Loyola of Los Angeles Entertainment Law Review

Volume 29
Number 3 *The Grammy Foundation Entertainment Law Initiative 2009 Writing Competition*

Article 8

6-1-2009

# Myspace-ing is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act

Ryan Patrick Murray

# MYSPACE-ING IS NOT A CRIME: WHY BREACHING TERMS OF SERVICE AGREEMENTS SHOULD NOT IMPLICATE THE COMPUTER FRAUD AND ABUSE ACT

*Written February 2, 2009* *

## I. INTRODUCTION

Imagine the following scenario: you are the typical American parent with a teenage daughter. She uses social networking sites[1] like MySpace[2] and Facebook[3] to stay connected with her friends, send messages, and even meet new people online.[4] You do your best to keep track of her online activity, and you make sure that she is not communicating with anyone without your approval. One day, your daughter receives a message from a cute boy on MySpace, and she asks you to let her message him back and become his online friend. After looking over the message, you approve the friendship, and your daughter excitedly begins a new online relationship. Though your daughter and her new friend seem to be getting along well, one day this boy begins sending mean and degrading messages to her, seemingly without justification. The nature of these messages hurts your

* This comment was written prior to the decision of Judge George Wu to overturn the conviction of Lori Drew; Judge Wu handed down his opinion on August 28, 2009. All arguments and analysis were constructed with no knowledge of the court's ultimate decision. A Postscript is included at the end of this Comment to address Judge Wu's ruling and evaluate its effect on the case and the future of attempts to combat cyberbullying. *See infra* Part VI.

1. Social networking sites are websites that allow their users to connect with other users of the service to send messages, meet new people, and share thoughts and ideas in one location. *See* Definition of: Social Networking Site, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=social+networking+site&i=55316,00.asp (last visited Apr. 11, 2009).

2. MySpace: A Place for Friends, http://www.myspace.com (last visited Dec. 13, 2008).

3. Welcome to Facebook, http://www.facebook.com (last visited Jan. 3, 2009).

4. *See* About Us - MySpace.com, http://www.myspace.com/index.cfm?fuseaction=misc.aboutus (last visited Mar. 13, 2009); *see also* Facebook is on Facebook, http://www.facebook.com/facebook?ref=pf#/facebook?v=info&viewas=3417891 (last visited Mar. 13, 2009).

daughter deeply and causes her to become so distraught that she retreats to her room.

Under normal circumstances, the situation may have ended there. Your daughter might cry for a while, but eventually her sadness would dissipate, and she would move on. Conversely, if she were particularly vulnerable because of severe depression and previous suicidal thoughts, this situation might be enough to push her over the edge. Imagine that your daughter took her life because of what someone said to her online. Imagine, further, that the individual responsible for the messages knew of her fragile emotional state. Finally, imagine what it would be like to know that the person responsible for causing your daughter to commit suicide was her friend's mother—a neighbor that she had known her entire life. Would you not want the justice system to use any means necessary to punish this woman for what she did to your daughter?

Unfortunately, this is more than just a hypothetical situation.[5] In 2006, a Missouri woman named Lori Drew created a MySpace profile under the name "Josh Evans."[6] Using the profile, Ms. Drew, along with her daughter and an employee, sent messages back and forth with a 13-year-old girl named Megan Meier.[7] After receiving hurtful comments from "Josh," Megan Meier tragically hung herself in her closet.[8] In the time following this appalling incident, significant public outcry forced the federal government to find some way to punish Lori Drew for her conduct. This outcry led the US Attorney's office to bring charges under the Computer Fraud and Abuse Act of 1984[9] (CFAA),[10] and to Lori Drew's eventual conviction.[11]

While many applauded the government's tenacity in finding a way to enact some sort of justice on Lori Drew, the implications of the verdict reach far beyond this isolated case.[12] No one doubts that Lori Drew deserves to face serious consequences for her reprehensible behavior, but

---

5. *See* Kim Zetter, *Lori Drew Indicted in MySpace Suicide Case*, WIRED, May 15, 2008, http://blog.wired.com/27bstroke6/2008/05/lori-drew-indic.html (describing the case of Lori Drew, who engaged in an online hoax on a teenage girl who later committed suicide).

6. Steve Pokin, *MySpace Hoax Co-creator Says Drew Wrote Some Messages*, ST. CHARLES J., Apr. 3, 2008, http://stcharlesjournal.stltoday.com/articles/2008/04/12/news/sj2tn20080403-0404stc-meier0.ii1.txt.

7. *Id.*

8. Steve Pokin, *A Real Person, A Real Death*, ST. PETERS J., Nov. 10, 2007, at A1.

9. 18 U.S.C. § 1030 (2006).

10. Zetter, *supra* note 5.

11. Traci Tamura, *Guilty Verdicts in Case of MySpace User's Suicide*, CNN.COM, Nov. 26, 2008, http://www.cnn.com/2008/CRIME/11/26/internet.suicide/index.html.

12. *See infra* Part IV.

because of the means used to punish her, the government may have turned many other individuals into federal criminals.[13]

The average American spends about thirty hours per month online;[14] there are approximately 130 million MySpace profiles[15] as well as over 175 million Facebook users.[16] The Terms of Service (TOS) agreements of these websites establish under what conditions a user can access the sites.[17] As Lori Drew's conviction rests on her violation of the MySpace TOS agreement, any user who fails to meet the requirements of the agreement could face the same charges.[18] Even though Lori Drew should have to answer for what she did to Megan Meier, the government must strike a balance between everyone's individual freedom and the need to bring one person to justice.

This comment discusses the apparent disconnect between the desire to punish Lori Drew and the need to protect the rights of all Americans. It also examines the government's inappropriate usage of the CFAA to penalize Lori Drew for her actions and offers suggestions for a better approach to preventing this type of incident in the future. Section II provides a background of social networking, Megan Meier, and the CFAA. Section III illustrates the statutory, judicial, and constitutional grounds for not extending the CFAA to criminalize violations of websites' TOS agreements. Section IV then examines the reasons—such as the current laws applicable to cyberbullying and the difficulty in updating these statutes—why the government has attempted to punish Lori Drew with the CFAA.

## II. BACKGROUND

### *A. The Unique Nature of Social Networking Sites*

Social networking sites have no analogue to traditional methods of personal interaction. The ability to instantaneously connect with millions

13. *See, e.g.*, Brief for Electronic Frontier Foundation, et al., as Amici Curiae Supporting Defendant, at 4, United States v. Drew, No. 08-00582 (C.D. Cal. Sept. 4, 2008) [hereinafter EFF Brief].

14. Natalie Paris, *Americans Spend Most Time on the Internet*, TELEGRAPH.CO.UK, May 9, 2008, http://www.telegraph.co.uk/news/1940196/Americans-spend-most-time-on-the-internet.html.

15. Jessi Hempel, *How Facebook is Taking Over Our Lives*, FORTUNE, Feb. 17, 2009, http://money.cnn.com/2009/02/16/technology/hempel_facebook.fortune/index.htm.

16. *Id.*

17. *See infra* Part II.C.

18. *See infra* Part III.B.

of individuals around the world can be both a blessing and a curse.[19] According to a recent study, fifty five percent of all teens use social networking sites like MySpace and Facebook.[20] The increased use has led to a rise in what has been dubbed "cyberbullying."[21]

Social networking sites allow their users to communicate with each other in various ways. MySpace, for example, allows its members to send personal individual messages to another user, post comments on another user's profile page, publish bulletins that multiple users can see, or join group discussions.[22] Facebook similarly offers these methods[23] as well as instant messaging capabilities.[24] The vast array of options for sending communications can easily lead to an abuse of this technology.[25] Because of the ease of creating a profile under an alias, cyberstalkers and cyberbullies can harass their victims anonymously.[26]

Though MySpace explicitly prohibits activity that "harasses or advocates harassment of another person,"[27] MySpace staff cannot possibly monitor the millions of users that visit the site each month.[28] Thus, it is possible that harassing material will ultimately reach a significant percentage of individuals on MySpace.[29] There is definitely a need to protect young people from the bullying that can happen on social

---

19. *See* Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 129 (2007) (explaining that the Internet allows for messages to be instantaneously disseminated to individuals around the world).

20. AMANDA LENHART & MARY MADDEN, PEW INTERNET, SOCIAL NETWORKING WEBSITES AND TEENS: AN OVERVIEW (2007), http://www.pewinternet.org/~/media/Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf.pdf

21. *See* Justin W. Patchin & Sameer Hinduja, *Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying*, 4 YOUTH VIOLENCE & JUV. JUST. 148, 148 (2006).

22. MySpace Quick Tour, http://www.myspace.com/index.cfm?fuseaction=userTour.home (last visited Oct. 15, 2008).

23. *See* Facebook is on Facebook, *supra* note 4.

24. Elizabeth Landau, *Facebook Unveils Instant Message Feature*, CNN.COM, http://www.cnn.com/2008/TECH/04/08/facebook.chat/index.html (last visited Mar. 13, 2009).

25. *See* Goodno, *supra* note 19, at 129 (noting that the internet allows cyberstalkers to quickly disseminate intimidating and threatening messages).

26. *Id.* at 130.

27. Terms & Conditions - MySpace.com, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Apr. 16, 2009).

28. *See* Matthew C. Ruedy, Comment, *Repercussions of a MySpace Teen Suicide: Should Anti-Cyberbullying Laws be Created?*, 9 N.C. J. L. & TECH. 323, 330 (2008) (stating that while MySpace does reserve the right to terminate the membership of a person violating the terms of service, it assumes no responsibility for monitoring the site for inappropriate content and that, ultimately, it is the responsibility of the teenage users and parents to protect themselves).

29. *See* I-SAFE, INC., I-SAFE STATISTICS 2, http://isafe.org/imgs/pdf/mediakit/i-SAFE_Stats.pdf (2008) ("22% of students know someone who has been bullied online.").

networking sites, but young people must be protected responsibly. The government cannot simply resort to questionable means for the sake of punishing someone who harasses another online—even in situations like that of Lori Drew.

### *B. The Story of "Josh" and Megan*

Megan Meier met "Josh Evans" in the fall of 2006. They did not meet at school or the mall—they met on MySpace.[30] Megan had received a friend request from Josh and asked her mother to let her start communicating with Josh online.[31] Their messages began innocently enough—just sharing information and getting to know each other—but eventually Josh turned on Megan.[32] On October 16, 2006, Josh sent several hurtful messages to Megan and even posted mean public messages on MySpace saying "Megan Meier is a slut . . . Megan Meier is fat."[33] According to Megan's father, Ron, the final message sent from Josh said, "Everybody . . . knows how you are . . . everybody hates you . . . [t]he world would be a better place without you."[34] After this barrage of insults, Megan went to her room and took her life.[35] Though this could have been the end to this tragic story, it was only the beginning.[36]

Six weeks after Megan's suicide, her parents found out that "Josh Evans" never existed.[37] Megan's family learned that the profile had been created by the mother of one of Megan's friends—someone who lived just a few houses down from Megan and her family,[38] a person that the Meiers knew and trusted.[39] The Meiers further learned that Lori Drew created the profile "in order to 'find out what Megan . . . was saying on-line about her daughter.'"[40] As the story of the attacks on Megan unfolded in the media, Lori Drew received international admonishment, but the county prosecutor had no way to criminally charge her for the part she played in Megan's

30. Pokin, *supra* note 8.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *See* Pokin, *supra* note 8.

37. Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23.

