Mercer Law Review

Volume 63
Number 2 *Articles Edition*

Article 6

3-2012

"Undercover Teachers" Beware: How that Fake Profile on Facebook Could Land You in the Pokey

Paul F. ("Pete") Wellborn III

"Undercover Teachers" Beware: How that Fake Profile on Facebook Could Land You in the Pokey

by Paul F. ("Pete") Wellborn III*

I. INTRODUCTION

A. *"Undercover Teachers" on the Internet*

Depending upon whom one asks, it is either: (1) the dirty little secret of American educators; (2) an effective tool for safeguarding the well-being of students and ensuring their compliance with both governing law and school policy; or (3) an overblown myth that rarely, if ever, actually occurs. "It" is the establishment and use by teachers and academic administrators of "undercover profiles" on social networking websites like Facebook[1] or MySpace,[2] pursuant to which the educator poses as a peer of the educator's teenage or college age students. When the educator's fictitious persona is "friended," or otherwise added, by a given student to that student's network of online insiders, the educator has an unadulterated view into the life of the monitored student. Due in large part to the false sense of security that arises from the student's ability to define and limit his circle of digital friends, the student's communications on the social networking website are often unguarded and unfiltered. It is not unusual for statements and pictures posted by a

* Founding and Managing Member, Wellborn, Wallace & Woodard, LLC, Atlanta, Georgia. Georgia Institute of Technology (B.S., 1986); Mercer University, Walter F. George School of Law (J.D., 1989). Member, State Bar of Georgia. Any opinions or viewpoints expressed in this Article represent those of the Author only.

1. FACEBOOK, http://www.facebook.com (last visited Oct. 11, 2011).
2. MYSPACE, http://www.myspace.com (last visited Oct. 11, 2011).

teenage or young adult user to include irrefutable evidence of conduct that violates his school's code of student conduct or, in some cases, constitutes an outright criminal violation.

B. *Social Networking Websites*

A social networking website allows its users to create personal profiles or pages and interact with other website members. This category of websites includes Internet destinations like Facebook, MySpace, Twitter,[3] and YouTube,[4] to name a few. Typically, a social networking website includes content that is available to any visitor to the website and content that is available only to members.[5] A social networking website member typically has the ability to designate the various portions of his personal profile, page, or other personal section of the website as public (meaning that it is available to all website visitors) or private (meaning that it is available only to those website members specially approved by the subject member).[6] Although the account set-up process for most social networking websites is free for the prospective member, the member must nonetheless accept and comply with the governing website user agreement.[7] Most social networking websites require, among other conditions of becoming a member (that is, of becoming an "authorized user" of the website), that the registering member provide accurate information during the sign-up process.[8]

The leading social networking website and, indeed, the most visited website in the world is Facebook.[9] There are more than 800 million unique Facebook users worldwide, and on any given day, over 400 million unique users access the Facebook website.[10] A substantial number of American Facebook users–roughly 65 million–are between the ages of thirteen and twenty-five years old.[11] For good or bad, the daily

---

3. TWITTER, http://twitter.com (last visited Oct. 11, 2011).

4. YOUTUBE, http://www.youtube.com (last visited Oct. 11, 2011).

5. *See, e.g.*, MYSPACE, *supra* note 2.

6. *See, e.g.*, *Sharing and Finding You on Facebook*, FACEBOOK, http://www.facebook.com/about/privacy/your-info-on-fb#control (last visited Oct. 24, 2011).

7. *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php (last visited Nov. 25, 2011).

8. *See, e.g.*, *id.* § 4.

9. Daniel Ionescu, *Google Names Facebook Most Visited Site*, PCWORLD.COM (May 28, 2010, 6:29 AM), http://www.pcworld.com/article/197431/google_names_facebook_most_visited_site.html.

10. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 11, 2011).

11. Ken Burbary, *Facebook Demographics Revisited–2011 Statistics*, WEB BUSINESS BY KEN BURBARY (Mar. 7, 2011), http://www.kenburbary.com/2011/03/facebook-demographicsrevisited-2011-statistics-2/.

use of social networking websites has become a ubiquitous part of student life for middle school, high school, and college students across the United States.

