COMPUTER HACKERS ON THE CUL-DE-SAC: MYSPACE SUICIDE INDICTMENT UNDER THE COMPUTER FRAUD AND ABUSE ACT SETS DANGEROUS PRECEDENT

CAROLINE G. JONES*

I. INTRODUCTION

Dardenne Prairie, Missouri is a quiet suburb of St. Louis home to only about seven thousand residents. It is the type of small town where neighbors still talk to each other over picket fences and know the codes to each other's garage doors.[1] It is not the type of place one would expect to become the epicenter of a legal battle that establishes precedent threatening to criminalize a wide range of ubiquitous and innocuous Internet activity. It all started in a quiet suburban neighborhood with a fake MySpace[2] profile, and the suicide of a thirteen-year-old girl.

The legal battle involves the novel use of a federal computer hacking statute to prosecute an unusual case of cyber bullying. Bullying is an unfortunate but common social phenomenon that has taken on new and precarious implications in the Internet era.[3] The interesting twist with the Missouri case is

* J.D., Widener University School of Law, *cum laude*.

1. *See* Lauren Collins, *Friend Game: Behind the Online Hoax that Led to a Girl's Suicide*, THE NEW YORKER, Jan. 21, 2008, at 34.

2. MySpace is an extremely popular social networking site that has over 100 million users worldwide. *Fact Sheet*, MYSPACE, http://www.myspace.com/pressroom/fact-sheet/ (last visited Dec. 3, 2010). MySpace offers web pages for members to post a profile of themselves—creating an online identity complete with photographs, music, and messages. Members can also "chat" with other members and add other user's profiles as their "friends." As a member adds more "friends," they are connected to other people who share the same "friends" online. This establishes a network of users who are connected to each other through each other. *See Terms & Conditions*, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Oct. 5, 2010) [hereinafter *Terms & Conditions*]. MySpace is especially popular among teens. *Fact Sheet*, MYSPACE, http://www.myspace.com/pressroom/fact-sheet/. This popularity among teens has brought MySpace to the forefront of many controversies. *See Cyber Bullies Hard to Stop: The Bryant Park Project,* NPR (Nov. 30, 2007), http://www.npr.org/templates/story/story.php?storyId=16763234 [hereinafter *The Bryant Park Project*].

3. A survey published in the Journal of Adolescent Health revealed that eighteen percent of middle school students report having been bullied online. Robin M. Kowalski & Susan P. Limber, *Electronic Bullying Among Middle School Students*, 41 J. ADOLESCENT HEALTH, (SUPPLEMENT) S22, S25 (2007). Further, a report from the CDC revealed that cyber bullying is up by 50% from just five years ago. MARCI FELDMAN HERTZ & CORINNE DAVID-FERDON, CENTERS FOR DISEASE CONTROL AND PREVENTION, ELECTRONIC MEDIA AND YOUTH VIOLENCE: A CDC ISSUE BRIEF FOR EDUCATORS AND CAREGIVERS 6 (2008) (citing Janis Wolak et al., *Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts*, 41 J. ADOLESCENT HEALTH (SUPPLEMENT) S51). *See also The Bryant Park Project*, *supra* note 2.

that the cyber bullying involved a middle-aged woman.[4] Lori Drew created a fake MySpace profile in an attempt to gain information from, and eventually harass thirteen-year-old Megan Meier.[5] Clinically depressed, Megan hanged herself after a lengthy Internet clash between herself and the fake MySpace identity. Both the State of Missouri and the United States Attorney's Office in Missouri failed to indict Drew for any crime directly relating to Megan Meier's suicide.[6] At the time, neither the State of Missouri nor the Federal system had legislation that could appropriately criminalize Lori Drew's conduct as cyber bulling.[7] In an attempt to build a case against Lori Drew, the prosecution was moved nearly 1,800 miles to Los Angeles, California, where the United States Attorney's Office for the Central District of California took up the charge in an unprecedented indictment.[8]

Lori Drew was indicted under the Computer Fraud and Abuse Act (CFAA).[9] The CFAA is a statute designed to protect computer owners against access to their computers that is either completely unauthorized or in excess of granted authorization. It is most commonly used to prosecute computer hackers who break into computer systems in order to steal or manipulate information. The government's theory was that by violating MySpace's Terms of Service agreement[10] and continuing to use the website, Lori Drew exceeded her authorization on MySpace's computers and as such she violated the CFAA.[11] This was the first time the Act has been used in a social networking case.[12] Following the indictment, Lori Drew pled not guilty to the felony

---

4. Kim Zetter, *Experts Say MySpace Suicide Indictment Sets 'Scary' Legal Precedent*, WIRED.COM, THREAT LEVEL BLOG (May 15, 2008, 5:39 PM), http://blog.wired.com/27bstroke6/2008/05/myspace-indictm.html [hereinafter Zetter, *'Scary' Legal Precedent*].

5. *Id.*

6. *Id.*

7. *Id.* After failing to bring charges against Drew, local Sheriff's Department spokesman Lt. Craig McGuire issued a statement saying that what Drew did "'might've been rude, it might've been immature, but it wasn't illegal.'" Christpher Maag, *A Hoax Turned Fatal Draws Anger but no Charges*, N.Y. TIMES, Nov. 28, 2007, at A23, *available at* http://www.nytimes.com/2007/11/28/us/28hoax.html?_r=1&em&ex=1196398800&en=b148a7356b77eef&ei=5087%0A.

8. The Central District of California asserts jurisdiction in this case because MySpace's servers are located in Beverly Hills, California, which is within the Central District. Indictment at 3, United States v. Drew, No. CR 08-0582-GW (C.D. Cal. May 15, 2008).

9. *Id.* at 9.

10. Terms of Service are agreements that users of a computer service must accept for authorization to use the service. *See Terms & Conditions*, *supra* note 2. The Terms of Service, among others things, are designed to protect computer owners from liability, or protect their computers from use that is threatening or contrary to their business, or to protect copy righted material. *Id.*

11. Indictment, *supra* note 8, at 4-6, 9-10.

12. *Lori Drew Pleads Not Guilty in MySpace Suicide Case*, WALL ST. J. L. BLOG (June 17, 2008, 9:07 AM), http://blogs.wsj.com/law/2008/06/17/lori-drew-pleads-not-guilty-in-myspace-suicide-case/.

charges but was ultimately found guilty by a jury of lesser included misdemeanor counts.[13] The district court ultimately overturned the jury verdict by granting the Defendant's Motion for Judgment of Acquittal.[14] Left unresolved by the Lori Drew case is whether under different facts, a violation of a website's terms of service can be successfully prosecuted under the CFAA. The outstanding questions left open by this case constitute an ongoing threat to computer users.

This note will discuss the unprecedented application of the CFAA to the facts of this case. This note will argue that while the law fits the crime, the use of this statute was inappropriate to criminalize the conduct in this case. In support, this note will discuss the policy arguments against the use of the CFAA and the implications of the government's theory of the case for Internet users. Further, this note will address the constitutional grounds addressed by the court in granting the defendant's motion and the outstanding dangers the indictment poses for Internet users. Finally, this note will discuss alternatives to the use of the CFAA, such as legislation to address the underlying conduct of cyber bullying and the possible constitutional limits of any new cyber bullying statutes.

II. BACKGROUND

A. The Computer Fraud and Abuse Act

The CFAA was first enacted in 1984 as a response to the inadequacy of traditional property law[15] and of later mail and wire fraud statutes that were enacted to combat the growing realm of computer crimes.[16] Since its enactment, Congress has continually broadened the coverage of the CFAA to respond to the fast paced development of cyber crime. Indeed the Senate reports reveal that the CFAA was meant to be a single but expansive statute in order to cover a wide range of computer crimes:

> As intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology. As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer

---

13. United States v. Drew, 259 F.R.D. 449, 452-53 (C.D. Cal. 2009). The prosecution asserted that Lori Drew's intentional infliction of emotional distress on Megan Meier established the felony counts under the statute. *Id.* at 452. Exceeding authorized access in violation of the CFAA becomes a felony when it, among other things, is in furtherance of tortious conduct. 18 U.S.C. § 1030 (2005).

14. *Drew*, 259 F.R.D. at 468.

15. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1613-15 (2003).

16. *See* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101, 112 (2001).

> Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.[17]

While the CFAA prohibits many types of conduct perpetrated against a computer owner,[18] the building block of the statute is the accessing of a computer without authorization or in excess of authorized access.[19] Commentators have suggested that the focus on authorization to access a computer likely stems from an analogy of traditional trespass crimes in property law to the trespass against a computer system.[20] Commentators have also suggested that the use of the CFAA may be easier to prove than traditional trespass claims, and as such has become an extremely useful tool for computer owners to control access to their online information.[21]

A trespasser, like a computer user, can be both totally prohibited from accessing the "property" or can exceed the scope of their license to use the "property."[22] Likewise, the CFAA can be used to combat unlawful access perpetrated by persons who are not authorized to access the computer at all.[23] Examples of this conduct include traditional computer hacking and the use of computer viruses, worms,[24] and denial-of-service attacks.[25] Additionally, the statute can be used to combat those who have at least some authorization to lawfully access the computer but exceed that authorization by going beyond what the computer owner intended to allow.[26] Indeed, violations of the CFAA often come up in the employment context, where an employee is free to use a computer, but only in a way dictated by their employment agreement; as such

---

17. S. REP. NO. 104-357, at 5 (1996).

18. *See* 18 U.S.C. § 1030 (2005). The statute proscribes seven different crimes that are all triggered by the initial access to a computer without authorization or are in excess of authorized access. Kerr, *supra* note 15, at 1616.

19. Kerr, *supra* note 15, at 1616-17.

20. *See id.* at 1617.

21. *See* 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, 323-24 (2004).

22. *See* Kerr, *supra* note 15, at 1619-20.

23. United States v. Morris, 928 F.2d 504, 509-11 (2d Cir. 1991).

24. A virus differs from a computer worm in that a virus attaches itself to the operating system of the computer and attacks other computers that access files stored on the infected computer. *Id.* at 505 n.1. A worm program, on the other hand, travels from computer to computer and attacks each computer, but does not attach itself. *Id.*

25. *See* United States v. Phillips, 477 F.3d 215, 218 (5th Cir. 2007). A denial-of-service attack is an attack by a computer hacker to disable a computer or server in such a way as to prevent legitimate users from accessing it. Kerr, *supra* note 15, at 1603-04. This is accomplished by bombarding the computer with requests in order to either have it shut down from an overload of requests or consume its resources. Mindi McDowell, *Understanding Denial-of-Service Attacks*, UNITED STATES COMPUTER EMERGENCY READINESS TEAM (Nov. 4, 2009), http://www.us-cert.gov/cas/tips/ST04-015.html.

26. Kerr, *supra* note 15, at 1604.

they are authorized to use the computer, but only in a limited scope.[27] The government's theory was the latter, that Lori Drew exceeded her authorization to access MySpace computers, and therefore her conduct fell within the ambit of the CFAA.

B. The Government's Theory of the Case

The United States Attorney's Office in California did not prosecute Lori Drew for the underlying conduct that led to the death of Megan Meier. The government's theory of the case was that Lori Drew victimized MySpace.[28] To establish that Drew's use of MySpace computers was criminal, the government had to prove that she accessed MySpace's computer without authorization and that she did so in order to obtain information. The government charged Drew with violating two sections of the CFAA[29] which make it a felony, punishable by up to five years in prison, if one "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" if "the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State."[30] To prove a violation of the CFAA as a misdemeanor, the government need only prove that the defendant accessed a computer, not that such activity was in furtherance of tortious conduct.[31] The foundation of the government's case was that the Terms of Service agreement dictates the scope of a user's authorization on MySpace computers, and a violation of the terms constitutes a violation of the CFAA. The government's theory was that in violation of the web site's Terms of Service agreement, Drew used MySpace to obtain information about Megan Meier and did so in furtherance of intentional infliction of emotional distress.[32]

1. Terms of Service Agreements Can Establish Scope of Authorization

Members of MySpace are authorized to use MySpace services only if they agree to abide by the Terms of Service.[33] Therefore the scope of a user's authorization is determined by following those agreed upon terms. Specifically, the government claimed that Lori Drew violated several of MySpace's terms including the requirement to:

> a. Provide truthful and accurate registration information; b. Refrain from using any information obtained by MySpace services to harass, abuse, or harm other

27. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-82 (1st Cir. 2001).

28. Brief for Elec. Frontier Found. et al. as Amici Curiae Supporting Defendant at 4, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (No. CR 08-0582-GW).

29. Indictment, *supra* note 8, at 1.

30. 18 U.S.C. § 1030 (2005).

31. *Id.*

32. Indictment, *supra* note 8, at 5.

33. *Id.* at 4-5. MySpace users agree to the Terms of Service when they become a member of the site by clicking a box stating that they have read and agree to the terms. *Id.* at 4.

> 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.[34]

At trial, the government proved several facts that established a violation of the Terms of Service. They proved that Drew registered for an account under a fictitious name, assuming the persona of a sixteen-year-old boy named "Josh Evans." She posted a picture of a handsome young man that she had found on the Internet, obviously without the knowledge or consent of that person.[35] Drew then struck up a flirtatious relationship with Megan Meier, calling her "sexi,"[36] and inviting Megan to "touch the 'snake' of 'Josh Evans.'"[37] After gaining her trust, Drew then used the MySpace account to gain information from Megan, a minor.[38] In doing so, Drew was attempting to find out what Megan was saying online and whether Megan was talking badly of her own daughter with whom Megan had a falling out.[39] Eventually, "Josh" turned on Megan, and began to harass her, ultimately sending a final message, "you're a shitty person, the world would be a better place without you in it."[40] Twenty minutes later, Megan's mother discovered her daughter with a cloth belt around her neck, hanging from her closet organizer.[41] Megan died the next day.[42]

The prosecution believed it had enough evidence to show that Drew had violated MySpace's Terms of Service, and did so in furtherance of tortious conduct, specifically intentional infliction of emotional distress.[43] At trial the jury deadlocked and failed to convict Drew for the felony counts.[44] Drew was found guilty of three lesser included misdemeanor counts, as the prosecution had successfully persuaded the jury that she exceeded authorization by violating MySpace's Terms of Service, but not that her conduct was in furtherance of any tortuous conduct.[45] Despite the precarious policy

---

34. *Id.* at 5.

35. *See* Collins, *supra* note 1.

36. Dan Slater, *Another Take on the MySpace Charges: 'The Statute Neatly Fits the Facts'*, WALL ST. J. L. BLOG (May 22, 2008, 12:52 PM), http://blogs.wsj.com/law/2008/05/22/another-take-on-the-myspace-charges-the-statute-neatly-fits-the-facts/.

37. Indictment, *supra* note 8, at 7.

38. *See id.* at 2, 6.

39. Collins, *supra* note 1.

40. *Id.*

41. *Id.*

42. *See id.*

43. *See* Indictment, *supra* note 8.

44. United States v. Drew, 259 F.R.D. 449, 452-53 (C.D. Cal. 2009).

45. Kim Zetter, *Lori Drew Not Guilty of Felonies in Landmark Cyberbullying Trial*, WIRED.COM, THREAT LEVEL BLOG (Nov. 26, 2008, 11:26 AM), http://blog.wired.com/27bstroke6/2008/11/lori-drew-pla-5.html.

implications of using the CFAA to prosecute this conduct, discussed below, the jurisprudence interpreting the scope of the CFAA supports the government's theory of the case.

III. ANALYSIS

While the connection between Lori Drew's conduct and computer hacking seems empirically attenuated, theoretically the law fits the crime as charged. Although primarily a criminal statute, the CFAA was amended to contain a civil remedy. [46] The statute has proven effective in prosecuting traditional computer hackers and because of the civil amendment it has become a useful tool for private computer owners. However, courts in civil cases tend to adopt a broader standard of liability than in criminal cases.[47] As a result, a dangerous jurisprudence is emerging.

A. Civil Cases Set Precedent for Contract Violations as Foundation for Unauthorized Access

Courts analyzing the CFAA have determined that "the scope of a user's authorization to access a protected computer [can be based on] the expected norms of intended use or the nature of the relationship established between the computer owner and the user."[48] In accordance, the courts have granted computer owners broad discretion to define what acts are unauthorized[49] and have recognized that the "intended use" of a computer can be established by a contractual arrangement.[50] When parties are bound by a contract that regulates their use of a computer, a breach of that contract makes the computer access unauthorized, and therefore establishes the predicate for a violation of the CFAA.[51] Courts have naturally extended this interpretation of the bounds of the CFAA to include Terms of Service agreements, which can dictate, by contract, the intended use of the computer.