38. Pokin, *supra* note 8.

39. *Id.*

40. *Id.*

death.[41]

Almost two years after Megan Meier's death, a federal jury in Los Angeles convicted Lori Drew for cyber crimes that she allegedly committed in the course of her interactions with Megan.[42] However, these alleged crimes had nothing to do with Megan's death.[43] In an effort to find some way to punish Lori Drew, the government used an anti-hacking statute to criminalize everyday Internet activity.[44] In the U.S. Attorney's view, Lori Drew had committed a federal crime[45] by ignoring the MySpace Terms of Service (TOS) agreement, which prohibits creating a profile under a fake name.[46] After the trial, the jury convicted Lori Drew on three counts of violating the CFAA,[47] but the tragic and appalling nature of the case may have clouded their judgment.[48]

### *C. The Ubiquity of Terms of Service Agreements*

Most, if not all, websites that offer services to users of the site have TOS agreements.[49] TOS agreements are boilerplate agreements intended to be legally binding contracts. The agreements establish rules and policies that users must follow to access the services on a particular site.[50] The users, therefore, have zero bargaining power and, in many cases, have no choice but to assent to the terms if they want to use the site.[51]

Websites present their terms in two types of agreements: "clickwrap"

---

41. Maag, *supra* note 37.

42. Zetter, *supra* note 5; Tamura, *supra* note 11.

43. *See generally* Zetter, *supra* note 5.

44. *Id.* (stating that the crime that the U.S. Attorney charged Lori Drew with stems from her failure to meet the MySpace TOS agreement before using the site). Following this logic, any other MySpace user who creates a profile without entering their real name is guilty of the same crime, regardless of their subsequent activity on the site.

45. Indictment at 5, United States v. Drew, No. 08-00582 (C.D. Cal. May 15, 2008) [hereinafter Drew Indictment].

46. Terms & Conditions – MySpace.com, *supra* note 27 ("By using the MySpace Services, you represent and warrant that . . . all registration information you submit is truthful and accurate . . . .").

47. Tamura, *supra* note 11.

48. *See* Scott Glover, *Myspace Trial Jurors Hear of Girl's Suicide*, L.A. TIMES, Nov. 20, 2008, at B1 (stating that Ms. Drew's attorney had "asked that prosecutors be banned from mentioning Megan's death because it would unduly prejudice the jury," but the court denied his motion).

49. *See, e.g.*, EFF Brief, *supra* note 13, at 14.

50. *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 459 (2006).

51. *Id.* at 466; Rachel Cormier Anderson, Comment, *Enforcement of Contractual Terms in Clickwrap Agreements: Courts Refusing to Enforce Forum Selection and Binding Arbitration Clauses*, 3 SHIDLER J. L. COM. & TECH. 11 (2007).

and "browserwrap" agreements.[52] Clickwrap agreements present the user of a particular site with its TOS and require the user to click on a button to indicate that the user agrees to those terms.[53] Browserwrap agreements, in contrast, only exist somewhere on a provider's site.[54] The user never sees the TOS agreement, but their terms state that the user agrees to them simply by visiting the site.[55] While it may seem irregular to enforce a contract against someone who may have never read it, some courts have enforced particular terms of browserwrap TOS agreements.[56] Nonetheless, these cases involve businesses or other institutional users, and commentators argue that holding individual users to the terms of the TOS would be materially unfair.[57]

### *D. The Growth of the CFAA*

The development of computers has contributed significantly to advancements in American society. Nonetheless, fraud and other abuses of computers led Congress to adopt the CFAA in 1984.[58] The current version of the CFAA imposes a criminal penalty on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record of a financial institution . . . ; [or] information from any department or agency of the United States; or . . . information from any protected computer."[59]

The CFAA made it a federal crime to access a computer without authorization for the purpose of committing fraud or causing damage.[60] The original version of the statute only criminalized unauthorized access of government or banking computers.[61] However, updates and amendments have added language that makes it a violation of the CFAA to access a

52. Lemley, *supra* note 50, at 459–60.

53. *Id.* at 459.

54. *Id.* at 460.

55. *Id.*

56. *See, e.g.*, Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974 (E.D. Cal. 2000) (finding a question of fact as to whether a website's browserwrap agreement was conspicuous enough to alert users to its existence); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 428–30 (2d Cir. 2004) (holding that a business that used a website was on notice of the terms of use of that site).

57. *See* Lemley, *supra* note 50, at 464 ("[I]f courts enforce browserwraps at all, enforcement should be limited to the context in which it has so far occurred—against sophisticated commercial entities who are repeat players.").

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

59. 18 U.S.C. § 1030(a)(2) (2006).

60. *See id.* § 1030.

61. Buckman, *supra* note 58, at 112.

"protected computer" either without authorization or beyond the scope of the authorization granted to the user.[62] A "protected computer" in the statute means a computer "which is used in interstate . . . commerce or communication."[63] Since any computer that is connected to the Internet is used in "interstate communication," the CFAA potentially applies very broadly.[64]

This statute was originally "directed at protecting classified information, financial records, and credit information on governmental or financial institution computers."[65] The overwhelming majority of defendants charged with violating the CFAA have done so by either hacking into a computer with the intention of gaining access to sensitive information or by causing damage to a computer system.[66] Therefore, by using the CFAA to convict Lori Drew, the U.S. Attorney has taken the statute in a new direction.

Although the Government has effectively used the CFAA to prosecute hackers over the years, Congress did not intend for the act to criminalize violations of TOS agreements.[67] The U.S. Attorney's novel extension of the CFAA to prosecute Lori Drew not only ignores the intent of the statute, but could also lead to an unprecedented number of individuals committing federal crimes without any knowledge of wrongdoing.

## III. WHY THE CFAA IS THE WRONG TOOL FOR THE JOB

Lori Drew's conduct, while despicable, should not have been wrestled into the scope of the CFAA[68]—a statute that appears to only reach hackers and other individuals that willfully access a computer without proper authorization.[69] In an effort to convict Lori Drew of some type of crime associated with her interactions with Megan Meier, the U.S. Attorney brought charges under the CFAA for creating an account on MySpace that

62. *Id.* at 113.

63. 18 U.S.C. § 1030(e)(2)(B) (2006).

64. By covering all computers connected to the Internet, the CFAA has the potential to reach 73% of Americans. *See* Infoplease.com, Percentage of Internet Users in the U.S., 2008, http://www.infoplease.com/science/computers/demographics-internet-users.html (last visited Nov. 22, 2008) (stating data that suggests 73% of American adults have Internet access).

65. Buckman, *supra* note 58, at 112.

66. *See id.*

67. *See* Official Comment, 18 U.S.C. 1030 (1984) (discussing the reasoning behind the statute, which was to criminalize the relatively new threat of hackers).

68. 18 U.S.C. § 1030 (2006).

69. *See supra* Part II.D.

violated the site's TOS Agreement.[70] This theory states that by breaching MySpace's TOS agreement, Lori Drew exceeded the scope of the access she had been granted to a "protected computer."[71] Though the theory allowed the government to obtain a conviction[72] and bring some much needed solace to Megan Meier's family, the government's action was ultimately a mistake. The government should not have brought charges against Lori Drew under the CFAA in the first place.

### *A. Breaching a TOS Agreement Should Not Constitute a Violation of the CFAA*

Since the 1984 codification of the CFAA, several cases have applied the statute to individual conduct; interestingly though, none support the position that the U.S. Attorney proffered in Lori Drew's case.[73] While the CFAA had traditionally been used to punish those that used devious means to access and, then, harm or steal sensitive information,[74] the U.S. Attorney managed to hold Lori Drew criminally liable for violating a civil contract (the MySpace TOS agreement).[75] This theory of liability ignores the plain language of the CFAA as well as grossly expands the idea of "exceeding authorized access" within the statute.[76]

#### 1. The Value of Plain English

A jury convicted Lori Drew of violating the CFAA, which punishes an individual who "intentionally access[es] a computer without authorization . . . and thereby obtains . . . information from any protected computer . . . involved in interstate or foreign communication."[77] A plain language reading of this statute leads to the conclusion that Congress designed it to punish computer trespass. The terms "intentionally access"

---

70. Drew Indictment, *supra* note 45, at 6.

71. *Id.* at 9.

72. *Id.* at 1.

73. The case history of the CFAA usually includes individuals being charged with the destruction or theft of valuable information. *See, e.g.*, United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (finding that the defendant violated the CFAA by sending a "worm" that harmed various computers); United States v. Mitra, 405 F.3d 492, 497 (7th Cir. 2005) (holding that the defendant violated the CFAA by interfering with a computer-based emergency communication system); United States v. Lloyd, 269 F.3d 228, 243 (3d Cir. 2001) (convicting defendant of violating the CFAA by destroying files on his employer's computers).

74. *See* cases cited *supra* note 73.

75. Drew Indictment, *supra* note 45, at 1.

76. *See* discussion *infra* Part III.A.1–2.

77. 18 U.S.C § 1030 (2006).

and "without authorization" indicate that the statute should only reach the conduct of individuals who purposefully gain access to a specific computer.[78] Additionally, the emphasis on "obtain[ing] information" suggests that hackers and other information thieves are the intended focus of the CFAA.[79]

This plain language interpretation of the CFAA should constrain the scope of the statute because a court may invalidate any law for unconstitutional vagueness if it proscribes conduct not clearly established in its language.[80] However, by charging Lori Drew with violating the CFAA, the U.S. Attorney's office appears to have ignored the plain language of the statute.[81] By suggesting that the breach of a TOS agreement—involving no intentional unauthorized access of a computer—falls within the scope of the CFAA, the government has forced many innocuous activities into the realm of criminal conduct.

Lori Drew did not circumvent any security measures or access protected data on a protected computer, she merely established an account on MySpace under a fake name.[82] Therefore, her conduct was not the type that the CFAA was enacted to prevent.[83] When reading the unambiguous terms referring to the "intentional unauthorized access,"[84] it seems clear that the CFAA should not punish an individual who neither sought to obtain information from, nor cause harm to, a particular computer.

The legislative history supports a plain language interpretation that the goal of the statute was to quell the activities of hackers.[85] The House Committee that enacted the legislation explained that "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense."[86] This evidence suggests that the enacting body chose the words of the statute for particular clarity.

Courts have also taken the position that the clear language of the statute indicates that it was intended to criminalize intentionally malicious

78. *See id.*

79. *See id.*

80. *See* Kolender v. Lawson, 461 U.S. 352, 353 (1983) (describing that vague statutes are a violation of the Fifth and Fourteenth Amendments to the Constitution); discussion *infra* Part III.C.

81. *See* 18 U.S.C § 1030.

82. *See supra* Part II.D.

83. *See supra* Part II.D.

84. 18 U.S.C § 1030 (2006).

85. H.R. REP. NO. 98-894, at 20 (1984).

86. *Id.*

conduct.[87] For example, in applying a similar subsection of the statute, the court in *US v. Morris* stated that intentional conduct was required to show a violation of the statute.[88] In applying this unambiguous language to the conduct that led to the conviction of Lori Drew, it appears that an unintentional violation of the MySpace TOS agreement fails to meet the requirements of the CFAA.[89] Merely failing to supply truthful identity information seems quite different than intentionally causing harm through the unauthorized access of a computer.