C. Crime and Punishment: Incriminating Evidence on Social Networking Websites

1. Witness for the Prosecution? An Alleged Wrongdoer's Own Social Networking Website Pages. Although details as to *how* the incriminating evidence is discovered are often murky, media reports of students hoisted with their own social networking website petards are appearing with increasing frequency. In Pearl, Mississippi, a high school student was removed from the cheerleading squad after her coach read e-mails sent via the student's Facebook account, to which the cheerleading coach required access pursuant to the squad policy.[12] At a high school in Fairfax, Virginia, campus police monitor student social networking accounts to glean information on the students' gang membership and criminal activities.[13] In Wisconsin, at the University of Madison-Lacrosse, campus police charged a number of underage drinkers on the basis of social networking website photographs showing the students' illegal use of alcohol.[14] The authorities there were able to access the incriminating pictures on the basis of an undercover social networking website-based investigation.[15] The dean of St. John's College in Cambridge, England, reportedly posed as "Pedro Amigo" to investigate an offensive comment made by a student in a social networking website group called "St John's Has Banned Us Taking Wine to Hall."[16] After a student recognized the e-mail address associated with the Pedro Amigo account as actually belonging to the dean, the dean made a hasty and embarrassing retreat and deleted the account.[17]

In Tennessee, a mother's Facebook posting about the mess her two football-playing sons made of their rooms each weekend led to the discovery that her sons did not satisfy the district residency requirement

---

12. Marquita Brown, *Pearl District Sued Over Alleged Facebook Incident*, CLARION-LEDGER (Jackson, Miss.), July 29, 2009.

13. Michael Birnbaum, *Campus Officers Cruise Facebook, MySpace for Clues to School-Related Crimes*, WASH. POST, Apr. 6, 2009, *available at* 2009 WLNR 6425763.

14. Bryan McKenzie, Column, DAILY PROGRESS (Charlottesville, Va.), Aug. 6, 2011, *available at* 2011 WLNR 15586553.

15. *Id.*

16. Caroline Gammell et al., *Cambridge Dean Joins Facebook to Monitor Students*, DAILY TELEGRAPH (United Kingdom), Oct. 29, 2008, *available at* 2008 WLNR 20594078.

17. *Id.*

for the high school they attended.[18] As a result, the two boys were declared ineligible and three of their school's football victories were vacated.[19] Three students at Chapel Hill Middle School in Atlanta, Georgia, were suspended for violation of school policy in relation to Facebook postings in which they referred to a teacher they disliked as a mentally-ill rapist and pedophile.[20] Students at Jonathan Dayton High School in Springfield, New Jersey, were punished for Facebook comments construed by school officials as being racist.[21] In Lake County, Illinois, school district authorities unanimously implemented a policy requiring that all students participating in extracurricular activities, including sports, fine arts, and other clubs, sign a pledge acknowledging that any online evidence of "illegal or inappropriate" behavior, including postings and pictures on social networking websites, would be grounds for discipline.[22] A sports media company recently unveiled a computer program called "YouDiligence," designed to monitor student-athletes' social networking website accounts for incriminating or inappropriate posts.[23] Finally, in Texas, a Burleson High School eleventh grader was suspended for allegedly profane content on her MySpace account.[24] A complete account of all instances of social network-related discipline meted out at high schools and colleges would fill volumes. As social networking website use by high school and college students continues to skyrocket, these incidents will no doubt continue to occur with ever-increasing frequency.

2. Student/Parent Reactions and Educator Liability. School-related discipline arising from comments or pictures appearing on a

---

18. *Tenn. Mom's Facebook Post Costs Sons' Football Team 3 Victories,* CITIZENS TIMES (Asheville, N.C.), Sept. 27, 2011, *available at* 2011 WLNR 19828384.

19. *Id.*

20. Ty Tagami, *Student: Principal Forced Deletion of Facebook Posts*, ATLANTA J. CONST. (Mar. 3, 2011, 5:53 PM), http://www.ajc.com/news/student-principal-forced-deletion-858326.html; *see also* Ty Tagami, *No Expulsion For Kids' Facebook Posts About Teacher*, ATLANTA J. CONST. (Mar. 10, 2011, 5:09 PM), http://www.ajc.com/news/no-expulsion-for-kids-867892.html.

21. Brett Biebelberg, *School Officials Crack Down on Student-Created Facebook Group*, SPRINGFIELD PATCH (Mar. 1, 2010), http://springfield.patch.com/articles/school-officials-crack-down-on-student-created-facebook-group.

22. *Changes Affect Student Posting Online*, CHICAGO TRIB., May 23, 2006, *available at* 2006 WLNR 8890519 (internal quotation marks omitted).

23. Dave Copeland, *Keep it Clean Kids, Software's Watching*, BOSTON GLOBE, Jan. 19, 2009, *available at* 2009 WLNR 1034021.

