwhile to look at a few current websites' TOS to illustrate just how overbroad the criminally enforceable TOS would be in practice.

---

[107] City of Chicago v. Morales, 527 U.S. 41, 56 (1999).

[108] Coates v. City of Cincinnati, 402 U.S. 611, 614 (1971) (law against three or more people congregating 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.").

MySpace.com serves again as a good example of potential liability. The MySpace.com TOS make it a violation if one "solicits personal information from anyone under 18."[109] Thus, if two relatives were registered users on MySpace and both were under the age of 18, and they were to solicit any personal information from the other, a violation would occur under the theory as presented by prosecutors in the Drew case. This result is especially odd when contrasted with the mission of MySpace.com as stated in the terms of service: "[MySpace] is a social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and new friends."[110] Oddly, the very purpose for which MySpace was created could lead to a violation of the CFAA and criminal prosecution.

Similarly, Match.com's terms of service require that all users of the website "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."[111] Therefore, if anyone who was married or under the age of 18 either registered for an account or even accessed the website, they would be open to criminal charges through the CFAA.

The Craigslist.org TOS also serves to show just how flawed the contract based approach to CFAA criminal prosecutions would be. Craigslist forbids people from "post[ing] the same item or service in more than one classified category or forum, or in more than one metropolitan area."[112] In this example, if a person living in Los Angeles and commuting to Orange County posted sports tickets for sale in both the "Los Angeles"

---

[109] Terms & Conditions, *supra* note 88, at 8.5.

[110] Terms & Conditions, *supra* note 88, at preamble.

[111] Match.com, *Terms of Use Agreement*, at 2, http://www.match.com/registration/membagr.aspx.

[112] Craigslist, *Terms of Use*, at 7, http://www.craigslist.org/about/terms.of.use.

and the "Orange County" sections of Craigslist, he or she would be an unauthorized user under the CFAA contract-based authorization approach and susceptible to criminal charges.

The above examples come from legitimate websites and terms of service agreements that were likely drafted by attorneys specializing in cyber law; however, there is no distinction in the CFAA, which would limit the contract-based approach only to legitimate websites. In fact, the possibility that the CFAA could be used by someone with an illegitimate purpose presents with disturbing clarity the danger of extending the CFAA.

For example, if a webmaster were to preclude all access to his or her website, any daring or confused web-surfer who entered that website would be susceptible to criminal charges. Truly devious manipulations of the contract-based approach to the CFAA would likely not occur in such a straightforward way. Webmasters could bury the most controversial terms deep within their terms of service and they could modify them regularly, making them unpredictable. Webmasters would have sole discretion to criminalize any conduct. They could create TOS agreements that disallowed access based on gender, age, race or any other factor they so desired, and if those excluded users accessed the website in question a technical violation of the CFAA would result. That is what is so troubling about the extension of law attempted in the Drew case—it has no rational limit.

E. ADDITIONAL EXAMPLES OF UNSOUND RESULTS

The contract-based extension could also have serious implications for corporate America. If an employee of one company accessed the public website of another, that

employee could be criminally liable if the website's TOS agreement states that no agents from competing companies can access the site.[113] Additionally, if the intent to access was considered a factor, an employee would be criminally liable for exceeding authorized access if they were looking for competitive intelligence on their competitor's website and the website similarly stipulated that such activity was prohibited. At a minimum, the legal extension happening in the Drew case will cause large companies to reevaluate their computer use and outside access policies to not only protect corporate interests, but individual employees as well.[114]

There are numerous undesirable side effects of extending the CFAA. Since most websites' TOS require a person to register their account with accurate information, a contract-based approach to authorization would prevent people from maintaining their anonymity online. This lack of anonymity would have a chilling effect on the First Amendment guarantee of freedom of speech.[115] Therefore, if the CFAA as applied in the Drew case were to effectively end the ability to communicate anonymously online, the statute could face First Amendment challenges.[116] Additionally, anonymity can be used

---

[113] James Eiszner, *Criminal Exposure For Competitive Intelligence Gathering On The Internet: Lessons From The Fallout Of The Myspace Suicide Case, Under Scrutiny: SHB's Government Enforcement & Compliance Update*, el.shb.com/nl_images/SHBWebsite/Newsletters/GECU/GECU8108.pdf.