Through Lori Drew's conviction, the government has substantially expanded the scope of the CFAA. Unfortunately, this means that anyone who fails to provide accurate information to MySpace or Facebook could be guilty of a federal crime.[90] While Lori Drew certainly deserved some form of punishment, her conviction may cause a serious problem for a large number of Americans. The expanded scope of the CFAA could make it illegal for anyone to use a website in violation of a TOS agreement.

### 2. Are We "Exceeding Authorized Access?"

The government convicted Lori Drew for exceeding the authorized access granted by MySpace when she failed to comply with the limitations on access imposed by the site's TOS agreement.[91] This conviction, therefore, greatly expands the concept of when an individual can exceed their authorized access. On the contrary though, recent cases exploring the idea of "exceeding authorized access" apply the CFAA more narrowly than the government did in Lori Drew's case.[92]

The original language of the CFAA found a crime only when *unauthorized* individuals accessed a "protected computer."[93] However,

87. *See* cases cited *supra* note 73.

88. *See* United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991) (stating that the statute only punishes those who intentionally access a computer without authorization).

89. *See Id.*

90. The TOS agreements of both of these sites require users to provide complete and accurate information. *See* Terms & Conditions - MySpace.com, *supra* note 27; Facebook Terms of Use, http://www.facebook.com/facebook?ref=pf#/terms.php?ref=pf (last visited Sept. 26, 2008).

91. *See* Drew Indictment, *supra* note 45, at 5.

92. *See, e.g.*, Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (rejecting the argument that a contractually prohibited use of a computer violated the CFAA); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (explaining "a violation . . . occurs where . . . the access of certain information is not permitted."); Brett Senior & Assocs. v. Fitzgerald, 2007 WL 2043377, at *2 (E.D. Pa. July 13, 2007) (explaining that the defendant "cannot be liable under the statute unless he, at a minimum, trespassed into [plaintiff's] computer system").

93. 18 U.S.C. § 1030 (1984).

Congress amended the statute in 1986 to include the phrase "exceeds authorized access."[94] One court explained that this was done to remove ambiguity from cases in which an *authorized* user of a "protected computer" used that computer for *unauthorized* purposes.[95] The U.S. Attorney's view, as evidenced by Lori Drew's conviction, is that using a website in violation of its TOS exceeds the authorized access of that website.[96] This view represents a broadening of the idea of "exceeding authorized access," which appears contrary to recent court decisions and scholarship advocating a narrower view of this particular CFAA provision.[97]

Professor Orin S. Kerr argues that "[c]ourts should reject a contract-based theory of authorization, and should limit the scope of unauthorized access statutes to circumvention of code-based restrictions on computer privileges."[98] Statutes and courts should, therefore, define the activities that amount to unauthorized access, instead of permitting private individuals to dictate the law through contracts.[99] This would allow "individuals to use the Internet without fear of criminal prosecution for a violation of sometimes incomprehensible contractual limits on use."[100]

Professor Kerr's idea becomes acutely relevant when exploring several TOS agreements. Many websites' TOS agreements contain vague and ambiguous terminology, have unexpected terms, and are not easily accessible to users.[101] Therefore, even if civil courts held these agreements enforceable against all users, Professor Kerr argues that it would not make sense to use the CFAA to extend that civil liability into criminal court.[102]

Professor Kerr wanted to dissuade courts from expanding the broad interpretation of "exceeding authorized access" that had recently developed at the time of his writing.[103] Apparently, the courts listened to Professor

---

94. *Id.*, *amended by* Pub. L. No. 99-474, § 2(c) (1986).

95. *Werner-Masuda*, 390 F. Supp. 2d at 499 n.12.

96. Drew Indictment, *supra* note 45, at 5.

97. *See, e.g.*, cases cited *supra* note 92; Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1643 (2003).

98. Kerr, *supra* note 97, at 1596.

99. *See id.* at 1600 ("The fact that computer use violates a contractual restriction should not turn that use into an unauthorized access.").

100. *Id.*

101. *See* EFF Brief, *supra* note 13, at 10–11, 31–34; Google Terms Of Service, http://www.google.com/accounts/TOS (last visited Apr. 13, 2009).

102. *See* Kerr, *supra* note 97, at 1600 (arguing that it would be unfair for courts to extend the civil liability from violating computer use agreements into the criminal context).

103. *Id.* at 1600–01.

Kerr's recommendations because judges began reducing the scope of the CFAA by narrowly interpreting the terms "authorization" and "access."[104] These cases represent a more appropriate application of the CFAA in situations where a violation of contractual terms could potentially lead to criminal liability.

In *International Association of Machinists and Aerospace Workers v. Werner-Masuda*, the Maryland District Court rejected the plaintiff's argument that using a union computer to access a membership list, in breach of an employment agreement, resulted in a union officer's violation of the CFAA.[105] The court found the defendant's conduct was not criminal, even though the defendant had breached the contract.[106] The court explained:

> [t]o the extent that Werner-Masuda may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established . . . , it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of . . . the CFAA.[107]

Like the employment contract that established the parameters for authorized access in *Werner-Masuda*, a TOS agreement sets out conditions that a user must meet before they are granted access to a particular website.[108] While a user may face consequences from breaching the TOS agreement, the failure to uphold the contract does not make a user's usage of the site an intentional unauthorized access of information.[109] Therefore, applying the court's reasoning in *Werner-Masuda* to Lori Drew's case implies an opposite conclusion than what ultimately occurred.[110] *Werner-Masuda* suggests that establishing a violation of the CFAA requires something more than the breach of a contract;[111] perhaps intentional efforts must be used to procure unauthorized access.

---

104. *See, e.g.*, cases cited *supra* note 92.

105. Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 498 (D. Md. 2005).

106. *Id.*

107. *Id.*

108. *See* Terms & Conditions – MySpace.com, *supra* note 27 ("This Agreement is accepted upon your use of the MySpace Website or any of the MySpace Services and is further affirmed by you becoming a Member."); Facebook Terms of Use, *supra* note 90 ("By accessing or using our web site . . . you [the "User"] signify that you have read, understand and agree to be bound by these Terms. . . .").

109. *See Werner-Masuda*, 390 F. Supp. 2d at 498.

110. *See id.*

111. *See id.*

A website's TOS agreement does not necessarily preclude access to the information on the site—at least not in the same way a password or other code-based impediment would.[112] Though MySpace requires a username and password to access an account, the accounts themselves are given freely to anyone that requests them.[113] In fact, on MySpace's signup page, users need only input their information and click a box that signifies they agree to the TOS;[114] MySpace does not attempt to enforce the provisions of the TOS before granting access.[115] Therefore, a visitor to the MySpace website has not had to circumvent restrictions in order to access the services therein and should not qualify as an unauthorized user for the purposes of the CFAA.[116] This reasoning also appears more in line with the original intent for the CFAA—punishing hackers for bypassing security measures and accessing protected information.[117]

### *B. An Improper Reliance on TOS Agreements*

Lori Drew's conviction for violating the CFAA is based on her failure to comply with the MySpace TOS agreement.[118] This means that any Internet user who breaches a website's agreement may be indicted under the same charges. This places an improper significance on a potentially unconscionable and unclear contract.

#### 1. Unconscionability of TOS Agreements

For her conduct to rise to the level of violating the CFAA, Lori Drew would have to access MySpace's servers without proper authorization.[119] The government theorized that this occurred when Lori Drew violated the

---

112. *See* Kerr, *supra* note 97, at 1600 (explaining the difference between contractual and code-based restrictions).

113. *See* MySpace.com Profile Signup Page, http://signups.myspace.com/index.cfm?fuseaction=signup (last visited Apr. 10, 2009).

114. *See id.* ("By clicking Sign Up, you are agreeing to the Myspace Terms of Service and Privacy Policy.").

115. For example, the site does not attempt to validate identification information before allowing the user to access the site. *See id.*

116. Much like Ms. Werner-Masuda, a user who creates a MySpace account in violation of the TOS agreement has breached that contract. However, this is not tantamount to a hacker who has used unscrupulous means to access information outside the scope of authorization; *see Werner-Masuda*, 390 F. Supp. 2d at 498.

117. *See* H.R. REP. NO. 98-894, at 20 (1984) (illustrating that the legislature enacted the CFAA in order to be able to punish hackers and others for what amounted to computer trespass).

118. Drew Indictment, *supra* note 45, at 6.

119. *See* 18 U.S.C. § 1030 (2006) ("exceeding authorized access").

MySpace TOS agreement, which prohibits supplying false information.[120] In effect, the government has imposed criminal liability for violating a contractual term—in a type of contract that even civil courts are reluctant to enforce.[121] In cases where courts have considered whether a website's TOS agreement was enforceable against a user, many courts have not upheld these terms in order to protect consumers.[122] The basic principles of contract law suggest that such importance should not be placed on TOS agreements.[123]

The doctrine of unconscionability suggests that a party should not have to uphold its part of a contract that would result in a distinctly unfair outcome.[124] The official comment to the U.C.C. clearly states that "[t]he principle is one of the prevention of oppression and unfair surprise."[125] This goal of preventing oppression and unfair surprise has lead to the adoption of *substantive* and *procedural* unconscionability.[126] For example, in *NEC Technologies, Inc. v. Nelson*, the court stated:

> Procedural unconscionability addresses the process of making the contract, while substantive unconscionability looks to the contractual terms themselves. A non-inclusive list of some factors courts have considered in determining whether a contract is procedurally unconscionable includes the age, education, intelligence, business acumen and experience of the parties, their relative bargaining power, the conspicuousness and comprehensibility of the contract language . . . .[127]

Applying the factors laid out in *NEC Technologies* to TOS agreements could easily result in the determination that these contracts are

---

120. Drew Indictment, *supra* note 45, at 6; Terms & Conditions – MySpace.com, *supra* note 27.

121. *See* discussion *supra* Part II.C.

122. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 35–38 (2d Cir. 2002) (refusing to hold consumers liable for terms in boilerplate agreement on a website); Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 556–57 (1st Cir. 2005) (holding that an employer could not change a provision of an employment agreement by posting it on the company intranet); Waters v. Earthlink, Inc., 91 F. Appx. 697, 698 (1st Cir. 2003) (requiring proof that a consumer had seen an arbitration clause before enforcing the provision).

123. *See, e.g.*, 7 ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 29.1, at 377 (Joseph M. Perillo ed., Matthew Bender 2002) (1951).

124. *Id.*

125. U.C.C. § 2-302 (2003) (Official Comment).

126. *See* Arthur Allen Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485, 487 (1967) (labeling the formation of the contract as procedural unconscionability (surprise) and the content of the contract as substantive unconscionability (oppression)).