24. Shirley Jinkins, *Burleson School Officials Remove Girl's Demerits, Drill Team Suspension*, FORT WORTH STAR-TELEGRAM, Aug. 12, 2009, *available at* 2009 WLNR 15607259.

student's social networking website account is often met with opposition and outrage by the involved students, their parents, their peers, and, in extreme circumstances, results in legal action on behalf of the disciplined students.[25] Almost without exception, media accounts of these incidents include comments from irate parents and students who believe that the school overstepped its bounds, overreacted, violated the student's right to freedom of speech, or otherwise acted inappropriately.[26] An educator whose investigation includes the use of a social networking website account through which the educator has posed as a peer of the disciplined student, however, could face a much graver consequence–criminal prosecution and jail time. A colorable argument exists that an educator's creation and use of such accounts constitutes a violation of state and federal criminal law, subjecting the involved educator–in a worst-case scenario–to fines or jail time, or both.[27]

The basis for the educator's potential criminal culpability arises from the right of a social networking website owner to define the mandatory rules with which all users of its website must comply.[28] The terms of service that set forth the agreement between a social networking website and a user–to which the user must expressly assent as a condition of account set-up and website use–typically require, among other provisions, that the user provide true and correct information during the account creation process.[29] By so responding, by otherwise complying

---

25. *See, e.g.*, Brown, *supra* note 12 (lawsuit for $50 million filed by parents of girl suspended from cheerleading squad for profanity in a Facebook posting); Tagami, *No Expulsion For Kids' Facebook Posts About Teacher*, *supra* note 20 (allegations that school violated the involved student's privacy); Wendy N. Davis, *No More Pencils, No More Facebooks*, 95 A.B.A. J. 18 (July 2009) (student who was disciplined for a parody MySpace he created of his school principal successfully sued the school for violation of his First Amendment rights); *see generally* Christi Cassel, *Keep Out of MySpace! Protecting Students from Unconstitutional Suspensions and Expulsions*, 49 WM. & MARY L. REV. 643 (2007).

26. *See* sources cited *supra* note 25.

27. *See* discussion *infra* Part II.A. Although beyond the scope of this Article, the theories underlying criminal culpability for the creation and use of bogus website profiles by educators arguably apply with equal force to the use of "undercover accounts" by private investigators and the creation of parody accounts by students and others that purport to belong to the parody subject. *See, e.g.*, Shirin Chahal, *Balancing the Scales of Justice: Undercover Investigations on Social Networking Sites*, 9 J. TELECOMM. & HIGH TECH. L. 285 (2011); Kevin P. Brady, *Student-Created Fake Online Profiles Using Social Networking Websites: Protected Online Speech Parodies or Defamation?*, 244 ED. L. REV. 907 (2009); Bradley Kay, *Extending Tort Liability to Creators of Fake Profiles on Social Networking Websites*, 10 CHI.-KENT J. INTELL. PROP. 1 (2010).

28. *See* discussion *infra* Part II.A.

29. As of October 2011, MySpace's "Terms of Use Agreement" requires that the user "represent and warrant that (a) all registration information . . . submit[ted] is truthful and accurate; [and that] (b) [the user] will maintain the accuracy of such information . . . ."

with the governing provisions of the website user agreement, and by promising continued compliance, the new member becomes an authorized user of the social networking website.[30] Conversely, if a new member gains access to the website via the intentional provision of false information or otherwise breaches the governing terms of the website user agreement, that member's access to and use of the website is not authorized.[31] In the latter instance, the resulting impermissible access to and use of the website arguably gives rise to a number of viable criminal charges against the unauthorized user. These criminal charges range from state laws prohibiting criminal trespass to federal laws–including the Computer Fraud and Abuse Act (CFAA)[32]–that generally prohibit unauthorized computer access.

D. Purpose of this Article

This Article does *not* advocate the prosecution of educators who establish and use social networking website accounts in the manner described above, nor does it offer any opinion regarding the propriety or ethics of such investigations. This Article also does not address the constitutionality of any discipline or punishment arising from the students' social networking website comments or postings. Rather, the Author's primary intent–indeed, his sole intent–is that this Article serve as a warning of the worst-case consequences to any educators who, unaware of the grave legal implications, might otherwise continue to use social networking website accounts in the undercover manner described above to monitor or investigate their students. This Article examines the relevant legal theories and surveys the issues and authorities pertinent to the prosecution and defense of any such charges.

Terms of Use Agreement, MYSPACE.COM http://www.myspace.com/Help/Terms, § 1 (last visited Oct. 11, 2011). The Facebook "Statement of Rights and Responsibilities" prohibits Facebook users from "provid[ing] any false personal information on Facebook, or creat[ing] an account for anyone other than [themselves] without permission." FACEBOOK, *supra* note 7, § 4.

30. *See, e.g.*, FACEBOOK, *supra* note 7, § 4.