[114] *Id.* at 3.

[115] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("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."); Doe v. 2themart.com Inc., 140 F. Supp. 2d 1088, 1092. (W.D. Wash. 2001) ("Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas. The ability to speak one's mind on the Internet without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate.") (citing Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999)) (internal quotations omitted).

[116] *McIntyre*, 514 U.S. at 357 ("[a]nonymity is a shield from the tyranny of the majority . . . [that] exemplifies the purpose [of the First Amendment] to protect unpopular individuals from

to protect vulnerable groups such as children[117]; however, if a child cannot remain anonymous online and must share his or her personal information, children may become more susceptible to predatory and harassing behavior—a harm the prosecutors in the Drew case think they are addressing, not compounding.

Allowing a website's TOS lead to criminal liability highlights the disconnect between traditional legal constructs and the rapidly evolving internet, which is not always suitable to such a framework.[118] There are no limits on the degree to which conduct could be criminalized; however, the examples from legitimate websites prove to show how the contract-based approach for authorization could criminalize the daily actions of millions of people. The unforeseen effects on anonymous communication also serve to show the serious legal implications that such an extension of law could create. Finally, these examples illustrate the power prosecutors would possess, entitling them to selectively choose who to prosecute among the millions of CFAA violations that would occur daily.

While the legal precedents discussed above in section II may not provide an absolute conclusion on how the CFAA should be used, the practical effect of making TOS agreements criminally enforceable leaves no doubt that the law should not be

---

retaliation … at the hand of an intolerant society."); 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); *2TheMart.com Inc.*, 140 F. Supp. 2d at 1092 ("The right to speak anonymously extends to speech via the internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas.").

[117] Get Safe Online, *Protect Children From Online Threats***,** http://www.getsafeonline.org/nqcontent.cfm?a_id=1124 (suggesting that children "[u]se a nickname, not your real name" to protect their safety online, which would run contrary to numerous terms of service agreements that require complete and accurate information).

[118] *See generally* Kerr, *supra* note 82, at 1602 (discussing shift in concepts between property law and offenses such as trespass and how these concepts may not work in the modern and evolving field of internet law).

extended in this manner. In trying to address the harm of cyber-harassment present in the Drew case, the extension of the CFAA would do much more than criminalize cyber-harassment. It would criminalize a great deal of currently legitimate internet usage and possibly bring lively discourse to a halt. To address the social ill of cyber-harassment, lawmakers should look not to the CFAA but to alternatives, such as new legislation carefully crafted to address such harms.

IV. LEGISLATIVE RESPONSES TO THE DREW CASE

In light of Megan Meier's tragic suicide and the revelation of the events surrounding her untimely death, her hometown of Dardenne Prairie, Missouri passed an anti-cyber-harassment and stalking resolution and accompanying ordinance.[119] The ordinance makes cyber-harassment occurring within Dardenne Prairie a misdemeanor.[120] The ordinance focuses on a "course of conduct" of harassment between a minor and someone over the age of 18 that "serves no legitimate purpose and would cause a reasonable person to suffer substantial emotional distress" and would "cause a reasonable parent to fear for the well-being of their minor child who is the target of the contact."[121]

This ordinance paints a broad brush and does not require actual harm to occur. It attempts to limit its scope by using an objective standard; however, it has come under fire for being too broad. Since the Dardenne Prairie ordinance's passage, more than seven

---

[119] Resolution No. 195 (Nov. 21, 2007), http://www.dardenneprairie.org/forms/CyberHarassmentResolution.pdf; Ordinance No. 1228 (Nov. 21, 2007), http://www.dardenneprairie.org/forms/CyberHarassmentOrd.pdf.

[120] Ordinance No. 1228, *supra* note 119.