127. NEC Techs., Inc. v. Nelson, 478 S.E.2d 769, 771–72 (Ga. 1996) (citations omitted).

both procedurally and substantively unconscionable.[128] The TOS agreements of most sites are hidden behind a hyperlink at the bottom of a webpage and are long, unorganized, and written in incomprehensible legalese.[129] For example, the TOS agreement for eBay can only be found by searching for the "User Agreement" hyperlink in fine print at the bottom of the site's home page.[130] Clicking the link takes users to a 3,000-word agreement that would be difficult to understand for anyone without a strong background in contract law.[131] Additionally, these agreements are standard boilerplate contracts that offer zero bargaining power to the users of the website;[132] users have no choice but to agree to the terms as the site presents them.[133]

Though this ambiguous language does not make TOS agreements *per se* unconscionable, the seemingly unfair nature of these contracts seriously casts doubt on their enforceability.[134] Because it may be unfair to enforce the terms of most TOS agreements on website visitors, assigning a criminal penalty for non-compliance with these terms would grant far too much weight to these contracts. While scholars and courts still disagree on the enforceability of TOS agreements on the civil side, it seems improper to assign criminal penalties for violating the terms of these agreements.[135]

### 2. The Vagaries of TOS Agreements

The inherent imperfection of TOS agreements extends beyond its potential unconscionability: many TOS agreements also contain unexpected terms and may change without notice.[136] For example,

---

128. Since most users of websites are relative laymen when it comes to TOS contracts, their lack of experience and business acumen would support a finding of procedural unconscionability; the fact that TOS agreements often contain ambiguous and difficult to find terms goes to their substantive unconscionability. *See id.*

129. EFF Brief, *supra* note 13, at 10–11.

130. Ebay.com, http://www.ebay.com (last visited Nov. 16, 2008).

131. *See* Your User Agreement, http://pages.ebay.com/help/policies/user-agreement.html?_trksid=m40 (last visited Nov. 16, 2008).

132. Anderson, *supra* note 51.

133. *Id.*; Lemley, *supra* note 50, at 465–66.

134. *See* CORBIN, *supra* note 123, at 379 ("Equity however, . . . will frequently order the avoidance of contracts.").

135. *See, e.g.*, Lemley, *supra* note 50, at 472–76 (discussing the reluctance of courts to unilaterally enforce contracts on web pages); Anderson, *supra* note 51 (explaining how recent cases have established a trend in enforcing standard provisions against business users, but not against consumers).

136. *See, e.g.*, Google Terms Of Service, *supra* note 101 (providing that "the form and nature of the services which Goggle provides may change from time to time without prior notice to you").

Google's TOS requires that anyone using its services first accept its contractual terms.[137] Moreover, the terms state, "[y]ou may not use the Services and may not accept the Terms if . . . you are not of legal age to form a binding contract with Google."[138]

In the aftermath of Lori Drew's conviction for violating the CFAA, any minor who performs a search on Google is now accessing a "protected computer" and, thus, is susceptible to federal prosecution.[139] This unexpected term, coupled with the fact that Google's TOS is relatively hidden on its site,[140] illustrates the danger of attaching criminal liability to the violation of TOS agreements.

### *C. Using the CFAA to Punish a TOS Violation is Unconstitutional*

Even though the application of the CFAA to criminalize infringement on a civil contract seems inappropriate, that is not the most significant problem with Lori Drew's conviction. Instead, the usage of the CFAA to criminalize conduct like that of Lori Drew constitutes an encroachment on civil liberties, e.g., the constitutional right to due process of law,[141] the freedom of speech,[142] and individual privacy.[143] If failing to comply with a website's TOS agreement in any and all circumstances violates the CFAA,[144] then the government will directly abridge these fundamental rights.

#### 1. Even MySpace Users Are Due Their Process

The Fifth Amendment to the Constitution's Due Process clause guarantees that the government cannot deprive an individual of "life, liberty, or property, without due process of law."[145] The Supreme Court interprets this clause to protect both procedural and substantive due process.[146] This means the government must follow proper procedures

137. *Id.*

138. *Id.*

139. *See generally* Drew Indictment, *supra* note 45 (showing that any violation of a TOS agreement may subject a user to criminal prosecution).

140. Google's TOS agreement can only be accessed by clicking a small link at the bottom of the site's main page. *See* Google, http://www.google.com (last visited March 24, 2009).

141. U.S. CONST. amend. V.

142. U.S. CONST. amend. I.

143. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding that there are certain "zone[s] of privacy created by several fundamental constitutional guarantees").

144. *See* Drew Indictment, *supra* note 45, at 1.

145. U.S. CONST. amend. V.

146. *See* United States v. Carolene Prods. Co., 304 U.S. 144, 152 (1938).

when interfering with an individual's liberties, have a valid reason for the interference, and use narrowly tailored means to achieve its interest.[147] The extension of the CFAA to criminalize violations of TOS agreements implicates both substantive and procedural due process because it infringes on individual liberties and causes the inconsistent terms of such agreements to have great importance.[148] While Part III.C.3 fully discusses the substantive issues below, the procedural matters have great significance as well.

A fundamental aspect of ensuring due process of law requires the government to clearly define what conduct a particular statute makes illegal.[149] Therefore, a criminal statute is invalid if it "fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden."[150] This standard appears to invalidate the U.S. Attorney's suggested interpretation of the CFAA: if traditionally vague and difficult to understand TOS agreements hold the same weight as criminal statutes, then the average Internet user would have difficulty fully comprehending exactly what conduct carries criminal liability.[151]

In *Kolender v. Lawson*, the Supreme Court struck down a California statute for being unconstitutionally vague as to what conduct actually violated the law in question.[152] The statute at issue in *Kolender* required persons loitering on the street to produce "credible and reliable" identification to a requesting police officer.[153] The court determined the statute violated Due Process because it was not sufficiently clear to alert ordinary citizens as to what specific conduct the statute criminalized.[154] In the opinion of the court, Justice O'Connor stated, "[o]ur Constitution is designed to maximize individual freedoms within a framework of ordered liberty. Statutory limitations on those freedoms are examined for substantive authority and content as well as for definiteness or certainty of expression."[155]

With the conviction of Lori Drew, the government has clearly adopted a statutory limitation on freedom with no clear definition of the

147. *See* Roe v. Wade, 410 U.S. 113, 155 (1973).

148. *See Carolene*, 304 U.S. at 152 n.4.

149. *See* Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939) ("No one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes. All are entitled to be informed as to what the State commands or forbids.").

150. United States v. Harriss, 347 U.S. 612, 617 (1954).

151. *See supra* Part III.B.2 (discussing the vague nature of TOS agreements).

152. Kolender v. Lawson, 461 U.S. 352, 361 (1983).

153. *Id.* at 353.

154. *Id.* at 361.

155. *Id.* at 357.

criminal activity subject to liability.[156] Since the outcome of Lori Drew's case means that all TOS agreements carry criminal liability for their violation, the CFAA can only be as clear as these inherently abstruse contracts.[157] The lack of clarity contained in TOS agreements has led the CFAA down the road of unconstitutional vagary.[158]

The Supreme Court also opined that the "void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness . . . in a manner that does not encourage arbitrary and discriminatory enforcement."[159] Much like the statute at issue in *Kolender*, a CFAA that relies on TOS agreements will lead to arbitrary enforcement.[160] The government has no control over what terms a website places in its TOS agreement, federal attorneys will thus be forced to either prosecute users who are in violation of atypical terms or arbitrarily enforce some agreements and not others.[161] For example, a website could place a term in its TOS agreement stating that women could not use the site. The government would then either have to bring all female users up on federal charges or decide not to enforce this specific term; thereby "vest[ing] virtually complete discretion in the hands" of federal prosecutors to decide when to enforce a website's terms—something that Due Process does not allow.[162]

### 2. Freedom ~~of Speech~~ to Be Held Criminally Liable

The Supreme Court in *Kolender* also worried about the "'potential for arbitrarily suppressing First Amendment liberties . . . .'"[163] The same concern should have impacted the court in the Lori Drew case where the U.S. Attorney extended the CFAA to include website TOS violations.[164] While extending the CFAA in this way may sufficiently punish online

156. *See* Drew Indictment, *supra* note 45, at 4–5 (relying on MySpace's unclear and easily modified TOS agreement to find liability under the CFAA).

157. *See, e.g.*, Terms & Conditions – MySpace.com, *supra* note 27; Facebook Terms of Use, *supra* note 90; Yahoo! Terms of Service, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited Mar. 1, 2009).

158. *Kolender*, 461 U.S. at 357 (stating that criminal statutes must "define the criminal offense with sufficient definiteness that ordinary people can understand").

159. *Id.*

160. Kerr, *supra* note 97, at 1659.

161. *Kolender*, 461 U.S. at 358 (stating that when a statute is vague, it "may permit 'a standardless sweep [that] allows . . . prosecutors . . . to pursue their personal predilections'") (citation omitted).

162. *Id.*

163. *Id.* (quoting Shuttlesworth v. City of Birmingham, 382 U.S. 87, 91 (1965)).

164. *See* Drew Indictment, *supra* note 45, at 6.

harassment, the "prospect of crime . . . does not justify laws suppressing protected speech."[165] The Supreme Court has held that speech on the Internet is protected by the First Amendment.[166] Thus, online speech warrants the same level of protection as other protected speech.[167] The criminalization that might occur under the new construction of the CFAA will severely undermine this protection.[168] The protections of free speech, including the ability to speak one's mind without fear of prosecution, should prohibit the CFAA from criminalizing violations of TOS agreements.[169]

By giving websites the power to dictate criminal liability simply through their seldom-viewed TOS agreements, the government is permitting actions that could potentially lead to serious interference with free speech.[170] Websites could include clauses in their TOS agreements prohibiting political or other particular opinions on public issues—exactly the type of speech that the Framers intended to protect through the First Amendment.[171] Such prohibitions would bring such protected speech within the reach of the CFAA.[172] Additionally, the vast protections afforded by the First Amendment go beyond simply protecting specific instances of speech, even invalidating some laws that might cause speakers to self-censor.[173]

In *Ashcroft v. Free Speech Coalition*, the Supreme Court struck down a law prohibiting "virtual child pornography"[174] because of its First Amendment implications.[175] The government certainly had noble motives in crafting the statute at issue in *Ashcroft*, just like the motives behind

165. Ashcroft v. Free Speech Coal., 535 U.S. 234, 245 (2002).

166. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) (stating that Supreme Court cases "provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]").

167. *See id.* at 868–70 (distinguishing the Internet from other speech restrictive mediums).

168. *See* EFF Brief, *supra* note 13, at 25 (arguing that the government's interpretation of the CFAA would make activities protected by the First Amendment "the basis for criminal liability").

169. *See* Ashcroft, 535 U.S. at 244 ("[I]mposing criminal penalties on protected speech is a stark example of speech suppression.").

170. *See* Kerr, *supra* note 97, at 1659 (arguing that breaching TOS agreements implicates criminal law and could "suppress a significant amount of free speech").

171. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964) (holding that "debate on public issues should be uninhibited, robust, and wide-open").

172. *See* Kerr, *supra* note 97, at 1659.

173. *See* Ashcroft, 535 U.S. at 244 (invalidating a law because it might lead some individuals to abstain from speech out of fear of prosecution, even though the speech would technically be protected under the First Amendment).

174. *Id.* at 241.