31. *See, e.g., id.*

32. 18 U.S.C. § 1030 (2006 & Supp. IV 2010). The CFAA was enacted in 1984 as an anti-hacking statute. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA), Pub. L. No. 98-473, § 2102, 98 Stat. 1837, 2190 (1984) (codified as amended at 18 U.S.C. § 1030). It has been amended numerous times, with each amendment broadening the statute's scope. *See* 18 U.S.C. § 1030. Subject to certain additional conditions, the CFAA prohibits unauthorized access to a computer and access to a computer in excess of the access actually granted. 18 U.S.C. § 1030(a).

II. THE LAW

A. *Criminal Culpability for the Establishment and Use of Undercover Accounts*

The analysis of a website user's liability for unauthorized access to the website, or access in excess of the authorization actually given, begins with acknowledgement of a computer owner's personal property interest in that computer. Courts have repeatedly ruled that all rights in and to the computer–including the right to access and use that computer from a remote location or via the Internet–lie with the computer owner.[33] The owner has the right to determine both who is allowed to access or use the computer *and* the scope of any limitations or rules governing that access or use.[34] Accordingly, not unlike that same owner's house or car, the owner's computer can be trespassed upon, unlawfully accessed, or otherwise misused by a third party in such manner as to give rise to viable criminal charges, civil causes of action, or both. It is important to note, however, that authorization to access or use a computer is not an "all or nothing" proposition. Even if a person is authorized to access or use some element or part of a computer or computer network, access or use of non-authorized parts of that same network may nonetheless give rise to a criminal charge or cause of action.[35]

The body of authority pertaining to computer access-related liability has grown in leaps and bounds over the past fifteen years, as the Internet has gone from an academic curiosity to a ubiquitous part of daily life for roughly eighty percent of United States households.[36]

---

33. *See, e.g.*, Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C98-20064 JW, 1998 WL 388389, at *6 (N.D. Cal. Apr. 16, 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450-51 (E.D. Va. 1998); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027 (S.D. Ohio 1997).

34. *See* sources cited *supra* note 33.

35. *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000). In *Shurgard*, the court found that the plaintiff stated a justiciable claim under the Computer Fraud and Abuse Act in relation to the defendant employees, who, in excess of the actual authorization they had in relation to their employer's computer, accessed the plaintiff's proprietary information and sent it to a competitor while still employed by the plaintiff. *Id.* at 1123.

36. According to the U.S. Census Bureau, as of October 2009, nearly eighty percent of households in the United States included one or more people who accessed or otherwise used the Internet. U.S. CENSUS BUREAU, *Internet Use in the United States: October 2009*, http://www.census.gov/hhes/computer/publications/2009.html (follow "Table 1. Reported

Many of these authorities address the CFAA,[37] computer trespass, and similar causes of action in the context of unauthorized use by senders of unsolicited commercial e-mail (spam) of private computer networks belonging to various Internet service providers (ISPs), all of whose policies forbade such use. Virtually without exception, courts considering spam-related cases have ruled that the plaintiff ISP (the owner of the computer network at issue) has the right to establish the rules governing third-party use of the ISP's computers, and that third-parties–the defendant spammers–who access or use the network in derogation of those rules unlawfully trespass upon the network and violate, among other prohibitions, the CFAA.

For example, in *Hotmail Corp. v. Van$ Money Pie Inc.*,[38] the United States District Court for the Northern District of California ruled that the defendant spammers' access to and use of the plaintiff ISP's mail servers in violation of Hotmail's terms of service constituted, among other causes of action, violation of the CFAA and trespass upon Hotmail's computer network.[39] Likewise, the United States District Court for the Eastern District of Virginia in *America Online, Inc. v. IMS*,[40] granted summary judgment to the plaintiff ISP on, among other counts, its cause of action for trespass to chattels against the defendant spammer.[41] Like the terms of service agreement in *Hotmail*,[42] America Online's (AOL's) terms of service prohibited the sending of spam through the AOL network, thereby rendering the spammers' use of the AOL network unauthorized.[43] AOL won another anti-spam victory in *America Online, Inc. v. LCGM, Inc.*,[44] a case in which the court found that the defendant spammers trespassed upon AOL's computer network and violated the CFAA in relation to the spammers' unauthorized use of AOL's computer network to send spam.[45] Finally, the United States District Court for the Southern District of Ohio in *CompuServe, Inc. v. Cyber Promotions, Inc.*,[46] granted a preliminary injunction against the defendant spammers in favor of the plaintiff ISP, rejecting the defen-

---

Internet Usage for Households" hyperlink) (last visited Oct. 24, 2011).