A good illustration of this is *EF Cultural BV v. Explorica*,[52] in which the court held that a violation of a contractual agreement could form the basis for a finding of exceeding authorized access.[53] EF Cultural, a tour company, sued their upstart competitor, Explorica, alleging that the competitor's use of a "scraper" computer program[54] violated the CFAA.[55] The scraper program

46. 18 U.S.C. § 1030(g) (2005).
47. Kerr, *supra* note 15, at 1642.
48. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).
49. Galbraith, *supra* note 21, at 338.
50. *See Phillips*, 477 F.3d at 219-21.
51. Kerr, *supra* note 15, at 1637.
52. 274 F.3d 577 (1st Cir. 2001).
53. *Id.* at 583-84.
54. A "scraper" is an automated computer program that collects information available on web pages. EF's website allows a visitor to do essentially the same thing by entering in a tour location and being able to see the price for each tour. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 60 (1st Cir. 2003).

would scour EF Cultural's publicly available website for tour information. Based on Explorica's principal's knowledge of special tour codes the scraper was able to compile a list of prices for each tour and Explorica was then able to undercut EF Cultural's prices.[56] The court held that the use of the scraper exceeded authorized access within the meaning of the CFAA.[57] The court reasoned that the ability of the scraper to function with efficiency depended on the knowledge of the special tour codes.[58]

The court further noted that while it was possible that a normal web user could decipher the tour codes, knowledge of the codes made the collection of the information very fast and accurate.[59] The source of the tour codes was one of Explorica's principals who was a former employee of EF Cultural.[60] Upon leaving EF Cultural, he signed a confidentiality agreement in which he agreed not to disclose any proprietary information.[61] Finding that the tour codes were proprietary information and that Explorica's principal was therefore in violation of his confidentiality agreement, the Court reasoned that Explorica exceeded authorized access of the computer because the use of the scraper program was facilitated by a breach of the contract terms.[62] This case established that a contractual relationship with a computer owner can dictate the scope of authorization on a public website and therefore dictate when a party has exceeded authorized access as a foundation for a violation of the CFAA.

By comparison, in another suit by EF Cultural against the computer programmer who designed the scraper program, the court did not find that his conduct exceeded authorized access because he lacked the predicate violation of a contractual agreement. In *EF Cultural Travel BV v. Zefer Corp*,[63] the court held that an injunction against the computer programmer, Zefer Corporation, was not proper because there was no evidence the it was exceeding authorization on their computers by use of the scraper.[64] Zefer was under no contractual obligation against using the proprietary information, as no one at Zefer was a former employee.[65] Further, EF Cultural's website did not have a notice restricting the use of automated devices such as a scraper.[66] The court noted in dicta that if EF Cultural wanted to ban the use of automated devices they could have established a Terms of Service agreement to regulate such

55. *Explorica*, 274 F.3d at 580.
56. *Id.* at 579-80.
57. *Id.* at 581.
58. *Id.* at 582-83.
59. *See id.* at 579.
60. *Id.*
61. *Explorica*, 274 F.3d 577, 582 (1st Cir. 2001).
62. *Id.* at 581.
63. 318 F.3d 58 (1st Cir. 2003).
64. *Id.* at 63.
65. *See id.*
66. *Id.*

conduct.[67] The court held that, "[a] lack of authorization could be established by an explicit statement on the website restricting access. . . . Many webpages contain lengthy limiting conditions, including limitations of the use of scrapers."[68] Moreover, the court noted that "[t]he CFAA . . . is primarily a statute imposing limits on access and enhancing control by information providers" and a "public website provider can easily spell out explicitly what is forbidden."[69] In failing to extend liability to Zefer for violation of the CFAA, the court established that contract terms, such as those provided in a website's Terms of Service, can establish a foundation for unauthorized access under the CFAA.[70]

Another case, *America Online, Inc. v. LCGM, Inc.*,[71] involved spammers who opened up an AOL account to "harvest"[72] email addresses of other AOL members.[73] The court held that the spammers' actions were in violation of AOL's Terms of Service and therefore constituted a violation of the CFAA.[74] After gathering the email addresses, the spammers "sent unauthorized and unsolicited bulk email[s]" to the addresses that they collected.[75] When sending out the bulk emails, the defendants replaced their own email address in the "from" line with "aol.com".[76] This caused confusion among the people receiving the emails about whether AOL endorsed the messages or if they came from AOL at all.[77] This bulk emailing activity violated AOL's Terms of Service.[78] AOL brought suit under the civil remedy portion of the CFAA alleging that the spammers violated the CFAA because they exceeded authorized access.[79] Without much analysis, the court plainly held that "the Defendants' actions violated AOL's Terms of Service, and as such was unauthorized."[80] The court held that the "information" gathered in violation of the Terms of Service agreement was the email addresses of other AOL users.[81]

---

67. *Id.*
68. *Id.* at 62.
69. *Zefer Corp.*, 318 F.3d at 63.
70. *See id.*
71. 46 F. Supp. 2d 444 (E.D. Va. 1998).
72. *Id.* at 448.
73. *Id.*
74. *Id.* at 450-51.
75. *Id.* at 448.
76. *Id.*
77. *America Online, Inc.*, 46 F. Supp. 2d at 448.
78. *Id.* at 450.
79. *Id.* at 450-51.
80. *Id.*
81. *Id.*

In totality, these cases[82] set precedent that a website's Terms of Service can provide the predicate for establishing that a person has exceeded authorized access in violation of the CFAA. The government's theory of the case in the indictment of Lori Drew was congruent with this precedent. The law fits the crime. However, even though the charge under the CFAA was a technical fit, there are other compelling considerations that call into question whether the prosecution was appropriate, or even constitutional.

B. Policy Arguments Against the Use of the Computer Fraud and Abuse Act

Terms of Service agreements are good mechanisms for computer owners to control conduct on their computers, and the CFAA can be an appropriate tool to impose civil penalties for those violations. But however useful the agreements can be in a civil context, contract disagreements with computer owners should not become *criminal* violations in most circumstances—at least not in the way that most people use the Internet and not if we want to preserve the Internet as a valuable tool for our society.

The Internet has profound social value for both freedom of expression and for the free market. As a result, there is a tension between leaving the Internet free and open in order to promote these values, but providing enough privacy protection and security online to facilitate its long-term viability as a tool for commerce.[83] Computer owners, like traditional brick and mortar businesses, have a legitimate interest in online security.[84] In the civil context the CFAA can be very useful for computer owners to protect their competitive positions. However, a click to agree contract, like a website's Terms of Service, does not adequately protect computer owners' security interests, and so its value fails to outweigh the burden placed on society.

Orin Kerr,[85] law professor and defense co-counsel in the Lori Drew case, has compared Terms of Service agreements to the use of the honor system; with the remedy for a violation being a breach of contract that is actionable in

---

82. *See also* Ticketmaster LLC v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1110 (C.D. Cal. 2007) (finding that a violation of Terms of Service resulted in unauthorized access); Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476, at *13 (E.D. Tex. Jan. 25, 2007) (finding unauthorized access established when conduct was in violation of agreements).

83. *See* Kerr, *supra* note 15, at 1649-50.

84. For more information on how computer owners can protect privacy and competitive position online see Adam R. Bialek & Scott M. Smedresman, *Internet Risk Management: A Guide to Limiting Risk Through Web Site Terms and Proactive Enforcement,* INTELL. PROP. & TECH. L.J., Nov. 2008, at 1, 1.

85. Kerr is a professor of law at George Washington University Law School. He was a criminal trial attorney in the Computer Crime and Intellectual Property Section at the Department of Justice as well as a Special Assistant U.S. Attorney for the Eastern District of Virginia. Orin Kerr accepted a position as pro bono co-counsel for Lori Drew. Kim Zetter, *Former Justice Dept. Prosecutor Joins Defense in MySpace Suicide Case*, WIRED.COM, THREAT LEVEL BLOG (Oct. 21, 2008, 10:15 AM), http://www.wired.com/threatlevel/2008/10/former-justice.

civil court.[86] Computer owners put up the terms and ask users of their website to abide by them, but cannot truly enforce them until a breach is discovered. Computer owners can be more effective in protecting their interests online by using prophylactic code-based tools[87] to avoid misuse of their websites. An appropriate use of the CFAA is as a cyber equivalent to traditional contract law in combination with a criminal law component strictly for cases of traditional computer hacking.[88] Expanding the scope of the CFAA to criminalize violations of Terms of Service agreements will have a severe chilling effect on important social activity conducted on the Internet, while having only a minimal effect on privacy and security interests of computer owners.[89] Therefore, it is not an appropriate use of the statute from a policy standpoint.