175. *Id.* at 244, 258.

applying the CFAA to Lori Drew's conduct. The provisions at issue in both cases may have even been quite effective at accomplishing their desired outcomes, namely protecting children and preventing online harassment.[176] Regardless, the government cannot achieve these goals through the proscription of protected speech, even if the majority of speech prohibited would receive no First Amendment protection.[177] This First Amendment requirement led the court in *Ashcroft* to hold that the terms of the statute were "overbroad and vague" and, therefore, could possibly lead some individuals to refrain from protected speech out of fear of prosecution.[178]

Similarly, since private websites are now permitted to define the parameters of a federal criminal statute through their TOS agreements,[179] some Internet users might refrain from exercising their freedom of speech because of the potential penalties. Since users may not clearly understand which type of speech a particular website might proscribe, their safest option would be to refrain from any speech. It is precisely this "chilling" of constitutionally protected speech that invalidated the law at issue in *Ashcroft*[180] and should require the overturning of the government's extension of the CFAA to include TOS violations.[181] As the Ashcroft *court stated*:

> The Government may not suppress lawful speech as the means to suppress unlawful speech. Protected speech does not become unprotected merely because it resembles the latter. The Constitution requires the reverse . . . . The overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process.[182]

The proposed increase in the scope of the CFAA "abridges the freedom to engage in a substantial amount of lawful speech"[183] and, thus, should not be allowed. "The Constitution gives significant protection from

176. For the government's reasoning behind the CPAA, which prohibited virtual child pornography, *see id.* at 241–42. The reasoning behind the indictment of Lori Drew, though a little more difficult to parse out, is most likely due to the desire to punish her any way possible; *see* Maag, *supra* note 37.

177. *See* Ashcroft, 535 U.S. at 245 (holding that the "prospect of crime . . . does not justify laws suppressing protected speech").

178. *Id.* at 243, 256.

179. *See* Drew Indictment, *supra* note 45, at 6.

180. *See* Ashcroft, 535 U.S. at 243, 256.

181. *See id.* at 255.

182. *Id.*

183. *Id.* at 256.

overbroad laws that chill speech within the First Amendment's vast and privileged sphere."[184] This protection means that the U.S. Attorney cannot arbitrarily increase the CFAA's scope in such a way that could lead to unconstitutional self-censorship.

### 3. The Right to Remain Anonymous

Anonymity has a special significance on the Internet.[185] The unique nature of the Internet allows individuals to "choose to say what [they] want to a mass audience in ways that obscure or conceal [their] real identities."[186] This ability to speak anonymously allows many individuals to share their true feelings without fear of retribution or to participate in activities that they would not want their neighbors to know about.[187] Most Internet users take comfort in the idea that their online presence is not directly connected to their offline world.[188] Despite the value of anonymous online speech, and the constitutional protections of anonymity and privacy, the government has effectively erased this protection by imposing criminal liability for providing false identification information to a website.[189]

The Supreme Court has stated that "fundamental rights" are protected by the Constitution from subversion by both the federal and state governments.[190] Certain liberties that are "deeply rooted in this Nation's history and tradition" are given stringent protection by the Constitution.[191] Anonymity is precisely the type of liberty that finds its roots bound up with the history of this nation.[192] When Alexander Hamilton and James Madison were advocating for the passage of the Constitution, they chose to publish their arguments under pseudonyms.[193] The fact that these

---

184. *Id.* at 244.

185. *See* MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 143–44 (rev. ed. 2003) (explaining that many individuals feel shielded from outside scrutiny simply because no one knows their true identity when they post online).

186. *Id.* at 143.

187. *See* Anonymity/Psuedonymity, Electronic Frontier Foundation, http://w2.eff.org/Privacy/Anonymity/ (last visited Oct. 20, 2008).

188. *See id.*

189. *See* Drew Indictment, *supra* note 45, at 6 (indicting Lori Drew for failing to disclose her true identity).

190. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003); Moore v. City of East Cleveland, 431 U.S. 494 (1977); Palko v. Connecticut, 302 U.S. 319 (1937); (providing examples of incorporated constitutional rights).

191. Moore, 431 U.S. at 503.

192. EFF Brief, *supra* note 13, at 23–24.

193. ALBERT FURTWANGLER, THE AUTHORITY OF PUBLIUS: A READING OF THE

"architects of the Constitution" [194] published their works anonymously speaks volumes regarding the deeply-rooted nature of this liberty and the constitutional protection that it should receive. Additionally, the Constitution's protection of free speech would surely be implicated if the government begins enforcing contractual requirements of identity disclosure. [195]

Many websites, including MySpace and Facebook, have clauses in their TOS agreements that require users to provide accurate personal information. [196] After the government's conviction of Lori Drew for violating the CFAA, anyone who exercises their constitutionally protected right of anonymity on these sites will commit a federal crime. [197] Private websites are operating well within their power when they infringe on a constitutional right, but once the government gets involved with the enforcement of a website's TOS, the Constitution gains some teeth. [198]

While it might be constitutionally permissible for MySpace to require users to disclose their personal information in a private contract, the Constitution precludes the government from enforcing such a provision. [199] In *Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton*, the Supreme Court struck down an ordinance that required door-to-door canvassers to first obtain a permit before canvassing in the village

---

FEDERALIST PAPERS 18 (1984).

194. *Id.* at 23.

195. *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 164 (2002) (holding a law that required door-to-door canvassers to first obtain a permit violated the First Amendment).

196. *See, e.g.*, Terms & Conditions – MySpace.com, *supra* note 27 ("By using the MySpace Services, you represent and warrant that . . . all registration information you submit is truthful and accurate . . . ."); Facebook Terms of Use, *supra* note 90 ("In consideration of your use of the Site, you agree to (a) provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ('Registration Data'); . . . (c) maintain and promptly update the Registration Data, and any other information you provide to Company, to keep it accurate, current and complete. . . ."); Yahoo! Terms of Service, *supra* note 157 ("You also agree to: (a) provide true, accurate, current and complete information about yourself as prompted by the Yahoo! Service's registration form (the 'Registration Data') and (b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete."); Google Terms of Service, *supra* note 101 ("You agree that any registration information you give to Google will always be accurate, correct and up to date.").

197. *See* Drew Indictment, *supra* note 45, at 6 (stating that Ms. Drew's violation of the CFAA occurred when she accessed the MySpace service by entering a false name).

198. *See* Shelley v. Kraemer, 334 U.S. 1, 20, 22 (1948) (holding that judicial enforcement of a private agreement qualifies as state action, which may lead to the agreement being struck down as unconstitutional).

199. *See Watchtower*, 536 U.S. at 164 (holding that a law requiring door-to-door canvassers to first obtain a permit before canvassing violated the First Amendment).

of Stratton.[200] The ordinance also required canvassers to present the identifying permit, containing their name, on demand.[201] The plaintiffs in *Watchtower* were religious proselytizers who went door-to-door to discuss their religion, though the court also took into account the effect the permit requirements might have on the spreading of other types of information, including political canvassing.[202]

Just as the Jehovah's Witnesses in *Watchtower* attempted to spread religious ideas through canvassing the village of Stratton, many individuals similarly use the Internet, and particularly social networking sites, to spread their ideas, thoughts, opinions, and political messages.[203] The court in *Watchtower* determined that it was unconstitutional to require someone to divulge their identity before they could share their ideas,[204] but that is exactly what the government has done by enforcing the identity disclosure requirement in the MySpace TOS agreement. As the Internet has become tantamount to the traditional public forums of old, *Watchtower* suggests that people have the constitutionally protected right to broadcast their views online anonymously.[205] Because Lori Drew's conviction established that it is a federal crime to violate the TOS agreements of MySpace, Facebook, Yahoo! and Google, all of which require the accurate disclosure of personal information,[206] the government is infringing on the rights of users of these sites.

In deciding *Watchtower*, the court stressed the value of anonymity when disseminating information: "'[t]he decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible.'"[207] These same motivations exist when individuals communicate online and so should the constitutional protections of privacy and anonymity. The right to assert one's opinion anonymously on the Internet easily follows from the traditional value given to anonymity and

200. *Id.*

201. *Id.* at 155.

202. *Id.* at 153.

203. *See, e.g.*, Jodi Kantor, *Obama's Online Strategy Seeks Big Bonus From Small Turnout*, N.Y. TIMES, Apr. 1, 2007, at A1 (describing how supporters of Barack Obama organized on a specialized social networking site).

204. *Watchtower*, 536 U.S. at 164.

205. *See id.*

206. *See* Terms & Conditions – MySpace.com, *supra* note 27; Facebook Terms of Use, *supra* note 90; Yahoo! Terms of Service, *supra* note 157; Google Terms of Service, *supra* note 101.

207. *Watchtower*, 536 U.S. at 166 (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995)).

the fundamental right to privacy that the Supreme Court has stated extends from the Constitution.[208] Extending the scope of the CFAA to allow private websites to dictate the elements of a criminal statute through their TOS agreements runs contrary to many American concepts of freedom and liberty—but this is exactly what the government has done.

In light of the numerous problems associated with Lori Drew's conviction for violating the CFAA,[209] in addition to the possible constitutional ramifications, the government should not have applied the statute in this particular situation. The appalling nature of Lori Drew's activities coupled with the apparent inability to bring charges under another statute led the U.S. Attorney's office to make a far reaching decision simply to effectuate justice.[210] However, the government would never have made such a decision if proper means of combating online harassment were available.

## IV. THE OTHER WAYS TO COMBAT ONLINE HARASSMENT

In a perfect world, Lori Drew would face severe consequences for her role in Megan Meier's death. Regardless, the government's extension of the CFAA does far more than punish Lori Drew for her activities on MySpace.[211] If the government begins enforcing the CFAA as it did against Lori Drew, there will be serious ramifications beyond the facts of that single case: it will effectively "convert the millions of internet-using Americans who disregard the terms of service associated with online services into federal criminals."[212] The government should use other statutory methods to prevent future conduct like that of Lori Drew; it need not unconstitutionally expand the scope of the CFAA to combat harassment on the Internet.

### *A. Current Laws*

The U.S. Attorney's use of an inappropriate statute to punish Lori Drew for causing Megan Meier's suicide illustrates the difficulty in applying current legislation to cyberbullying and cyberstalking cases.[213] Many current laws are too antiquated to adequately combat the emerging

208. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (discussing certain "zone[s] of privacy created by several fundamental constitutional guarantees").

209. *See* discussion *supra* Part III.A–B.

210. *See* Drew Indictment, *supra* note 45, at 1.

211. *See* U.S.C. § 1030(a)(2) (2006).

212. EFF Brief, *supra* note 13, at 4.

213. *See* Drew Indictment, *supra* note 45, at 1.

forms of online harassment.[214] While some states have taken the initiative to create laws to specifically address these new issues,[215] many states and the federal government have aging statutes containing significant gaps, despite the legislatures' attempts to institute updates.[216]

### 1. On the Federal Books

Most federal statutes available to combat cyberbullying and other forms of online harassment originally only handled traditional stalking and harassment.[217] This archaic design frequently leads to inadequacies in these statutes.[218] Consequently, individuals, and especially children, who find themselves dealing with harassing messages online generally have little recourse.[219] Although social networking sites like Facebook and MySpace have specific provisions in their TOS agreements that prohibit users from sending harassing or threatening communications, deleting the offending user's account is usually the only possible punishment these sites can levy.[220] Nonetheless, using an overly broad interpretation of the CFAA will cause too much conduct to fall into the realm of illegality. Therefore, federal statutes that specifically address the issues of cyberbullying and cyberstalking are necessary to combat the problem.