37. 18 U.S.C. § 1030 (2006 & Supp. IV 2010).
38. No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 (N.D. Cal. 1998).
39. *Id.* at *6-7.
40. 24 F. Supp. 2d 548 (E.D. Va. 1998).
41. *Id.* at 551.
42. *See Hotmail*, 1998 WL 388389, at *1-2.
43. *See Am. Online, Inc.*, 24 F. Supp. 2d at 550.
44. 46 F. Supp. 2d 444 (E.D. Va. 1998).
45. *Id.* at 450-51.
46. 962 F. Supp. 1015 (S.D. Ohio 1997).

dants' First Amendment[47] defense and finding that the defendants had trespassed upon AOL's computer network.[48]

Because a website is, in fact, a collection of data and information housed on a server (a type of computer) and available via the Internet, the website and the server or servers upon which it resides are protected in exactly the same manner as were the e-mail networks in the spam-related cases cited immediately above. For example, in *Multiven, Inc. v. Cisco Systems, Inc.*,[49] the Northern District of California found that the plaintiff's former employee was liable to the plaintiff under the CFAA for his unauthorized access to the plaintiff's website.[50] Likewise, the Southern District of Ohio in *Jedson Engineering, Inc. v. Spirit Construction Services, Inc.*,[51] ruled that the plaintiff did indeed present a colorable cause of action in relation to its claim of unauthorized access to its website by the defendant.[52] In *Snap-On Business Solutions, Inc. v. O'Neil & Associates, Inc.*,[53] the United States District Court for the Northern District of Ohio found that, in relation to the defendant's unauthorized access to and use of the plaintiff's website, the plaintiff's computer trespass claim and its CFAA claim presented justiciable issues of fact.[54] Finally, in *Craigslist, Inc. v. Naturemarket, Inc.*,[55] the Northern District of California found that the defendant violated the CFAA by marketing software that allowed users to make automated postings to the website, to scrape the website to gather user e-mail addresses, and to circumvent security measures built into the website, all in violation of the website's terms of service.[56]

As these cases demonstrate, courts generally are not reluctant–*in a civil setting*–to enforce a website owner's terms of service against website users who violate those terms (that is, against "unauthorized users"). The same is not true, however, in a criminal setting. As explained in detail below at Part II.B, the primary obstacle to the imposition of criminal culpability for unauthorized or excessive access to a website arises from a perception–or misperception, depending upon one's point of view–that governmental enforcement of owner-drafted terms of service would represent an impermissible delegation of law-making authority to

47. U.S. CONST. amend. I.
48. *CompuServe, Inc.*, 962 F. Supp. at 1026-28.
49. 725 F. Supp. 2d 887 (N.D. Cal. 2010).
50. *Id.* at 895.
51. 720 F. Supp. 2d 904 (S.D. Ohio 2010).
52. *Id.* at 926-27.
53. 708 F. Supp. 2d 669 (N.D. Ohio 2010).
54. *Id.* at 678, 680.
55. 694 F. Supp. 2d 1039 (N.D. Cal. 2010).
56. *Id.* at 1048-50, 1056-57.

the website owner. This judicial concern, however, is arguably misplaced because virtually *all* criminal laws that pertain in any way to violation by one person of another's personal or real property rights include some element of owner-defined authorization or consent.[57]

For example, section 16-7-21 of the Official Code of Georgia Annotated (O.C.G.A.)[58] defines Georgia's law of criminal trespass in terms of property damage, interference, or entry "without consent" or "without authority" of the owner.[59] Georgia's Computer Crimes statute[60] defines Georgia's prohibition against computer theft, computer trespass, computer invasion of privacy, and computer password disclosure in terms of further-defined, prohibited acts undertaken "without authority."[61] O.C.G.A. § 16-7-23[62] defines the offense of "criminal damage to property in the second degree" in terms of damage to the property of another "without his consent."[63] Likewise, Georgia's burglary statute[64] requires, among other wrongful acts, the wrongdoer's entry or continuing presence within a dwelling "without authority."[65]

In relation to each of these criminal statutes, the prosecution of a defendant *necessarily* includes examination and application of any consent, limited authority, or other such license or permission that the complaining party may have given to the defendant. Conceptually, the idea of a computer or website owner defining the scope of authorities that ultimately determine who is and is not an "authorized user" is indistinct from a real property owner defining the scope of the licenses that ultimately determine who is and is not a trespasser. Accordingly, across the board application of a prohibition against the prosecution of any criminal charges that rely in whole or in part upon the scope of the license granted to third parties by a computer owner (that is, upon "private rules") would gut the CFAA in its entirety. The rights of use and access, or the lack thereof, in relation to *any* given computer, network, or website are necessarily defined by the owner and, accordingly, are at issue in every CFAA-related case.

---

57. Georgia law is used herein to illustrate the permeation of owner-defined rights and licenses in virtually all statutes that protect the owner's property interests. The law of Georgia in this area is generally unremarkable and is substantially similar to corresponding protections enacted in other states.