1. Power Delegated to Private Computer Owners

A serious implication of the indictment of Lori Drew under the criminal portion of the CFAA is the power it delegates to private computer owners, such as MySpace, and the effect that will have on average Internet users. Criminal statutes are carefully drawn policy determinations made by elected legislative bodies, unlike a Terms of Service agreement that is drafted by a private computer owner—with no such interest in policy or standards—and is drafted for completely self serving, and non-transparent reasons. If the government's interpretation of the CFAA is correct, computer owners have been given the authority to dictate the scope of criminal liability with their Terms of Service agreements.[90]

In his influential law review article Kerr argues that "[b]y granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner."[91] Andrea Matwyshyn, a law professor at the University of Pennsylvania warns that "[e]mpowering terms of use to be key pieces of evidence in criminal matters—when terms of use are generally thought of by the people who are entering into them as purely contract or civil matters—is something that should be done carefully."[92] The interpretation of the CFAA

86. Kerr, *supra* note 15, at 1645-46.

87. Code based tools are a way for a computer owner or website administrator to regulate each user's rights (or access to certain files or directories) on the website. *Id.* at 1644. This is often done by supplying a unique account with a password to which certain privileges are attached. *Id.* This provides a level of protection that requires a hacker to guess at or break into an account to be able to exceed the authorization allowed. *Id.* at 1644-45. These tools, while not impenetrable by hackers, are a convenient way to clearly establish the scope of authorization on a site, a task which they accomplish more effectively than a Terms of Service agreement. *Id.* at 646.

88. *Id.* at 1651.

89. *Id.* at 1650-51.

90. Defendant's Motion to Dismiss Indictment at 6, United States v. Drew, No. CR 08-0582-GW (C.D. Cal. July 23, 2008) 2008 WL 2848961.

91. Kerr, *supra* note 15, at 1651.

92. Zetter, *'Scary' Legal Precedent*, *supra* note 4.

pursued in the Lori Drew case enables private computer owners to harness the power of the criminal justice system to enforce their own contract terms.[93] Contract law is sufficient to satisfy the interests of privacy and security invoked by violations of Terms of Service agreements without applying criminal sanctions to that same conduct.[94]

2. The Requirement of Intent and Obtaining Information: Interpretation Threatens to Criminalize Innocuous Internet Conduct

Few users actually read the Terms of Service agreements on the websites they visit.[95] Many Terms of Service agreements are drafted by legal departments and are difficult to understand, arbitrary, or vague in their construction.[96] While the CFAA requires that the defendant intentionally access a computer without authorization, prosecutors in the Lori Drew case were able to set aside the fact that Drew never read the Terms of Service by establishing her intent circumstantially.[97] In their brief in opposition to Drew's Motion for Acquittal, the prosecution asserts that it is not necessary under the CFAA to show that the defendant actually read the Terms of Service.[98]

> [T]he statute merely requires that defendant intend to access a computer without authorization or in excess of authorization . . . . Nothing in the statute, therefore, can be read as requiring that a defendant must actually read the [Terms of Service] that render her access unauthorized so long as there is alternative evidence from which a jury can infer this knowledge.[99]

By presenting evidence that Lori Drew knew that creating a fake MySpace profile might be wrong, and that she deleted the account after learning of Megan's death, the government contended that the jury would be able to infer knowledge of the terms.[100] Further, the government alleged that Drew's continued use of the website in a way that she knew was against the website's policies establishes the intent required by the statute.[101] If this construction of

---

93. Kerr, *supra* note 15, at 1658-59. *See generally* Kim Zetter, *Can Lori Drew Verdict Survive the 9th Circuit Court?*, WIRED.COM, THREAT LEVEL BLOG (Dec. 1, 2008, 3:03 PM), http://www.wired.com/threatlevel/2008/12/can-lori-drew-v/ [hereinafter Zetter, *Can Lori Drew Verdict Survive*] (noting that critics fear that the verdict meant that any computer user who violates a service provider's Terms of Service could now face criminal prosecution for what in the past would have been a civil breach of contract).

94. *Kerr*, *supra* note 15, at 1651.

95. *Id.* at 1659.

96. *Id.*

97. *See* Zetter, *Can Lori Drew Verdict Survive*, *supra* note 93.

98. Government's Opposition to Defendant's Motion for Judgment of Acquittal at 6, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2008) (No. CR 08-0582-GW).

99. *Id.*

100. *Id.* at 9-10.

101. *Id.* at 7-11.

the statute is followed in other cases, it threatens to criminalize a wide range of Internet activity. Knowledge that conduct might violate a website's Terms of Service should be insufficient to establish the necessary *mens rea* for the crime.[102]

The prosecution defended the assertion that using the CFAA in this way threatens to criminalize ubiquitous and innocent Internet conduct by stating that the CFAA "is applicable only where unauthorized access is used to obtain information . . . . Even if many people falsify personal information to obtain access in contravention of the [Terms of Service], the underlying assumption that they commonly do so to obtain information is questionable."[103] While the CFAA does not define what is meant by "obtains information," the Senate report to the 1996 amendments sheds some light onto the congressional intent. The report states that "the term 'obtaining information' includes merely reading it."[104] An interpretation of the CFAA consistent with the Senate report suggests that if a person visits a website in violation of the Terms of Service and merely reads what is on the screen, they are in violation of the CFAA. Therefore, the prosecution's defense of the limitations of the statute likely fails and puts Internet users at risk.

In sum, if the statute does not require the prosecution to prove that the defendant actually read the Terms of Service and the limiting factor of obtaining information is mere pretense, then this construction does threaten to criminalize a wide range of innocuous and ubiquitous Internet conduct. For policy reasons, the statute should be construed to avoid allowing such a broad reading. Any other construction would put many Internet users at risk.

3. Effect of Prosecution on Goals of Criminal Justice System and Role of Courts

After Missouri's failure to criminalize Lori Drew's conduct, there was outrage across the country. Many were incensed that an adult woman, a mother, preyed on the insecurities of a fragile girl—and was getting away with it.[105] After Drew's name was outed on the Internet by an enraged blogger, she received death threats, a brick was thrown through a window in her home, and there were calls on the Internet to have her house set aflame.[106]

One could speculate that this outcry of public condemnation of Drew's actions may have influenced the U.S. Attorney's Office to proceed with their

---

102. *See* Rule 29 Motion for Judgment of Acquittal at 3, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2008) (No. CR 08-0582-GW).

103. Government's Opposition to Defendant's Motion to Dismiss the Indictment for Vagueness at 18, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2008) (No. CR 08-0582-GW).

104. S. REP. NO. 104-357, at 7 (1996).

105. Zetter, *'Scary' Legal Precedent*, *supra* note 4.

106. Kim Zetter, *Cyberbullying Suicide Stokes the Internet Fury Machine*, WIRED.COM, THREAT LEVEL BLOG (Nov. 11, 2007), http://www.wired.com/politics/onlinerights/news/2007/11/vigilante_justice [hereinafter Zetter, *Internet Fury Machine*].

unique and untested prosecution.[107] The prosecution itself recognized that the "unusual nature of the charge is a product of the unique nature of the crime."[108] The prosecution defended its unprecedented use of the CFAA on the fact that cyber bulling is a new phenomenon and the use of MySpace has only been in existence since 2000.[109] This line of reasoning might suggest that if a statute for cyber bullying would have been available, the prosecution might have proceeded under that statute, not under the CFAA. After all, the outrage against Drew did not stem from her violation of MySpace's Terms of Service, it stemmed from the underlying conduct of harassing a young girl. If state or federal laws were better able to address cyber bullying,[110] especially crimes by adults against children, prosecutors might not need to resort to creative charges to provide justice for victims.

Legislation designed to criminalize cyber bullying may serve as a more effective deterrent to this type of conduct than prosecution under a computer hacking statute. Indeed, prosecution under the CFAA for this type of conduct will have a profound effect on a citizen's relationship with the criminal justice system. Over the past several decades, the federal criminal law has expanded immensely. There are currently over 4,450 federal offenses.[111] As a result, average Americans are increasingly unfamiliar with what of their conduct can be considered criminal, which results in the federal criminal code arguably failing to serve its most important societal function, to deter.[112] The criminal justice system's role is to inform citizens of the requirements of the law, thereby enabling them to avoid conduct that the law considers deserving of punishment.[113] It is the criminal law's deterrence effect which is most effective in preventing lawlessness in society.[114] That deterrence effect is severely limited when conduct that is not viewed by the vast majority of people as wrongful is punished at the federal level.[115] Expanding the scope of a federal criminal code to encompass more crimes that are *male prohibitum* upsets the balance between government and its people and the goals of criminal law. The use of the CFAA in the context of a violation of a website's

---

107. Zetter, *'Scary' Legal Precedent*, *supra* note 4.

108. Government's Opposition to Defendant's Motion to Dismiss the Indictment for Vagueness, *supra* note 103, at 21.

109. *Id.* at 22.

110. *See infra* Part IV.A.

111. Brian W. Walsh, *Doing Violence to the Law: The Over-Federalization of Crime*, 20 FED. SETN'G REP. 295, 295 (2008).

112. *See id.*

113. *Id.*

114. The power to punish crimes is the greatest power that government has over its own citizens, because the power to punish is the power to deprive citizens of their most basic of civil liberties—freedom. *See id.* at 296. Therefore, the emphasis of the criminal law is, and should be, placed on deterring conduct that is anti-social or morally wrong, rather than focusing on providing punishments. When a criminal law fails to deter, it is not performing its most essential function, and should be re-evaluated.