Despite the fact that federal statutes enacted to punish stalking and other forms of harassment did not initially leave room for new methods of possible victimization, some recent efforts have been made to update the statutes.[221] For example, the Violence Against Women Act[222] (VAWA)

---

214. Goodno, *supra* note 19, at 156.

215. *See, e.g.*, 720 ILL. COMP. STAT. ANN. § 5/12-7.5 (2002); LA. REV. STAT. ANN. § 14:40.3 (Supp. 2001); MISS. CODE ANN. § 97-45-15 (2000 & Supp. 2003); N.C. GEN. STAT. § 14-196.3 (2003); R.I. GEN. LAWS § 11-52-4.2 (2002); WASH. REV. CODE § 9.61.260 (Supp. 2004).

216. Goodno, *supra* note 19, at 140–52.

217. *See, e.g.*, 18 U.S.C. § 875(c) (2006) (making it a crime to transmit "any threat" to injure a person in "interstate commerce"); 47 U.S.C. § 223 (2006) (making it illegal to anonymously and knowingly use a "telecommunications device" to "annoy, abuse, threaten or harass" a person); 18 U.S.C. § 2261A (2006) (criminalizing conduct that involves interstate stalking that places victims in "reasonable fear of death").

218. Goodno, *supra* note 19, at 147–52.

219. *See id.* at 125 (describing how victims have few options to combat online harassers).

220. *See* Terms & Conditions – MySpace.com, *supra* note 27; Facebook Terms of Use, *supra* note 90.

221. *See generally* 47 U.S.C. § 223 (2006) (exemplifying a stalking statute that did not punish new methods of victimization).

222. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, Tit. I, § 113, 119 Stat. 2960, 2987 (2006) (codified as amended in 47 U.S.C. § 223).

amended the Federal Telephone Harassment Statute[223] (FTHS), which previously only punished harassing telephone calls,[224] to include "any device or software that can be used to originate . . . communications that are transmitted . . . by the Internet."[225]

Though this amendment updated the statute significantly, many types of cyberbullying still do not fit within the purview of the statute.[226] The Sixth Circuit Court of Appeals has interpreted the FTHS to require the harasser to use direct anonymous communications to place their victim in fear.[227] This interpretation not only excludes victims that know their harasser, it also fails to punish indirect communication such as postings on message boards or other online forums.[228] Additionally, the requirement that the victim actually fear their harasser leaves out bullying behavior that merely antagonizes the victim without actually threatening violence.[229] Other federal statutes, including the Interstate Communications Act (ICA)[230] and the Federal Interstate Stalking Punishment and Prevention Act (FISPPA),[231] also contain flaws that prevent them from fully protecting victims from cyberbullying and cyberstalking.[232]

In recent years, the government has used the ICA to prosecute cyberstalkers who have used the Internet to send threatening messages.[233] The ICA makes it a crime to transmit any threat of injury to a person through interstate commerce,[234] and at least one court has interpreted the term "interstate commerce" to include Internet communications.[235] Still, the ICA misses a large portion of online harassment because of its threat

223. 47 U.S.C. § 223 (2006).

224. *Id.*

225. *Id.* § 223(h)(1)(C).

226. *See* United States v. Bowker, 372 F.3d 365, 382–83 (6th Cir. 2004) (describing the elements of the Federal Telephone Harassment Statute, which requires the victim be in fear of their harasser and that the communication be anonymous), *vacated on other grounds*, 543 U.S. 1182 (2005).

227. *Id.* at 383.

228. Goodno, *supra* note 19, at 150.

229. *See Bowker*, 372 F.3d at 382–83 (requiring that the victim be in fear of their harasser to invoke the statute).

230. 18 U.S.C. § 875 (2006).

231. *Id.* § 2261A.

232. *See* Goodno, *supra* note 19, at 149–52.

233. *See, e.g.*, United States v. Kammersell, 196 F.3d 1137, 1138 (10th Cir. 1999), United States v. Alkhabaz, 104 F.3d 1492, 1493 (6th Cir. 1997).

234. 18 U.S.C. § 875(c) (2006).

235. *See Kammersell*, 196 F.3d at 1139 (holding that email messages that the defendant sent to the victim in the same state were in interstate commerce because the messages traveled through interstate phone lines).

requirements—illustrated by *United States v. Alkhabaz.*[236]

*Alkhabaz* involved the defendant posting an explicit story about the rape of a classmate in an online chat room.[237] Though the victim felt harassed and afraid, the court determined that the defendant had not violated the ICA because his communications did not contain an actual threat.[238] The threat requirement means that the ICA would not apply to many forms of cyberbullying and online harassment and is therefore inadequate to address and prevent this conduct.[239]

Just as VAWA had amended the FTHS to include language that could be used to combat cyberstalking, it also made significant changes to the FISPPA.[240] The new language in the FISPPA prohibits individuals who travel in "interstate or foreign commerce" from using "any interactive computer service" to cause "substantial emotional distress" to an individual.[241] This language makes the FISPPA more effective than the FTHS and the ICA because it does not require an actual threat or anonymous harassment.[242] Additionally, the increased flexibility of the "substantial emotional distress" requirement could address situations of serious harassment that might not involve fear but still result in emotional harm to the victim.[243] While this statute has the most promising ability to curtail most cyberstalking and cyberbullying, the FISPPA does not address every potential method of harassment.[244]

### *B. Solving the Problem*

There is an obvious need for a federal anti-cyberbullying statute that could specifically address the issues raised by the unfortunate case of Megan Meier.[245] However, two serious limitations exist that may prevent

---

236. *Alkhabaz*, 104 F.3d at 1496.

237. *Id.* at 1493.

238. *Id.* at 1496.

239. *See id.* at 1496–97 (Krupansky, J., dissenting) (criticizing the majority's decision to apply the ICA only in cases where the threat is "conveyed with the general intent 'to effect some change or achieve some goal through [intimidation]'").

240. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, Tit. I, § 114(a), 119 Stat. 2960 (2006) (codified as amended in 18 U.S.C. § 2261A).

241. *Id.*

242. *Id.*

243. *See* Goodno, *supra* note 19, at 152 (indicating that the new statute provides separately for "reasonable fear" and "substantial emotional distress").

244. *See id.* (discussing how the FISPPA does not cover instances of innocent third party harassment such as the harasser posting sexual invitations in the victim's name).

245. If current legislation could adequately address this issue, the U.S. Attorney's Office

the enactment of an all-encompassing statue: (1) the lack of manageable standards and (2) the constitutional protection of free speech and other individual liberties.[246] Thus, anyone that attempts to draft legislation to prevent cyberbullying and other forms of online harassment needs to remain cognizant of these limitations.[247]

For an online harassment prohibition to effectively protect Internet users, especially children, it must have broad language that criminalizes any type of harassing communications.[248] While previous statutes that required actual threats have failed to punish clearly harassing behavior,[249] others have not covered entire methods of harassment.[250] The ability of Internet users to transmit messages through several different channels means that legislation must be made flexible enough to cover methods of harassment that have no real world counterpart.[251] Nonetheless, this need for broad sweeping statutes must be balanced against the freedoms guaranteed by the Constitution.[252]

Legislation can assuage constitutional concerns by clearly defining its scope to include only intentionally harassing conduct.[253] The First Amendment does not protect all speech unequivocally.[254] Harassment, defamation, threatening speech, or language that could incite violence does not receive the same constitutional protection as political or other forms of valuable speech.[255] Therefore, any legislation that aims to prevent cyber-harassment should include elements that ensure specific intent to harass

---

would not have to resort to trying to punish Lori Drew under the CFAA. *See supra* Part III.

246. *See* Goodno, *supra* note 19, at 155 (suggesting that criminalizing cyberstalking could raise precarious constitutional issues, and that the data on cyberstalking is somewhat uncertain); Ruedy, *supra* note 28, at 344 (arguing that it would be difficult for a broad anti-cyberbullying law to survive constitutional scrutiny).

247. *See* Goodno, *supra* note 19, at 155.

248. *Id.*

249. *See* United States v. Alkhabaz, 104 F.3d 1492, 1496 (6th Cir. 1997) (holding that criminally harassing communications must contain an actual threat).

250. *See* Goodno, *supra* note 19, at 152 (discussing how the FISPPA does not cover instances of innocent third party harassment such as the harasser posting sexual invitations in the victim's name).

251. For example, online harassers can easily and convincingly impersonate their victim so as to cause harm— something that would be nearly impossible to do in the real world.

252. Ruedy, *supra* note 28, at 339.

253. Goodno, *supra* note 19, at 155.

254. *See* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW 1063–65 (6th ed. 2000) (discussing the lack of an absolute right to Free Speech).

255. *See id.* at 1060–62 (outlining the types of speech that deserve constitutional expression); *see also* Brandenburg v. Ohio, 395 U.S. 444 (1969) (establishing that speech inciting violence does not receive constitutional protection).

and a provision excluding constitutionally protected activity.[256]

Other issues that also plague the creation of legislation that could effectively curtail the potential rise in online harassment include the difficulty in catching some harassers and the lack of information on the actual level of cyber-harassment.[257] Since some harassers can employ creative means of antagonizing their victims with complete anonymity,[258] law enforcement officers could encounter severe impediments in executing the laws. Additionally, a lack of data exists on the true levels of online harassment; different jurisdictions report significantly contrasting statistics on cyberstalking.[259] However, these discrepancies may occur because of victims' lack of reporting and law enforcement agencies' lack of training.[260] Regardless of the number of victims affected by online harassment, cyberstalking and cyberbullying are serious issues that the federal government must directly address with new legislation.

Since the Constitution prohibits ex post facto laws,[261] the government cannot use any new legislation adopted in response to Megan Meier's suicide to charge Lori Drew. Nevertheless, federal legislators could use this unfortunate situation as a learning experience and adopt relevant legislation to prevent or punish future conduct similar to that found in the Lori Drew case.[262] The adoption of new legislation, specifically targeted at cyberbullying, could drastically reduce the likelihood of another tragedy like Megan Meier's suicide.

## V. CONCLUSION

Despite the fact that Lori Drew's indictment was based on an untenable legal foundation of an almost certainly unconstitutional extension of the CFAA, the U.S. Attorney's office obtained a conviction.[263] This conviction means that an individual who accesses a

256. Goodno, *supra* note 19, at 155.

257. *Id.* at 156.

258. Concealing one's identity while harassing others can easily be accomplished by creating fake email addresses, using computers at Internet cafes, etc. Even Lori Drew's true identity might not have been discovered if she had not revealed it to a neighbor.

259. U.S. DEP'T OF JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

260. *Id.*

261. U.S. CONST. art. I § 9.

262. Local legislators in Megan Meier's hometown have already passed city ordinances criminalizing cyberstalking and online harassment. *See* DARDENNE PRAIRIE, MO., MUNI. CODE § 210.030 (2007).

263. Tamura, *supra* note 11.

website in violation of a TOS agreement can be held liable in the same manner as Lori Drew. Lori Drew's conviction could lead to millions of unsuspecting Americans being charged with a violation of the CFAA for simply breaching a website's TOS agreement.