58. O.C.G.A. § 16-7-21 (2011).

59. *Id.* § 16-7-21(a)-(b).

60. *Id.* § 16-9-93 (2011).

61. *Id.*

62. *Id.* § 16-7-23 (2011).

63. *Id.* § 16-7-23(a)(1).

64. *Id.* § 16-7-1 (2011).

65. *Id.* § 16-7-1(a).

B. No Criminal Culpability for the Establishment and Use of Undercover Accounts

The argument against criminal culpability for the establishment and use of undercover social networking website accounts was set forth in expansive detail in an opinion arising from a polarizing matter that dominated headlines across the country–the prosecution of Lori Drew (Drew) in relation to the tragic death of thirteen-year-old Megan Meier (Megan).[66] In September 2006, Drew was a forty-seven-year-old female living in O'Fallon, Missouri.[67] Drew's daughter Sarah was the former classmate of their neighbor Megan.[68] The once-close friendship between Sarah and Megan had, for whatever reason, chilled when Megan changed schools.[69] On or about September 20, 2006, Drew and others (the conspirators) accessed the MySpace social networking site and set up a bogus profile for a fictitious sixteen-year-old boy they named "Josh Evans."[70] Drew posted a picture purporting to be Josh that was, in fact, a picture of an uninvolved teenage boy who had no knowledge of the use of his likeness. Posing as Josh, Drew and the conspirators struck up an online flirtation with Megan that soon blossomed into a digital romance via the exchange of many messages via MySpace.[71] On or about October 15, 2006, the messages from Josh suddenly turned mean and insulting, culminating with an October 16, 2006 message in which Josh told Megan that "the world would be a better place without her in it."[72] Immediately thereafter, apparently inconsolable over Josh's comments, Megan committed suicide by hanging herself with a belt.[73] Upon learning of Megan's suicide, Drew deleted the "Josh Evans" MySpace account and directed a teenage neighbor with knowledge of the scheme to "keep her mouth shut."[74]

After Drew's plot was uncovered, the matter ignited a media firestorm. Drew was charged with, among other crimes, violation of the CFAA under the theory that her access to and use of the MySpace website was unauthorized because of her intentional violation of the MySpace terms

---

66. *See* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

67. *Id.* at 452; Christopher Maag, *A Hoax Turned Fatal Draws Anger But No Charges*, N.Y. TIMES, Nov. 28, 2007, http://www.nytimes.com/2007/11/28/us/28hoax.html.

68. *Drew*, 259 F.R.D. at 452.

69. Maag, *supra* note 67.

70. *Drew*, 259 F.R.D. at 452.

71. *Id.*

72. *Id.* (internal quotation marks omitted); Maag, *supra* note 67.

73. *Drew*, 259 F.R.D. at 452; Maag, *supra* note 67.

74. Maag, *supra* note 67.

and conditions.[75] Ultimately, Drew was found guilty of "accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor."[76] On appeal, the United States District Court for the Central District of California deemed the central appellate question to be "whether a computer user's intentional violation of one or more provisions in an Internet website's terms of service (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C)."[77] Forecasting its ultimate holding, the court noted that "[i]f the answer to that question is 'yes,' then seemingly, any and every conscious violation of that website's terms of service will constitute a CFAA misdemeanor."[78]

The court found that the second and third elements of 18 U.S.C. § 1030(a)(2)(C)[79]–the obtaining of information from a protected computer and the involvement of an interstate or foreign communication–are necessarily present anytime an Internet user contacts, communicates with, or accesses a website.[80] This left, as the pivotal issue, the first element of § 1030(a)(2(C)–whether there occurred the intentional access of a computer without authorization or in excess of the authorization actually granted.[81] In the context of Drew's alleged violations, the court reiterated as the "primary question" the issue of "whether any conscious violation of an Internet website's terms of service" would necessarily constitute access "without authorization or exceeding authorization."[82]

The court first explained that, in a civil (as opposed to criminal) setting, "most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization," citing a long list of supporting cases.[83] The court reiterated that

---

75. *Drew*, 259 F.R.D. at 451.

76. *Id.* at 453 (internal quotation marks omitted).

77. *Id.* at 457.

78. *Id.*

79. 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. IV 2010).

80. *Drew*, 259 F.R.D. at 457-58. The second element is no longer a requirement as the 2008 amendment to the CFAA struck that provision. *Id.* at 458 n.14; *see also* Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 203, 122 Stat. 3560, 3561 (codified at 18 U.S.C. § 1030).

81. *Drew*, 259 F.R.D. at 458.

82. *Id.* (internal quotation marks omitted).