115. *See id.* at 295.

Terms of Service agreement reflects the dangers of an expansive criminal code that is not tailored to meet the specific needs of society, or is so overbroad as to criminalize otherwise innocuous Internet activity.

However, there exists in our criminal justice system a tension between the compelling need of prosecutors to keep up with criminals and the desire to maintain the balance of power between the government and citizens.[116] In order to effectively combat emerging and shifting criminal activity, such as computer crime, prosecutors must be able to construe statutes to criminalize new forms of illegal conduct. The legislative process is often protracted, so the need to punish conduct that should be criminal, but that has yet to be legislatively addressed, in compelling. Often legislatures leave their statutes broad and ambiguous in order to enable prosecutors to penalize crimes that could not have been imagined at the time of the drafting.[117] The CFAA itself was passed at a time when the Internet was in its infancy and legislatures were not sure how Internet crime might develop. In their brief to the court in the Lori Drew case, the prosecution argued that the CFAA was left intentionally broad in order for it to be an effective omnibus criminal statute to address the new and expanding realm of cyber crimes.[118] Congress thus chose a broad construction, instead of "'identifying and amending every potential applicable statute affected by advances in computer technology.'"[119]

Despite this important government interest, the risk of over aggressive prosecutions that construe statutes beyond their intended limits can have a severe effect on the rights of individuals.[120] Indeed, while Lori Drew could have anticipated harassment charges or even a civil suit for her conduct online, she could not have anticipated being in violation of the CFAA, a computer hacking statute.[121] Consequently, the effect of the CFAA to deter conduct such as Drew's is nebulous.

Because of this tension, the courts play an important role in striking the balance between the needs of the government in staying on the cutting edge of computer crime and the interests of the people in being free from unexpected prosecution.[122] The Supreme Court has long recognized its authority to limit broad and ambiguous criminal statutes in order to avoid the danger of over criminalization of innocent conduct.[123] The rule of lenity is a judicial doctrine that requires that when a court is "confronted with 'two rational readings of a criminal statute, one harsher than the other, we are to choose the harsher only

---

116. *See The Supreme Court, 2007 Term-Leading Cases, Immigration and Naturalization Act, Voluntary Departure:* Dada v. Mukasey, 122 HARV. L. REV. 465, 479-80 (2008) [hereinafter *The Supreme Court, 2007 Term-Leading Cases*].

117. *See id.* at 480-81.

118. Government's Opposition to Defendant's Motion to Dismiss the Indictment for Vagueness, *supra* note 103, at 20 (citing S. REP. NO. 104-357, at 5 (1996)).

119. *Id.* at 21 (quoting S. REP. NO. 104-357, at 5 (1996)).

120. *See The Supreme Court, 2007 Term-Leading Cases*, *supra* note 116, at 481.

121. *See id.* at 481 n.64.

122. *Id.* at 481.

123. *Id.* at 480, 482.

when Congress has spoken in clear and definite language.'"[124] Under the rule of lenity, a criminal statute is construed in favor of the accused in situations in which there is a reasonable doubt regarding the statute's intended scope even after looking into the statute's plain language, statutory structure, legislative history, and policies.[125]

While seemingly dormant, the rule of lenity has recently made resurgence in Supreme Court jurisprudence.[126] Some lower courts have applied the rule of lenity in interpreting the CFAA, noting the danger of a broad and expansive reading of the statute.[127] Given that the Supreme Court has seemingly revived the doctrine of lenity, if a case like the Lori Drew case did make it up to the Supreme Court, it seems like a perfect candidate for lenity. By interpreting statutes with more deference to defendants, the Court places the burden on the legislature to be clearer about its intentions for a statute or to come up with a more appropriate sanction for Drew's conduct.[128]

C. Constitutional Vagueness Doctrine as a Defense to Use of the CFAA

The same policy arguments against the use of the CFAA to criminalize violations of Terms of Service agreements may also trigger the constitutional void for vagueness doctrine. In fact, the district court in the Lori Drew case relied on vagueness grounds when it granted the Defendant's Motion for Judgment of Acquittal. After the jury returned a verdict of guilty to the lesser included misdemeanor charges, the judge finally ruled on the Defendant's Motion holding that the jury verdict would render the statute void on vagueness grounds. In its opinion, the court held that

> if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute [a violation of the CFAA] . . . the result will be that section 1030(a)(2)(c) [of the CFAA] becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[129]

Essentially, if the government's theory that any violation of a website's Terms of Service can constitute a violation of the CFAA, the statute is unconstitutionally vague. This ruling is a substantial step in the direction of avoiding the use of the CFAA for prosecution of Terms of Service agreements.

---

124. Pasquantino v. United States, 544 U.S. 349, 383 (2005) (Ginsburg, J., dissenting) (quoting McNally v. United States, 483 U.S. 350, 359-60 (1987)).

125. Moskal v. United States, 498 U.S. 103, 108 (1990).

126. *See, e.g.*, United States v. Santos, 553 U.S. 507, 514 (2008).

127. *E.g.*, Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. 2006).

128. *See The Supreme Court, 2007 Term-Leading Cases*, *supra* note 116, at 483-84.

129. United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (quoting City of Chicago v. Morales, 527 U.S. 41, 64 (1999)).

The granting of the Defendant's Motion in the Drew case is an example of the important role the courts play in balancing the interests of the criminal justice system and an Internet society, and represents a positive jurisprudential trend. It should be noted, however, that the opinion fell short of holding that the statute itself is unconstitutional. Rather, the effect of the decision on the motion for acquittal was only to admit a lack of evidence sufficient with which to sustain the jury's verdict.[130] Therefore, the ultimate question of constitutionality of the statute on vagueness or other grounds is still up for interpretation by the courts.

The void for vagueness doctrine is derived from and embodied in the Fifth Amendment's Due Process Clause. The oft-quoted language of *Lanzetta v. New Jersey*[131] is that "[n]o one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes."[132] Determining whether a statute is unconstitutionally vague, and therefore violates the due process clause, requires an inquiry into whether a statute provides fair notice of what conduct is prohibited and what a citizen must do to be in compliance with the law. Further, the statute must have definable standards so as to avoid discriminatory enforcement of criminal sanctions of conduct.[133] In that respect, the void for vagueness doctrine is comprised of two related elements. First, the statute must give sufficient notice to a citizen such that it is not "so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application."[134] Second, the statute must provide sufficient guidelines to law enforcement so as to avoid arbitrary enforcement of the law.[135]

The prosecution of Lori Drew then necessarily begs the question whether an average person would know that a breach of a website's Terms of Service constitutes a federal crime under the CFAA. The district court agreed that average users of the Internet would not expect that a violation would render them liable for criminal sanctions. The court noted that especially in a case of a free service, such as that offered by MySpace, an average user would not think that their conduct that might be in violation of a website's many and often pro forma terms of service, and that violation of those terms would be illegal.[136] The average Internet user of "common intelligence" routinely

---

130. The motion was based on Federal Rules of Criminal Procedure Rule 29(c). These motions may be made by a defendant who is challenging the conviction and can be raised and ruled on after the close of all evidence or after the jury has returned its verdict. The standard of review is whether in the light most favorable to the non-moving party, the evidence is insufficient to sustain a conviction. FED. R. CRIM. P. 29 cmt.

131. 306 U.S. 451 (1939).

132. *Id.* at 453. For a historical discussion of the void for vagueness doctrine as a rule of construction, see Cristina D. Lockwood, *Defining Indefiniteness: Suggested Revisions to the Void for Vagueness Doctrine*, 8 CARDOZO PUB. L. POL'Y & ETHICS J. 255, 263-94 (2010).

133. Kolender v. Lawson, 461 U.S. 352, 357-58 (1983).

134. Connally v. Gen. Const. Co., 269 U.S. 385, 391 (1926).

135. *Kolender*, 461 U.S. at 357-58.

136. United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

ignores Terms of Service agreements.[137] The clicking of the box at the bottom of the page to confirm that you have read the terms has become as ubiquitous as the Internet itself. In that respect, notice that a violation of any of the terms may constitute a crime is likely unconstitutionally vague, and certainly not in accordance with how most people use the Internet.