As previously discussed, many TOS agreements have unclear language that is hidden from view and contains unsuspected terms.[264] Additionally, the ability of websites to dictate the law could raise serious constitutional issues.[265] Nonetheless, even if all TOS agreements used the utmost clarity, remained visible to all users, and contained no unconstitutional subject matter, something would still be amiss. It seems fundamentally unfair to turn average Internet users into criminals for completely innocuous activities such as providing inaccurate personal information to a website. Still, this strange and improper outcome does make sense given the extreme nature of the situation that occurred between Lori Drew and Megan Meier.

The growth of the Internet over the last two decades coupled with the increasing sophistication of young people continues to lead to an exorbitant amount of kids and teenagers spending hours online every day.[266] Subsequently, social networking sites have sprung up to cater to the needs of an Internet-generation.[267] With these sites becoming the preferred social meeting place for young people, many social, academic, and entertainment activities have found their way online.[268] Unfortunately, bullying has also leapt into the digital age, and an increasing number of individuals have to deal with harassing communications online.[269] Some schools and other jurisdictions have responded to these developments,[270] but many remedies fall short of solving the ultimate problems that cyberbullying and other forms of online harassment pose to America's youth.

There are undoubtedly numerous victims of cyber-harassment, and Megan Meier's devastating story has certainly been one of the most publicized.[271] While the events that led Megan Meier to take her life were

---

264. *See supra* Part III.B.

265. *See supra* Part III.C.

266. *See* Alexandra Rankin Macgill, *Memo: Parent and Teenager Internet Use*, PEW INTERNET, Oct. 24, 2007, http://www.pewinternet.org/pdfs/PIP_Teen_Parents_data_memo_Oct2007.pdf.

267. *See* MySpace, *supra* note 2; *see also* Facebook, *supra* note 3.

268. Patchin & Hinduja, *supra* note 21, at 148.

269. I-SAFE, INC., *supra* note 29.

270. Ruedy, *supra* note 28, at 327–28.

271. *See* Kim Zetter, *Prosecutor Will Review Megan Meier Cyberbullying Case*, WIRED, Nov. 19, 2007, http://blog.wired.com/27bstroke6/2007/11/prosecutor-will.html (describing how Megan Meier's "story has received national attention").

reprehensible and her family may never receive adequate redress, this lack of justice should not lead to an unconstitutional and improper extension of the CFAA. Nevertheless, this case may bring the shortcomings of current anti-harassment legislation to light and convince legislators to either modify existing laws or enact new statutes to better address the growing trend of cyberbullying.

The motivation behind the U.S. Attorney's desire to use any means necessary to convict Lori Drew can be easily understood given the facts of this case. Still, the nature of the crime does not excuse the government's improper reliance on an anti-hacking statute to penalize conduct that has nothing to do with hacking. Not only do violations of TOS agreements fail to fit within the statutory framework of the CFAA, but the government attaching criminal liability to the breach of these civil contracts almost certainly violates constitutional protections of individual liberties.[272] Lori Drew should have to answer for her role in Megan Meier's death, but not in a way that sacrifices civil liberties.

A positive result could still ensue from Megan Meier's tragic death. If this unfortunate situation leads to the adoption of legislation specifically aimed at protecting young people from online harassment, or if the popularization of Megan's story raises awareness of the potential dangers of cyberbullying, perhaps the potential for future stories like Megan's will diminish. However, only time will tell.

## VI. POSTSCRIPT

### *Added September 10, 2009*

In the aftermath of Lori Drew's conviction for violating the CFAA,[273] many commentators have taken the position argued in this Comment that the conviction represents an improper usage of the CFAA and undermines the constitutional protections that Internet users deserve.[274] Apparently, the arguments against the conviction were sufficient to sway the opinion of the judge who presided over Lori Drew's case, the Honorable George Wu, U.S. District Judge for the Central District of California; in July, 2009,

---

272. *See supra* Part III.C.

273. *See* Tamura, *supra* note 11.

274. *See* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/archives/archive_2008_11_30-2008_12_06.shtml#1228319830 (Dec. 3, 2008, 09:57 PST) (describing how both The Los Angeles Times and USA Today both ran editorials condemning Lori Drew's conviction).

Judge Wu announced that he would overturn the conviction.[275] On August 28, 2009, nine months after a jury chose to convict Lori Drew,[276] the charges against her were dismissed.[277]

### *A. Judge Wu's Final Opinion*

Though the jury in Lori Drew's case entered their verdict on November 26, 2008,[278] the sentencing portion of the case was postponed for several months while Judge Wu considered a defense motion to dismiss the case allowed by Fed. R. Crim. P. 29(c).[279] Judge Wu observed that "a motion for judgment of acquittal under Fed. R. Crim. P. 29(c) may be made by a defendant seeking to challenge a conviction on the basis of the sufficiency of the evidence, . . . or on other grounds including ones involving issues of law for the court to decide."[280] Here, the ultimate question for Judge Wu to decide was whether or not an intentional violation of a website's TOS agreement implicated the CFAA, and if so whether the prosecution had enough evidence to establish that Lori Drew had in fact violated the statute.[281] Though Judge Wu did not address the evidentiary issues, he concluded that the Constitution's prohibition on vague criminal statutes precluded the use of the CFAA to punish breaches of TOS agreements.[282]

#### 1. The TOS and Authorized Access

Lori Drew was convicted under the provision of the CFAA that criminalizes unauthorized access to computers;[283] this interpretation, however, represented a great expansion of the concept of unauthorized

275. Posting of Eugene Volokh to The Volokh Conspiracy, http://volokh.com/archives/archive_2009_06_28-2009_07_04.shtml#1246566948 (July 2, 2009, 16:35 PST).

276. *See* Tamura, *supra* note 11 (stating that Lori Drew was convicted in November of 2008).

277. *See* Decision on Defendant's F.R. Crim. P. 29(c) Motion at 32, United States v. Drew, No. 08-00582 (C.D. Cal. Aug. 28, 2009) [hereinafter Drew Dismissal].

278. Tamura, *supra* note 11.

279. *See* Kim Zetter, *Judge Postpones Lori Drew Sentencing, Weighs Dismissal*, THREAT LEVEL, WIRED.COM, May 18, 2009, http://www.wired.com/threatlevel/2009/05/drew_sentenced/.

280. Drew Dismissal, *supra* note 276, at 10 (citing United States v. Freter, 31 F.3d 783, 785 (9th Cir. 1994), United States v. Pardue, 983 F.2d 843, 847 (8th Cir. 1993)).

281. Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/archives/archive_2009_05_10-2009_05_16.shtml#1242229570 (May 13, 2009, 11:55 PST).

282. Drew Dismissal, *supra* note 276, at 32.

283. *See* Drew Indictment, *supra* note 45, at 5.

access in terms of criminal liability.[284] Therefore, in his order dismissing Lori Drew's conviction, Judge Wu spends substantial time addressing the CFAA provision that criminalizes intentional access to a computer without (or in excess of) authorization and its relationship to TOS agreements.[285] "[T]he only basis for finding that Drew intentionally accessed MySpace's computers/servers without authorization and/or in excess of authorization was her . . . violations of the [MySpace TOS] by deliberately creating the false Josh Evans profile . . . ."[286] Thus, if breaching a website's TOS agreement were insufficient to satisfy the first element of the CFAA,[287] then the case against Lori Drew would have to be dismissed.[288] In order to resolve this question, Jude Wu explored both the nature of TOS agreements themselves and the undefined language of the CFAA.[289]

Websites specifically use TOS agreements for the purpose of defining what conduct will and will not be acceptable on the site.[290] Moreover, it makes sense that a website has the right to establish the extent and conditions under which members of the public will be allowed access to its services.[291] Thus, websites should be able to use TOS agreements to place limits on the level of access authorized to any given user.[292] However, issues may be raised as to the sufficiency of the notice and assent to the particular terms of an agreement, and other concerns might limit enforcement of certain restrictions.[293] Regardless, more than likely a website's TOS agreement will be able to define the terms under which it will allow access to its site.[294]

Taking the concept of websites using their TOS agreements to define authorized users to its logical conclusion, it appears that an individual who uses a site contrary to its TOS would be "exceeding authorized access" to a computer and therefore in violation of the CFAA. Simply put, the

---

284. *See supra* Part III.A.2.

285. Drew Dismissal, *supra* note 276, at 12–22.

286. *Id.* at 20.

287. *See* 18 U.S.C. § 1030(a)(2)(C) (2006) ("exceeding authorized access").

288. Drew Dismissal, *supra* note 276, at 20.

289. *See id.* at 20–22.

290. Lemley, *supra* note 50, at 459.

291. *See generally* United States v. Phillips, 477 F.3d 215, 219–21 (5th Cir. 2007); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 245–46 (S.D.N.Y. 2000); CompuServe Inc. v. Cyber Promotions,Inc., 962 F.Supp. 1015, 1023–24 (S.D. Ohio 1997).

292. Drew Dismissal, *supra* note 276, at 21.

293. *See id.*; *see also supra* Part III.B (discussing the circumstances under which it would be improper to enforce provisions of a website's TOS agreement).

294. Drew Dismissal, *supra* note 276, at 21.

language of the CFAA is very broad and unclear in its meaning,[295] thus it could be used to criminalize several forms of everyday conduct.[296] Contrary to the fact that many commentators[297] have argued for a more restrictive interpretation of the CFAA,[298] Judge Wu decided that "[t]here is nothing in the way that the undefined words 'authorization' and 'authorized' are used in the CFAA . . . which indicates that Congress intended for them to have specialized meanings."[299] Therefore, Judge Wu used the broad definition of the terms of CFAA and the principle that websites can define authorized access through their TOS to conclude that "an intentional breach of the [MySpace TOS] can potentially constitute accessing the MySpace computer/Server without authorization and/or in excess of authorization under the statute."[300] Clearly, Judge Wu determined that under the language of the CFAA, breaching a TOS agreement could subject a website's user to liability under the statute[301]—however the enforcement of that statute raises its own issues.

### 2. Void-for-Vagueness

Despite the fact that a website is free to determine the scope of access to its services, and the CFAA criminalizes the activity of an individual who accesses a computer without authorization, it is nonetheless unconstitutional to enforce the CFAA against a user of a website who does so in violation of the site's TOS.[302] This enforcement would be unconstitutional because of the void-for-vagueness doctrine.[303] As discussed in Part III.C.1 of this Comment above, the void-for-vagueness doctrine requires the government to define the activity criminalized with sufficient clarity so as to put the public on notice and prevent arbitrary enforcement.[304] Judge Wu concluded, just as this Comment had above,[305] that "basing a misdemeanor CFAA violation . . . upon the conscious

295. *See id.* at 12–20 (stepping through the key language of the CFAA provision under which Lori Drew was convicted, namely "intentional," "access," and "without authorization").

296. *See supra* Part III.A.

297. Including the Author of this Comment. *See supra* Part III.

298. *See* Drew Dismissal, *supra* note 276, at 16–19 (describing the standards for interpreting the language of the CFAA proffered by many scholars including Mark Lemley, Orin Kerr and Patricia Bellia).

299. *Id.* at 20–21.

300. *Id.* at 20.