83. *Id.* at 460.

> It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. . . . Nor can it be doubted that the owner can relay and impose those limitations/restrictions/conditions by means of written notice such as terms of service or use provisions placed on the home page of the website. . . . While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, . . . and while public policy considerations might in turn limit enforcement of particular restrictions, . . . the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.[84]

Despite concluding that MySpace did indeed have the right to define the limits of "authorized access" to its website, the court then undertook an analysis of Drew's conviction under the void-for-vagueness doctrine.[85] The court characterized the key vagueness-related issue as "whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine."[86]

The court commenced its vagueness analysis by reference to Justice Holmes's explanation of the "fair warning" requirement:

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.[87]

Citing *United States v. Lanier*,[88] the court then noted three scenarios in which the fair warning doctrine would bar enforcement of a criminal statute: (1) situations in which the forbidden or required acts are "so vague" that reasonable men would have to guess at the meaning and might differ as to the effect; (2) situations in which the "strict construction" rule would require limitation of the statute's scope to conduct

---

84. *Id.* at 461-62 (citations omitted).

85. *Id.* at 462-68.

86. *Id.* at 464.

87. *Id.* at 462-63 (quoting McBoyle v. United States, 283 U.S. 25, 27 (1931)) (internal quotation marks omitted).

88. 520 U.S. 259, 266 (1997).

clearly covered by the statute; and (3) situations in which a court uses a "novel construction" to extend the statute to conduct for which neither the statute itself nor construing cases have given any forecast of coverage.[89]

The court next explained that, as applied to any of these three situations, the void-for-vagueness doctrine embodies two "prongs" or requirements: (1) a "definitional/notice sufficiency requirement" pursuant to which the challenged statute must sufficiently describe the prohibited conduct to ensure fair notice to the public and to eliminate the possibility of arbitrary enforcement; and (2) a "minimal guideline[]" requirement pursuant to which the legislature must have crafted the law in such manner as to eliminate the possibility of "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections."[90]

The court reiterated that, to survive a void-for-vagueness challenge, a "criminal statute must contain 'relatively clear guidelines as to prohibited conduct' and provide 'objective criteria' to evaluate whether a crime has been committed."[91]

In its analysis, the court offered several rationales to support its ultimate finding that Drew's conviction was barred by the void-for-vagueness doctrine:

- that Drew's misdeeds on the MySpace site were, in fact, mere breaches of contract that did not involve criminal violations;[92]
- that, because MySpace does not charge any fee in relation to the establishment of user profiles, it was not damaged by Drew's unauthorized access;[93]
- that the owner of a website is, in effect, "darned if he does and darned if he doesn't" because any effort to characterize only certain user agreement violations as unauthorized access would be too vague and any effort to characterize all such violations as constituting unauthorized access would be overbroad;[94]
- that criminal liability for terms-of-service violations impermissibly allows a website owner to define what conduct is criminal;[95] and

89. *Drew*, 259 F.R.D. at 463 (quoting *Lanier*, 520 U.S. at 266) (internal quotation marks omitted).

90. *Id.* (alteration in original) (quoting Kolender v. Lawson, 461 U.S. 352, 357-58 (1983)) (internal quotation marks omitted).

91. *Id.* (quoting Gonzales v. Carhart, 550 U.S. 124, 149 (2007)).

92. *Id.* at 464.

93. *Id.*

94. *Id.* at 464-65.

95. *Id.* at 465.

- that MySpace's terms-of-service define authorized access in terms of the user's *promise* to abide by those terms, rather than the user's *actual compliance* with the terms.[96]

In further support of its ultimate holding that Drew's prosecution was barred by the vagueness doctrine, the court then–somewhat curiously–undertook a discussion best characterized as "everyone else is doing it, so why can't Drew?"[97] The court cited, as examples of other users potentially breaching the MySpace/user agreement (other "unauthorized users"), lonely hearts who lie about their age and appearance, users who post photographs of their friends, and parents who use their respective accounts to help their daughters sell girl scout cookies.[98] The court also noted that thirteen-year-old Megan herself was in violation of the MySpace Terms of Service, which required that users be at least fourteen years old.[99] These various justifications are, to say the least, less than compelling.[100]

In relation to the "minimal guideline" requirement, citing *United States v. Sablan*,[101] the Government argued that the CFAA's scienter requirement is satisfied when the user *intends* to violate the governing terms of service, thereby overcoming any vagueness-related challenge.[102] The court rejected the Government's position on the basis of

---

96. *Id.*

97. *See id.* at 466.