The court further went on to articulate that there is a danger when the website owner, by use of their Terms of Service, is able to define what conduct is in violation, and therefore subject to possible criminal sanctions. The owner's description of the Terms of Service itself might be so vague that the average Internet user would not know what was prohibited.[138] Further the terms can often be changed unilaterally, and without notice to the computer user and the user can still be determined to be bound by them.[139] By wedding criminal sanctions to essentially contractual provisions, it renders the statute incredibly over broad, which necessarily leads to discretionary prosecution, thus rendering the statute void for vagueness on the second element.[140]

Indeed, in recent years, holdings have focused on the second prong, raising it to a level of higher importance in the due process analysis.[141] It is arguable that if a computer user is given sufficient notice that violations of Terms of Service may subject them to criminal sanctions it may be sufficient to satisfy the first prong. But the potential for arbitrary enforcement is a more likely ground to invalidate the statute. To avoid arbitrary enforcement the statute must not "permit 'a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections.'"[142] Moreover, an overly broad and vague statute that does not set clear guidelines or criteria to limit enforcement by law enforcement effectively transfers the balance of power between the legislature to the criminal justice system, and "[l]egislatures may not so abdicate their responsibilities for setting the standards of the criminal law."[143]

---

137. As a coda to the argument that most website users do not take seriously a public website's Terms of Service, the founder of MySpace is charged with having misrepresented his age on his own MySpace account—a clear violation of his own website's Terms of Service agreement. Jessica Bennett, *Is Age Just a Number?*, NEWSWEEK (Oct. 27, 2007), http://www.newsweek.com/2007/10/27/is-age-just-a-number.html.

138. *Drew*, 259 F.R.D. at 465. *See supra* Section III.B.1.

139. *See* Galbraith, *supra* note 21, at 339-42. "It is difficult to see how a website visitor that has not provided any possible acceptance to the site's terms and conditions can be deemed to have consented to them through the mere use of the Internet site. But recent court decisions have facilitated the enforcement of such contracts." *Id.* at 342 (citations omitted).

140. *Drew*, 259 F.R.D. at 466-67.

141. Kolender v. Lawson, 461 U.S. 352, 358 (1983). *See* Lockwood, *supra* note 132, at 275.

142. *Kolender*, 461 U.S. at 358 (quoting Smith v. Goguen, 415 U.S. 566, 575 (1974)) (alteration in original); U.S. v. Williams, 553 U.S. 285,304 (2008) (stating that a conviction is void for vagueness "if the statute it is obtained under . . . is so standardless that it authorizes or encourages seriously discriminatory enforcement").

143. Smith v. Goguen, 415 U.S. 566, 575 (1974).

Terms of Service agreements are often lengthy and contain many terms drafted only for the benefit of the website owner himself. Because the terms are written by the website owner, they can be extremely broad, and have the tendency to sweep in otherwise innocuous or trivial conduct into potential criminal activity. They can contain numerous arbitrary and capricious terms. Because the terms are written by the private computer owner there is no limitation or criteria as to which violations of the website's Terms of Service are going to be enforced criminally. Therefore, using a website's Terms of Service agreement as the gravamen for a violation of the CFAA constitutes a standardless sweep, and necessitates arbitrary enforcement. It fails to set standards and objective criteria to guide law enforcement, and delegates the responsibility of the legislature to define what is criminal, to private computer owners.

IV. ALTERNATIVE SUGGESTIONS TO CRIMINALIZE LORI DREW'S CONDUCT

In order to avoid implicating the serious policy concerns and constitutional considerations incident to using the CFAA to prosecute conduct similar to that of Lori Drew's, alternative options should be explored with which to provide the justice that society cries out for in this case.

A. Amendment to Federal and State Laws to Address Cyber Bulling

One such option is that lawmakers could amend bullying and harassment statutes to more precisely address the conduct in this case. Instead of punishing Lori Drew for violating MySpace's Terms of Service, prosecutors could more directly punish her for the underlying act of cyber bullying. Cyber bullying, often referred to as cyberstalking,[144] is the use of the Internet or other electronic media with the intent to hurt or embarrass another person.[145] Cyber bullying can prove to be much more serious and pervasive than traditional bullying because of the relative anonymity of the Internet and the prevalence of its use,[146] which add to the overall potential for cyber bulling.[147]

---

144. *The Bryant Park Project*, *supra* note 2. Cyber bulling is used often interchangeably with the term cyber stalking, however there are practical differences between the two types of conduct that have implications for statutory drafting. *Id.*

145. *See* Wolak et al., *supra* note 3, at S52. *See also* Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 126 (2007) (stating that "cyberstalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual").

146. Kowalski & Limber, *supra* note 3, at S23.

147. *See* Goodno, *supra* note 145, at 129-31. A 2007 study suggests that eighteen percent of elementary school students studied had been bullied online in the past couple of months. Kowalski & Limber, *supra* note 3, at S25. The Megan Meier case is not the only recent story that has a social networking site at the center of the suicide of a teenager. In September 2010, a college student committed suicide after a video of him engaging in a sexual encounter with another student was posted to the Internet by a classmate. Rita Giordano & Darran Simon, *Cyberbullying and Bias Issues in Rutgers Student's Suicide*, PHILADELPHIA INQUIRER, Oct. 1, 2010, at A16. In late November of 2008, a Florida teenager committed suicide live over the Internet.

The outcome of the Drew case, ending in acquittal for vagueness grounds, may push legislatures to enact more appropriate legislation.

However, specific legislation that addresses cyber bulling also raises constitutional concerns as it runs the risk of being overbroad and chilling free speech. In response to the failure of the local authorities to charge Drew, Dardenne Prairie immediately passed a city ordinance that outlawed cyber harassment. Although only a misdemeanor, it is punishable by up to ninety days in jail and a fine.[148] On June 30, 2008, Missouri governor, Matt Blunt, signed a bill updating the state's own harassment statute to include harassment over the Internet. Upon signing the law, Governor Blunt stated, "[w]e must take every step possible to protect our youth and to punish those who want to bring them harm. Social networking sites and technology have opened a new door for criminals and bullies to prey on their victims, especially children."[149] Just three months after the statute went into affect seven people were charged using the new cyber harassment law.[150]

At the federal level Representative Linda Sánchez (D-CA) re-introduced bipartisan legislation that would criminalize cyber bullying. The Megan Meier Cyberbullying Prevention Act provides "[w]hoever transmits in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior, shall be fined under

---

The teen posted his suicide note to an Internet web site "Justin.tv" and streamed a live video of himself after taking a lethal overdose of anti depressant medications. Rich Phillips et al., *Officials: Teen Commits Suicide on Webcam as Others Watch*, CNN.COM (Nov. 21, 2008), http://www.cnn.com/2008/CRIME/11/21/webcam.suicide/index.html?iref=mpstoryview. Viewers were able to witness his death and post comments as they watched the video. *Id.* Some of the comments urged him to take more drugs, questioning whether he had taken enough to kill himself. *Id.* Others egged him on, and still others posted messages suggesting the event was a fake. *Id.* The video streamed for ten hours before a viewer had the courage to contact the site's moderator who then contacted the police. *Id.* The teen was found dead in his bed. *Id.*

The anonymity of the Internet creates a disconnect that unfortunately allows more to happen online than might happen in real life. *See* Kowalski & Limber, *supra* note 3, at S23. It seems unlikely that if bystanders saw the Florida teen attempting to commit suicide in real life that they would be egging him on or be so complacent in trying to get him help. Likewise, Lori Drew used the anonymity and cover of the Internet to her advantage in order to gain information from and harass Megan. Had it not been for the use of MySpace, Lori Drew's plan may not have worked, nor may she have been willing to contact Megan directly.

148. Stevie Smith, *Cyber Bullying Declared Illegal Following Child Suicide*, MONSTERS AND CRITICS (Nov. 23, 2007, 3:10 AM), http://www.monstersandcritics.com/tech/news/article_1375817.php.

149. *Internet Law – Missouri Governor Signs Cyber-Bullying Bill into Law*, INTERNET BUSINESS LAW SOCIETY (July 14, 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?id=2095&s=latestnews.

150. Kim Zetter, *Prosecutors Charge 7 People Under New Cyberbullying Law*, WIRED.COM, THREAT LEVEL BLOG (Dec. 19, 2008, 3:38 PM), http://blog.wired.com/27bstroke6/2008/12/seven-people-ch.html.

this title or imprisoned not more than two years, or both."[151] Kenny Hulshof (R-MO), a co-sponsor on the identical bill introduced in the 110th Congress, stated in a press release that the bill "establish[ed] a fair legal standard. It sets needed limits for online conduct while protecting free speech."[152] Despite assurances by these two lawmakers that their cyber bullying legislation would protect free speech on the Internet,[153] there are several concerns about cyber bullying legislation in general that would need to be addressed carefully by lawmakers in order to adequately protect free speech.