[121] *Id.* at 1-4.

people have been charged under it.[122] An attorney representing someone charged under the ordinance has stated that the law was hastily passed and poorly written, in an attempt to appease public outrage over the Drew case.[123] Whether the Dardenne Prairie ordinance will be challenged or struck down is a question that remains to be answered. What is clear is that the new statute does give law enforcement a tool to address a previously non-criminalized social ill. It may be a new and rudimentary tool, but it is one that can be honed and refined to better protect individuals in the future and put everyone on notice as to what type of behavior is considered criminal. It is likely that the Dardenne Prairie statute may need to be further focused and reworked much like the CFAA has been amended numerous times throughout its existence. This refinement, however, will lead to a better law that protects the public and gives fair notice to possible violators.

It is noteworthy that other states have passed legislation dealing with cyber-harassment, specifically protecting children from harassment by their peers and from adults as well.[124] Despite the many statutes that states have passed attempting to address cyber-harassment, it is unclear if many of them would criminalize what Drew did to Megan Meier. Most statutes require threats or clearly harassing messages to be sent. What Drew did was much more subtle and may not be caught by such statutes. It is a

---

[122] Kim Zetter, *Prosecutors Charge 7 People Under New Cyberbullying Law*, http://blog.wired.com/27bstroke6/2008/12/seven-people-ch.html.

[123] *Id.*

[124] *See, e.g.,* Or. Rev. Stat. §§ 163.730-.732, 166.065; Cal. Civil Code § 1708.7; Cal. Penal Code §§ 422, 646.9, 653m; *see generally* National Conference of State Legislatures, State Electronic Harassment or "Cyberstalking" Laws, http://www.ncsl.org/programs/lis/cip/stalk99.htm.; Working to Halt Online Abuse, Cyberstalking Laws, http://www.haltabuse.org/resources/laws/index.shtml (list of pending or passed cyber-stalking legislation).

fine line to walk because there is a risk of criminalizing too broad a range of activity, leading to the problems created by extending the CFAA.

The clear failure of the CFAA to adequately address cyber-harassment necessitates that new laws be drafted. In fact, the use of the CFAA in the Drew case independently illustrates the need for more appropriate laws. Lori Drew participated in despicable acts, and there were no laws criminalizing her actions. The use of the CFAA was a last resort attempt by prosecutors to quench the public's thirst for justice.

Legislation addressing cyber-harassment must accomplish four essential tasks: 1) it must clearly define the victims it intends to protect and the activity it intends to criminalize to deter behavior similar to what happened in the Drew case and to protect those susceptible to *actual harm* from such behavior; 2) it must be limited in scope as not to criminalize behavior or actions outside of the scope of cyber-harassment, thereby preventing prosecutors from having too much discretion or even defeating the statute by having it being ruled unconstitutionally vague; 3) it must carefully consider the jurisdictional and venue issues ensuring the venue has a connection to the crime and the defendant; and 4) it must be clearly constructed, sharply limited and changed frequently to address new technology and the social problems that arise from the use of that technology.

A carefully constructed statute to address cyber-harassment is needed. State-based approaches are more likely to be fruitful, because each state can act as a laboratory tweaking what the statute criminalizes and having a federal statute on the matter could create the same jurisdictional issues as mentioned above. It should be a priority of the states to address an increasingly common and serious social ill in cyber-harassment.

V. CONCLUSION

The Drew case is a series of tragedies. What happened to Megan Meier was a tragedy. The lack of a law to properly bring Lori Drew and her cohorts to justice was also a tragedy. And the extension of the CFAA well beyond its rational bounds may also turn out to be a tragedy, should the prosecutor's theory survive on appeal. This case epitomizes a very human reaction to the unnecessary loss of life. However, appalling facts should not prevent us from seeing the treacherous extensions of the law. So, while Lori Drew may escape prosecution for what she has done, it is important to respect the rule of law, and write new laws that will properly address such actions in the future. Otherwise, the Drew case becomes a situation where bad facts create bad law.

The CFAA has functioned effectively for more than twenty years to deter and punish hacking and other unauthorized access to computer systems. This does not mean, however, that it should be used to punish crimes it was never conceived to confront. That challenge should be left to new legislation, carefully contemplated to deal with the intricacies of current technology and associated abuses. Ideally, legislation will be created to address the type of harassment that Megan Meier suffered at the hands of Lori Drew, thus preventing future tragedies like Megan's suicide and offering clear and fair avenues to punish those who use computers to harass and abuse others online.