301. *Id.*

302. *Id.* at 22–32.

303. *Id.*; *see* discussion *supra* Part III.C.1.

304. *See supra* Part III.C.1.

305. *See supra* Part III.C.1.

violation of a website's [TOS] runs afoul of the void-for-vagueness doctrine."[306] Judge Wu based his conclusion on both the "absence of minimal guidelines to govern law enforcement" and "actual notice deficiencies."[307]

a. Lack of Adequate Notice

As to the notice requirement of the void-for-vagueness doctrine, Judge Wu observed: "the question is whether individuals of 'common intelligence' are on notice that a breach of a [TOS] contract can become a crime under the CFAA."[308] Ultimately, he answered this question in the negative because of four reasons: the language of the CFAA, the lack of definiteness as to what terms within a given TOS actually preclude authorized access, the discretion vested in websites to determine TOS violations, and the application of contractual terms to deciding criminal liability.[309]

First, Judge Wu inquired as to "whether the statute, as it is written, provides sufficient notice"[310] because "the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has 'criminalized breaches of contract' in the context of website [TOS agreements]."[311] The court observed that breaches of contract are not normally the basis for criminal prosecution, thus an ordinary individual would not anticipate criminal penalties for violating a website's TOS agreement.[312] Moreover, Judge Wu noted that "this would especially be the case where the services provided by MySpace are in essence offered at no cost to the users and, hence, there is no specter of the users 'defrauding' MySpace in any monetary sense."[313] The ordinary Internet user could not expect to be held criminally liable for breaching a TOS contract, and would thus not have the requisite notice if the CFAA penalized such conduct.[314]

Second, Judge Wu observed that if TOS agreements could define authorization for purposes of CFAA liability, then the statute "would be

306. Drew Dismissal, *supra* note 276, at 25.

307. *Id.*

308. *Id.*

309. *Id.* at 25–28.

310. *Id.* at 25.

311. *Id.*

312. Drew Dismissal, *supra* note 276, at 25–26; *see also* discussion *supra* Part III.B.1 (arguing that not only would criminal liability for breach of contract be inappropriate, but the contracts themselves might be civilly unenforceable as well).

313. Drew Dismissal, *supra* note 276, at 26.

314. *See id.*

unacceptably vague because it is unclear whether any or all violations of the [TOS] will render the access unauthorized, or whether only certain ones will."[315] As it is highly unlikely for a website's TOS to outline which specific violations make further access unauthorized, as apposed to which violations may have different penalties, the average user would not be on notice as to when their authorization is terminated and criminal penalties have arisen under the CFAA.[316] Though this issue may be solved by attaching criminal liability to any violation of a website's TOS, this strategy would raise another issue:

> If *any* violation of *any* [TOS] is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.[317]

Because users are unaware of which breaches will subject them to criminal liability, and which will not, the notice requirement of the void-for-vagueness doctrine has not been met.[318]

Third, the court found that by vesting the power to define which conduct carries criminal liability in a website owner, further vagueness problems will arise.[319] The description of a particular term in the TOS may be vague in and of itself, such as "unfair" or "sexually suggestive,"[320] or the scope of a provision could be decided "*ad hoc* and/or pursuant to undelineated standards."[321] This lack of clarity fails to provide the notice required for attaching criminal liability to these agreements, and thus using the CFAA to punish the breach of a TOS agreement cannot withstand the scrutiny of the void-for-vagueness doctrine.[322] Moreover, Judge Wu stated that some TOS agreements may allow for unilateral amendment or modification of their terms without notice to users—further leading to a lack of notice as to prohibited conduct.[323]

Fourth, Judge Wu noted that because TOS agreements are "essentially

---

315. *Id.*

316. *See id.*

317. *Id.* at 26–27 (emphasis in original).

318. *See id.*

319. Drew Dismissal, *supra* note 276, at 27.

320. *Id.* (citing specific examples of unclear terms from the MySpace TOS agreement).

321. *Id.* (illustrating how the MySpace TOS "provides that what constitutes 'prohibited content' on the website is determined 'in the sole discretion of MySpace.com'").

322. *See id.*

323. *Id.*

a contractual means for setting the scope of authorized access,"[324] the application of specific terms or contract law in general may lead to improper vagueness.[325] For example, the MySpace TOS requires that a dispute arising under the agreement be settled through arbitration; this could mean that criminal liability may not be settled until after the completion of the arbitration.[326] Moreover, the general principles of the relevant contract law may set out remedies for nonperformance of a TOS agreement other than termination of the contract.[327] The contract itself could also specify particular remedies.[328] Therefore, a breach of the agreement may not in all circumstances lead to the user accessing the site outside the scope of authorization—this creates a situation of impermissible uncertainty when criminal liability is attached to the agreement through the CFAA.[329]

b. Insufficient Standards for Enforcement

In addition to the insufficient notice provided to average Internet users, Judge Wu also recognized that a CFAA that criminalizes breaches of TOS agreements would fail to provide adequate guidelines to govern enforcement of the law.[330] The court corroborated the argument proffered by this Comment when it stated: "Treating a violation of a website's [TOS], without more, to be sufficient to constitute 'intentionally access[ing] a computer without authorization or exceed[ing] authorized access' would result in transforming [the CFAA] into an overwhelmingly overbroad enactment that would convert . . . innocent Internet users into . . . criminals."[331] Given the potentially broad scope of a CFAA that criminalized violations of TOS agreements, Judge Wu "question[ed] as to whether Congress has 'establish[ed] minimal guidelines to govern law enforcement.'"[332] Because he felt that the required guidelines were not present, Judge Wu determined that law enforcement would have far too

---

324. *Id.*

325. Drew Dismissal, *supra* note 276, at 27.

326. *See id.* at 27–28.

327. *See id.* at 28 (describing how under California law the remedies of breach of contract include damages, declaratory relief, rescission and restitution, specific performance, and injunction among others).

328. *Id.*

329. *See id.*; *supra* Part III.C.1.

330. Drew Dismissal, *supra* note 276, at 29.

331. *Id.*; *see also supra* Part III.C.1.

332. Drew Dismissal, *supra* note 276, at 29 (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)).

much discretion and consequently the statute would be unconstitutionally vague.[333]

In an effort to overcome the challenge of unconstitutional vagueness, the government suggested a scienter requirement existed in the CFAA provision that punished "intentional" access of a computer without authorization.[334] In the government's view, because conviction under the CFAA requires proving malicious intent on behalf of the perpetrator, the statute is not vague and provides sufficient guidelines to direct law enforcement as to when to charge individuals with violation.[335] The argument is essentially that law enforcement will only charge individuals whom they can prove had the requisite intent, therefore the statute is precise as to which individuals deserve prosecution, and which do not.[336] Nonetheless, Judge Wu rejected this interpretation of the statute: "The only scienter element in section 1030(a)(2)(C) is the requirement that the person must 'intentionally' access a computer without authorization or 'intentionally' exceed authorized access."[337] Moreover, the government's position that "the 'intentional' requirement is met simply by a conscious violation of a website's [TOS] . . . basically eliminates any limiting and/or guiding effect of the scienter element."[338] In an attempt to broaden the CFAA to prosecute Lori Drew, the government in effect destroyed any argument that it could have made in relation to the statute providing guidance to law enforcement.[339]

Judge Wu also recognized that because any breach of a TOS agreement could garner prosecution, the statute would provide the government with free reign to prosecute some offenders and not others.[340] "[I]f every such breach does qualify [as a CFAA violation], then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution."[341] Therefore, a large cross-section of conduct prohibited in a TOS agreement[342] could be prosecuted under the CFAA, from posting child-pornography to uploading pictures of friends without

333. *Id.* at 29–31.

334. *Id.* at 30.

335. *See id.*

336. *See id.*

337. *Id.* at 31.

338. Drew Dismissal, *supra* note 276, at 31.

339. *See id.*

340. *Id.* at 31–32.

341. *Id.* at 31.

342. *See supra* Part III.B (discussing certain types of conduct prohibited in various TOS agreements).

permission.[343] "Given the 'standardless sweep' that results, federal law enforcement entities would be improperly free 'to pursue their personal predilictions.'"[344] The vesting of complete discretion in law enforcement whether or not to prosecute is precisely the type of outcome the void-for-vagueness doctrine aims to prevent[345]—this combined with the lack of notice to Internet users as to what conduct would actually be treated as criminal caused the court to grant the defense Fed. R. Crim. P. 29(c) motion and dismiss the charges against Lori Drew.[346]

### *B. Where Do We Go From Here?*

More than three years after Megan Meier's death[347] and even now that Lori Drew's conviction has been overturned, the state of the law as it relates to cyberbullying is no clearer than it was before.[348] Though one court has decided it would be improper to extend the CFAA to punish violations of website TOS agreements, all federal law enforcement offices are not bound by the ruling.[349] Moreover, because Judge Wu dismissed this case because a lack of required definiteness, the government could overcome this hurdle by changing the language of the CFAA or adopting provisions for standardized TOS verbiage that would be sufficient to guide law enforcement and put citizens on notice.

It is clear from the saga of Lori Drew that serious limitations exist in the current state of laws that could be used to protect children from and punish cyberbullying.[350] Additionally, the scope of the relationship between TOS agreements and the CFAA can extend to other situations as well.[351] In circumstances where a broad reading of the CFAA can lead to

---

343. Drew Dismissal, *supra* note 276, at 31

344. *Id.* at 31–32 (quoting Kolender v. Lawson, 461 U.S. 352, 358 (1983)).

345. *Id.* at 32.

346. *Id.*

347. *See* Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, THREAT LEVEL, WIRED.COM, July 2, 2009, http://www.wired.com/threatlevel/2009/07/drew_court/.

348. *See* Posting of Eugene Volokh to The Volokh Conspiracy, http://volokh.com/posts/1241740320.shtml (May 7, 2009, 19:52 PST) (discussing the problems with proposed legislation aimed at criminalizing cyberbullying).

349. As this was merely the opinion of a district court, the decision is not binding precedent on any courts in other jurisdictions.

350. *See supra* Part IV (discussing the ineffectiveness of current laws to protect children from harassment online).

351. *See* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/archives/archive_2009_02_22-2009_02_28.shtml#1235510297 (Feb. 25, 2009, 01:03 PST) (discussing United States v. Nosal, a federal case in California using the a broad reading of the CFAA to bring criminal charges on a former employee of a company who accessed

criminal liability for noncompliance with vague contractual terms, the Judge Wu's holding in this case may be whittled away over time. Eventually, the state of the law could be right back to where it was before Judge Wu dismissed Lori Drew's case, and more unknowing website users could be haled in front of federal criminal courts.

*Ryan Patrick Murray* *

computers outside of the scope of the authorization granted to him in an employment contract).

* J.D. Candidate, Loyola Law School, Los Angeles, 2010; B.S., California Polytechnic State University, San Luis Obispo, 2007. Thank you to Professor Charlotte Goldberg for her comments and revisions, Professor Christopher Peters for his tips on Constitutional Law, and Professor Daniel Selmi for his inspiration and support. Additionally I would like to thank the members of the Loyola of Los Angeles Entertainment Law Review, especially Gary Wax and Mark D. Robertson. I give never-ending gratitude to my parents for always believing in me, and to Meghan for more than you know.

,