1. Does Cyber Bullying Legislation Survive First Amendment Attacks?

In the flurry to respond to this new and emerging area of online harassment, legislatures should be careful to preserve constitutional bounds. Any law that would criminalize cyber bullying in some form would likely implicate the First Amendment. However, freedom of speech is not absolute, even online. First Amendment jurisprudence has classified certain types of speech as categorically unprotected. These are categories of speech that the government is free to regulate.[154] The most relevant unprotected categories of speech for cyber bullying would be directed by the "true threats" and "incitement" doctrines and as such many states draft their statutes in this way to avoid constitutional attacks. Many states currently have legislation that outlaws cyber harassment in some form.[155] However, many statutes would have fallen short to criminalize Lori Drew's conduct. For example, many state statutes, such as Missouri's, require a true threat or a "credible threat" of bodily injury before the criminal statute is triggered.[156] In the case of Lori Drew nothing she did would have amounted to a true threat.[157] At least one state, Ohio, has adopted a reasonable person standard, triggering the statute if a reasonable person would fear immediate bodily harm or suffer emotional distress.[158] This may be a more encompassing and useful statute to prosecute cyber bullying as it focuses on the effect of the actions on the victim, and may have appropriately criminalized Drew's conduct.

In order to be constitutionally regulated, cyber bulling must be classified as either a true threat or incitement, or otherwise the legislation must be able to

---

151. Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009). Representative Sánchez's bill is identical to the bipartisan bill she introduced in the 110th Congress. Megan Meier Cyberbullying Prevention Act, H.R. 6123, 110th Cong. (2008).

152. Press Release, Linda Sánchez, Rep. Linda Sánchez Introduces Bipartisan Megan Meier Cyberbulling Prevention Act (May 22, 2008), *available at* http://lindasanchez.house.gov/index.php?option=com_content&task=view&id=347&Itemid=34 (relating to the first version of the bill, which was introduced in the 110th Congress).

153. *Id.*

154. *See, e.g.*, Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942) ("[I]t is well understood that the right of free speech is not absolute at all times and under all circumstances.").

155. *See The Bryant Park Project*, *supra* note 2.

156. *Id.*

157. *Id.*

158. *Id.*

pass strict scrutiny. While interpretations of the definition of a "true threat" vary, the general consensus among lower courts is that a true threat is "'governed by an objective standard—whether a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of intent to harm or assault.'"[159] Although the communications sent to Megan Meier's MySpace account likely caused some emotional distress, there were no true threats of violence or physical harm, so it is not likely that the conduct of Drew would meet the reasonable person standard.[160]

Statutes could attempt to criminalize cyber bullying if it reaches the level of the incitement to violence doctrine under *Brandenburg v. Ohio*.[161] *Brandenburg* established that speech that is likely to produce imminent lawless action is an unprotected class of speech under the First Amendment.[162] While suicide is illegal, it seems tenuous that Drew's words to Megan were likely to produce imminent suicide. However, there is evidence to suggest that Drew knew that Megan was on anti-depressant medications that she suffered from Depression, as well as Attention Deficit Disorder.[163] Despite being despicable, and obviously evincing poor judgment, it seems improbable that Drew's intent was to incite Megan to commit suicide.

One option to take cyber bullying legislation out of the ambit of the First Amendment is to focus on legislation aimed at schools to control their student's online activity.[164] The Supreme Court has recognized a compelling state interest in the protection of minors as long as the regulation does not restrict access to speech by adults.[165] Particularly in the school setting, the Court has found compelling government interests in regulating speech or conduct that disrupts school activities or is in contrast to their learning environment.[166]

A student's MySpace activity, especially involving cyber bullying, could implicate the interests of schools to protect children and their learning environment. Indeed, as the text of the proposed federal cyber bullying

---

159. Planned Parenthood of the Columbia/Williamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1074 (9th Cir. 2002) (quoting United States v. Orozco-Santillan, 903 F.2d 1262, 1265 (9th Cir. 1990)).

160. *See* Goodno, *supra* note 145, at 135-137.

161. 395 U.S. 444 (1969).

162. *Id.* at 447-48.

163. Maag, *supra* note 7, at A23.

164. Most laws against cyber bullying are aimed at school. At least thirteen states have passed such laws and the trend is likely to continue. Ashley Surdin, *In Several States, A Push to Stem Cyber-Bullying*, WASH. POST, Jan. 1, 2009, at A3.

165. *See* Reno v. ACLU, 521 U.S. 844, 869, 874-75 (1997) (invalidating the Communication Decency Act because although it protected minors on the Internet, it prevented adults from receiving the same information, and such, was unconstitutionally overbroad).

166. *See* Surdin, *supra* note 164. *See, e.g.*, *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969); *Morse v. Frederick*, 551 U.S. 393 (2007).

legislation recognizes, "[f]our out of five United States children aged 2 to 17 live in a home where either they or their parents have access to the Internet" and "[c]yberbullying can cause psychological harm, including depression [and may] negatively impact academic performance, safety, and the well-being of children in school."[167] Taken as true, the effects of cyber bullying would likely be a severe disruption to the school environment, and educators may have a case for censoring speech on MySpace in order to avoid frustration of their educational mission. This is in accordance with Supreme Court jurisprudence on the limits of when a school may censor speech.

In the landmark case *Tinker v. Des Moines Independent Community School District*,[168] the Court held that while school students do not completely shed their First Amendment rights when they enter school property, their rights may be constitutionally abridged due to the unique circumstances of the school setting.[169] The *Tinker* case involved students who wore a black armband to school to protest the Vietnam War in violation of a school policy restricting the wearing of such armbands.[170] The Court held that the armband was a form of expressive speech and as long as it did not disrupt the school or its activities, any action censoring such speech was unconstitutional.[171] This case also stands for the inverse proposition that speech or expressive conduct that frustrates or inhibits the educational mission of schools can be constitutionally restricted.[172]

Not fully addressed by the Supreme Court's First Amendment jurisprudence is whether the special circumstances of the school setting that can limit student's constitutional rights may extend beyond the schoolyard to restrict speech that occurs outside of school, or even restrict the speech of adults that has a negative effect on the school environment. Indeed, in the context of the Megan Meier case, her cyber bully was not a student at all, but rather an adult outside of the school environment. The reality is that most of students' Internet activity occurs at home, and not on school grounds. However, the pervasiveness and permanence of the Internet creates a greater risk that speech at home will creep into the schoolyard.

Indeed, lower courts are currently grappling with the issue of regulating out of school activity on MySpace. The Third Circuit Court of Appeals heard two such cases with similar facts, but issued disparate rulings. In the Middle District of Pennsylvania, a district court judge ruled that a school could permissibly suspend a student who posted a fake MySpace page that depicted her principal as a pedophile.[173] The court of appeals initially affirmed the

---

167. Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009).

168. 393 U.S. 503 (1969).

169. *Id.* at 511-14.

170. *Id.* at 504.

171. *Id.* at 514.

172. *Id.* at 509.

173. J.S. v. Blue Mountain Sch. Dist., No. 3:07cv585, 2008 WL 4279517 (M.D. Pa. Sept. 11, 2008), *aff'd*, 593 F.3d 286, 301 (3rd Cir. 2010); *see also* Shannon P. Duffy, *3rd Circuit Mulls School Discipline for Hoax Web Pages*, LAW.COM, THE LEGAL INTELLIGENCER (Dec. 11 2008), http://www.law.com/jsp/pa/PubArticlePA.jsp?id= 1202426654073.

decision and held that the *Tinker* reasoning could be extended to conduct occurring outside of school that has an effect on the school. "[W]e hold that off-campus speech that causes or reasonably threatens to cause a substantial disruption of or material interference with a school need not satisfy any geographical technicality in order to be regulated pursuant to *Tinker*."[174] However, in the Middle District of Pennsylvania a different district court ruled that school officials could not suspend a student for creating a fake MySpace profile of his principal.[175] In affirming the decision, the court of appeals held that since the profile was created on a home computer, off of school property, there failed to be a sufficient nexus to implicate *Tinker*. The court held "[i]t would be an unseemly and dangerous precedent to allow the state in the guise of school authorities to reach into a child's home and control [the student's] actions there to the same extent that they can control that child when he [or] she participates in school sponsored activities."[176]

On appeal, the Third Circuit Court of Appeals, sitting in two different three judge panels affirmed each ruling, despite the contrary holdings and reasoning applied to such similar facts.[177] Since issuing those opinions, the court sitting *en banc* has vacated each decision and has recently heard oral arguments in order to reconcile the cases.[178] With lower courts, and even appellate courts, differing so greatly in their judgments about the reach of constitutional protection for online activity, the Internet and the dangers of cyber bullying are sure to become the new frontier of First Amendment law.