98. *Id.*

99. *Id.*

100. The finding that Drew's misdeeds were mere breaches of contract represents a virtual Sword of Damocles that threatens every future prosecution under the CFAA. In any criminal cases involving unauthorized access or access in excess of the permission actually granted, if there exists *any* contract between the complaining party and the accused–whether in the context of employer-employee, owner-contractor, or any other such relationships–the table is set for the Drew argument: "Aw, shucks, your honor, this is nothing more than a breach of contract case." The court's reliance on the fact that the establishment of MySpace did not entail any cost or fee is similarly meritless. MySpace, like Facebook, is a for-profit company whose primary asset is its universe of members and whose primary income source–advertising–depends in substantial part upon the accuracy of the user information maintained by the company. Finally, the court's "everyone else is doing it" discussion is especially specious. The substance of this reasoning is that violation of a website terms of service can never give rise to criminal charges because so many users commit minor violations (for example, the lonely heart who lies about his age or the user who posts unauthorized pictures). Taken to its logical conclusion, states would have to cease enforcement of speeding laws on some stretches of interstate highways because virtually every driver exceeds the speed limit and because some violations are less egregious than others (that is, enforcement of a 65 mph speed-limit nets both the driver who is going 66 mph and the driver going 96 mph).

101. 92 F.3d 865 (9th Cir. 1996).

102. *Drew*, 259 F.R.D. at 467.

three arguably meaningless distinctions between *Sablan* and the facts underlying Drew's prosecution: (1) *Sablan* involved access to a computer, while Drew accessed a website server; (2) the mens rea issue in *Sablan*, although also involving the CFAA, did not involve the vagueness doctrine; and (3) *Sablan* was a felony case that involved a different subsection of the CFAA.[103]

The court instead ultimately held the following:

> Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals . . . .
>
> In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[104]

III. CONCLUSION

A common mistake made by first-year law students and other non-lawyers is to ask, in relation to a given hypothetical fact pattern, "Can you sue?" when, in fact, they mean, "Does a colorable cause of action exist?" and "How likely is it that a lawsuit would be successful?" For decades, law school professors have responded to their students' question with an old axiom that highlights the inherent error in the students' formulation: "You can sue the Bishop of Boston for bastardy–you just won't win." This old saw underscores the extraordinarily low barrier for the commencement of a lawsuit in the United States legal system. As a result, even in cases best characterized as frivolous–cases that the plaintiff should never have filed–far too often, the only true winners are the attorneys collecting the fees from their respective clients. Accordingly, except in cases involving exigent or unusual circumstances, the prudent attorney sets a course for his client that minimizes the likelihood of his client being sued, rather than a course that merely increases the likelihood of winning some inevitable lawsuit.

---

103. *Id.*

104. *Id.* at 466-67 (alterations in original) (quoting City of Chicago v. Morales, 527 U.S. 41, 64 (1999)).

The educator considering whether to commence the use of, or continue to use, bogus social networking website accounts in the manner described herein should plot a similarly prudent course. The educator's guiding question should not be, "If I am charged or sued, would I prevail?" Rather, the "undercover educator" must understand that, even in the best possible circumstances and jurisdiction, he is still only a zealous prosecutor, an angry, influential parent, or a bad set of underlying facts away from becoming a criminal defendant. The educator should recognize that the undercover use of these accounts is, legally speaking, a bad idea.[105] The prudent decision therefore mandates the educator's immediate cessation of any undercover social networking website activities. There are enough challenges already to being an educator without adding the threat of jail time to the list.

105. Interestingly, there may exist reasons wholly unrelated to the threat of criminal prosecution that make the use of "undercover accounts" a bad idea. In an effort to minimize the likelihood of inappropriate communications or activities between teachers and students, a growing number of jurisdictions are implementing outright bans on social networking website "friend" relationships between teachers and students. Missouri Revised Statute § 162.069, a part of the Amy Hestir Student Protection Act, Mo. S.B. 54, Reg. Sess., 2011 Mo. Laws 1151, prohibited teachers and students from being "friends" on any social networking websites that allowed the possibility of private communications between the two. Mo. S.B. 54, 2011 Mo. Laws at 1161 (to be codified at MO. REV. STAT. § 162.069). The statute was almost immediately declared unconstitutional in *Missouri State Teachers Ass'n v. State*, No. 11 AC-CC00553, 2011 WL 4425537 (Mo. Cir. Ct. Sept. 23, 2011). In Lee County, Florida, school authorities instructed teachers that they should not "friend" students. Bob Sullivan, *Teachers, Students and Facebook, a Toxic Mix*, THE RED TAPE CHRONICLES (Oct. 22, 2010, 10:00 AM), http://redtape.msnbc.msn.com/_news/2010/10/22/6345537-teachers-students-and-facebook-a-toxic-mix (internal quotation marks omitted).

***