B. Online Solicitation of a Minor Statutes

None of the research for this article suggested that a criminal charge under any applicable sex offense statute was considered in the Drew case. As noted previously, the indictment alleged that messages to Megan from the "Josh Evans" account were flirtatious and sexual in nature. They urged Megan to "touch the snake" of Josh Evans.[179] Perhaps if Drew were a man who was pretending to be a sixteen-year-old boy in order to chat with a thirteen-year-old girl, an online solicitation of a minor charge might have been considered. One alternative option to punish Drew is the federal[180] coercion and enticement statute, 18 U.S.C. § 2422, which states:

---

174. J.S. v. Blue Moutain Sch. Dist., 593 F.3d 286, 301 (3rd Cir. 2010).

175. Layshock v. Hermitage Sch. Dist., 412 F. Supp 2d 502 (W.D. Pa. 2006).

176. Layshock v. Hermitage Sch. Dist., 593 F.3d 249, 260 (3rd Cir. 2010).

177. *Compare id. with Blue Mountain Sch. Dist.*, 593 F.3d 286.

178. Donal Brown, *Pennsylvania Online Student Speech Cases Slated for June Review*, FIRST AMENDMENT COALITION, http://www.firstamendmentcoalition.org/2010/04/pennsylvania-online-student-speech-cases-slated-for-june-review/ (last visited Dec. 3, 2010).

179. Indictment, *supra* note 8, at 7.

180. Alternatively, the applicable Missouri state statute is MO. REV. STAT. § 566.151 (2006).

> [w]hoever, using the mail or any facility or means of interstate or foreign commerce . . . knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.[181]

The statute does not require that the intent of the perpetrator be to engage in sexual conduct with the minor, rather it is the intent to entice a minor to engage in sexual activity that is made criminal by the statute. The Sixth Circuit addressed this issue in *United States v. Bailey*.[182] The case involved the use of the Internet by the defendant to solicit minors to engage in sexual activity. On appeal, the defendant insisted that the statute must require that there be the specific intent to commit the illegal sexual acts, otherwise it would "criminalize mere sexual banter on the [I]nternet."[183] In rejecting that argument, the court held that "Congress has made a clear choice to criminalize persuasion and the attempt to persuade, not the performance of the sexual acts themselves. Hence, a conviction under the statute only requires a finding that the defendant had an intent to persuade or to attempt to persuade."[184]

In defense to a charge under the federal enticement statute, Drew might argue, as the defendant in *Bailey* did, that she had no intent to actually have sex with Megan. A second defense might be that the sexual nature of the chatting conducted between Drew and Megan did not rise to the level Congress intended to proscribe. The indictment only mentions vaguely the sexual content of some of the messages; prosecutors would have to access the complete records of the chats between "Josh" and Megan and only then would be able to make that determination.[185]

C. Non Criminal Remedies

Perhaps the statement to the world condemning Drew's conduct should not be in the voice of the criminal justice system at all. Once the outrage has subsided the legal policy direction set by this case will remain. The consequences of this case will likely have far reaching effects on the average American who uses the Internet. Are we willing to make such a sacrifice for justice in that form? After all, Drew's criminal indictment wasn't for causing harm to Megan, but rather it was for harming MySpace. This note has suggested several other options with which to criminalize Lori Drew's

---

181. 18 U.S.C. § 2422(b) (2006).

182. 228 F.3d. 637, 638 (6th Cir. 2000).

183. *Id.*

184. *Id.* at 639.

185. For more information on the Federal statute and its effectiveness to catch sexual predators who use the Internet, see generally Bridget M. Boggess, Note, *Attempted Enticement of a Minor: No Place for Pedophiles to Hide Under 18 U.S.C. § 2422(b)*, 72 MO. L. REV. 909 (2007) (discussing relevant law concerning attempted enticement of a minor and the potential defenses to a claim of attempted enticement under § 2422(b)).

conduct. Overlooked in the media storm, and in this article until now, is the possibility that criminal charges might not be appropriate. Perhaps the possible social and financial ruin Drew and her family face is a sufficient form of justice.

Since the outing of Drew by an Internet blogger[186] the Drews' lives have been challenging. The Drews run a small advertising business, and their customers and business partners were all harassed by phone calls and demands not to do business with them.[187] Drew and her husband report that they were getting harassing calls at all hours of the day and night on their cellular, home, and work phones.[188] In a bit of irony, their own cellular phones were hacked into. The outgoing message was changed to "this is Lori Drew the world famous MySpace murderer, if you would like some advice about how to kill a beautiful teenager, you have come to the right place."[189] In addition to the public outrage against them, the Drews will likely face civil action from the parents of Megan, and a judgment may take most of their assets. Perhaps the social disgrace Drew and her family will suffer and the public awareness surrounding cyber bullying is a sufficient form of justice in this case.

IV. CONCLUSION

Using the CFAA against Lori Drew, while legally sound, was an inappropriate use of the statute. The jurisprudence established by her indictment under the CFAA for violating MySpace's Terms of Service threatens to criminalize ubiquitous and innocuous Internet conduct. If the government's theory of the scope of the CFAA continues, it will chill important social activity that is conducted on the Internet. There are other options with which to criminalize the type of behavior Drew engaged in—if society is willing to do so. Federal cyber bullying statutes might be one such option, however, this type of legislation has the danger to run afoul of the First Amendment.

While it is important that the criminal justice system carries a big stick, it should proceed carefully to avoid the type of over criminalization that upsets the fair government/citizen balance. Undoubtedly, the CFAA can be a useful statute with which to criminally prosecute traditional computer hacking. Recently, a federal court sentenced 23 year-old David Kernell to one year in

---

186. Zetter, *Internet Fury Machine*, *supra* note 106. A blogger used her blog to post Lori Drew's name online. *Id.* A virtual lynch mob formed and the combined efforts of savvy Internet users led to the publication of her personal information. *Id.*

187. *Id.*

188. Steve Pokin, *Pokin Around: 'Kill Yourself,' 'Go to Hell,'- Lori Drew Talks About Her Phone Messages*, SUBURBAN JOURNALS (Feb 19, 2008, 5:23 PM), http://www.stltoday.com /suburban-journals/article_d55f11bd-6302-57a1-a81f-e761e9a6922a.html.

189. *Id.*

custody and three years of probation for hacking[190] into Vice Presidential candidate Sarah Palin's personal email.[191] Kernell accessed the former governor's private email account, captured some of her personal information and photos, and disseminated them on the Internet.[192] With similarity to the Drew case, the United States Attorney's Office for the Eastern District of Tennessee had initially pursued the felony enhancement, but ultimately was unable to argue that successfully to the jury. A jury found Kernell guilty of, among other charges, a misdemeanor violation of the CFAA.[193]

As our society becomes more technological and more of our activities are conducted online, we become more aware of the need for protection against cyber criminals. The CFAA, which is a broad and expansive statute, can be an extremely useful tool to combat online crime. However, with that great power comes a greater responsibility for the criminal justice system to self regulate and avoid prosecuting conduct just because the statute is a technical fit. Justice Holmes declared acutely that, "hard cases make bad law."[194] The impulse to punish Drew in some way is understandable. When an adult woman preys on the trust and insecurities of a troubled teenager, society's sense of what is moral and right is likewise assaulted. The surreptitious nature of her conduct calls for a public outing—dragging her out from behind her home firewall and into the public view where she can be chastised and an example made of her. But as compelling as the demand for justice is in this case, using the CFAA to punish her is bad law.

---

190. The author admits that the word "hacking" may not be the most appropriate term to describe the activity in this case. According to the indictment, the defendant merely used the email provider's password reset feature to gain access to the account. The defendant guessed at a series of answers to "secret" questions by using the Internet and information provided by the Governor herself about her own background. He was then able to change the password to the account and gain complete access to the information stored there. Indictment at 2, United States v. Kernell, No. 3:08-CR-142 (E.D.Tenn. 2009).

191. Press Release, Dep't of Justice, David C. Kernell Sentenced For Illegally Accessing Former Governor Sarah Palin's Email Account and Obstructing Justice (Nov. 11, 2010), *available at*, http://www.justice.gov/usao/tne/pr/2010/November/111210%20Kernell%20Sentencing%20E-mail%20Hacking.html.

192. The 2008 Republican Vice Presidential candidate faced criticism after the outing of her email hack in the press. Two of the published email exchanges involved state politicians. Many questioned whether it was appropriate that she used a private email account to conduct state business. Furthermore, after she was alerted to the hack, all the emails and the account were erased drawing criticism that she was avoiding freedom of information laws. Several commentators suggested that her conduct amounted to destruction of evidence relating to the federal investigation of her office over the "trooper-gate" scandal. M.J. Stephey, *Sarah Palin's E-Mail Hacked*, TIME (Sept. 17 2008), http://www.time.com/time/politics/article/0,8599,1842097,00.html.

193. United States v. Kernell, No. 3:08-CR-141, 2010 WL 3937421, at *1 (E.D. Tenn. Sept. 23, 2010).

194. N. Sec. Co. v. United States, 193 U.S. 197, 400 (1904) (Holmes, J., dissenting).