SOCIAL NETWORKING WEBSITES' LIABILITY FOR USER ILLEGALITY

*Joseph Monaghan**

INTRODUCTION

The purpose of this Comment is to examine social networking websites' liability for the criminal actions of their users beyond copyright infringement. Specifically, the Comment will illustrate that social networking websites are

* J.D., 2011, Seton Hall University School of Law; B.S., Mechanical Engineering, 2008, The College of New Jersey. The author would like to give a special thanks to Professor Jennings for his help and insights throughout the writing process.

capable of providing more effective protection, but have no incentive to do so because of the broad immunity granted to them by judicial interpretation of section 230 of the Communications Decency Act (CDA).[1] Therefore, legislation and increased liability for social networking websites are needed to bring about effective safety changes.

Part I provides necessary technical information and also discusses the origins of immunities granted to social networking websites and their owners by Congress through section 230, as well as the expansion of these immunities through judicial interpretation. Next, Part II examines some of the societal problems facilitated by social networking websites, including sexual abuse and cyberbullying. Part III explains why social networking websites should incur increased liability compared to other websites. Part IV discusses currently implemented but ineffective solutions to problems introduced in Part III, such as age verification and the banning of registered sex offenders. Part V discusses more effective solutions, such as those implemented by MySpace and development of parental-notification software.[2] In addition, it also discusses other possible solutions that have not yet been implemented. Lastly, Part VI explains why legislation is necessary to bring about effective safety changes on social networking websites.

I. HISTORY AND CONTEXT

A. Technical Background

An Internet Service Provider (ISP) is a company that offers its customers access to the Internet, for example, AT&T, Comcast, and Sprint.[3] An Internet Content Provider (ICP) is a party that creates or acquires information for distribution via the Internet, for example, Google, Amazon,

1. 47 U.S.C. § 230 (1996).

2. *See* Julia Angwin, *MySpace Moves to Give Parents More Information*, WALL ST. J., Jan. 17, 2007, http://online.wsj.com/article/SB116900733587978625.html; *see also infra* Part V.

3. ORG. FOR ECON. CO-OPERATION & DEV., OECD GLOSSARY OF STATISTICAL TERMS 418 (2007) ("[An ISP is a] company which provides end-users with a data connection allowing access to the internet and the associated services . . . .") [hereinafter OECD GLOSSARY].

Yahoo, Wikipedia, Facebook, MySpace.[4] ISPs provide the "pipes" through which data travels, although courts and academics may erroneously use the term ISP to cover ICPs as well. This Comment is limited to ICP liability, not ISP. As explained below, the reason for expanding ICP liability is because ICPs are in a better position than ISPs to monitor relationships among online identities and Internet Protocol (IP) addresses.

IP addresses are vital to the function of the Internet.[5] The Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA) create and coordinate IP addresses.[6] Under the control and supervision of ICANN,[7] IANA distributes IP addresses to five Regional Internet Registries (RIR) that redistribute them to ISPs in their specific geographical area.[8] ISPs then assign an IP address to a device, usually a modem.[9] If the modem is connected to a router, all of the devices connecting to the Internet through that modem share the same IP address.[10]

The IP address of a residential Internet connection—as well as some businesses and institutions—is not static.[11] If device one disconnects, the ISP may reassign that IP address to device two, and then assign device one a new IP address

4. *Internet Content Providers,* HOOVERS, http://www.hoovers.com/industry/internet-content-providers/1457-1.html (last visited Mar. 1, 2011).

5. *See* OECD GLOSSARY, *supra* note 3.

6. *See About ICANN*, ICANN, http://www.icann.org/en/about/(last visited Feb. 22, 2011); *Number Resources,* IANA, http://www.iana.org/numbers/ (last visited Feb. 22, 2011).

7. Contract Between ICANN and the U.S. Gov't for Performance of the IANA Function C.2.1.1 (Mar. 17, 2003), *available at* http://www.icann.org/en/general/iana-contract-17mar03.htm.

8. *Number Resources*, *supra* note 6; Kim Davies, Internet Assigned Nos. Auth., Presentation at the ICANN at Large Community Briefing: An Introduction to IANA (Sept. 2008), http://www.iana.org/about/presentations/davies-atlarge-iana101-080929.pdf.

9. *What is the Difference Between Dynamic and Static IP Addresses?*, SPEEDGUIDE.NET, http://www.speedguide.net/faq_in_q.php?category=88&qid=137 (last visited Feb. 14, 2011) [hereinafter *Dynamic and Static IP Addresses*].

10. *See id.* ("The limited IP address space is one of the reasons for the wide use of NAT routers . . . ."); Definition of NAT, SPEEDGUIDE.NET, http://www.speedguide.net/terms_popup.php?seek=^NAT$ (last visited Mar. 23, 2011) ("NAT [network address translation] permits a large number of LAN [local area network] users to share one external IP address.").

11. *Dynamic and Static IP Addresses*, *supra* note 9. ("Residential Internet connections, whether broadband or dialup usually use dynamic IP addresses . . . .").

when it reconnects.[12] ISPs recycle IP addresses because there are not enough IP addresses to assign each device a different address.[13] This is why IP addresses have limited utility in tracking someone's identity.[14]

The system currently used is IPv4, and provides over four billion unique IP addresses.[15] ICANN is running out of IP addresses to distribute,[16] and is introducing a new system called IPv6 as a result, which provides substantially more IP addresses.[17] Although computers are currently being built that incorporate IPv6 compatibility, very few use it.[18] This means that monitoring capabilities and Internet security may change drastically with the new system.[19]

B. Communications Decency Act

In 1996, Congress passed the CDA as part of the

12. *Id.* ("With dynamic IP addressing, there is a pool of IPs that your ISP can assign to users. When you connect to the Internet, your computer is leased one IP address from that pool for a number of hours. When you disconnect, or when the lease expires the IP address is freed and put back into the pool of available IPs.").

13. *Id.* ("The need for dynamic IP addresses arises from the limited number of IP addresses available in IPv4 (Internet Protocol version 4). . . . That way, ISPs can have more subscribers than number of IP addresses . . . and ease IP maintenance.").

14. Andy Johnson, *The IP Mystery: How Police Track Your Online Activity*, CTV NEWS (Sept. 12, 2007, 7:21 PM), http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070912/spying_background_070912/20070912/.

15. *See Number Resources*, *supra* note 6; *What is IPv6?*, WHAT IS MY IP ADDRESS?, http://whatismyipaddress.com/ip-v6 (last visited Mar. 23, 2011) ("IPv5 currently supports a maximum of approximately 4.3 billion unique IP addresses.").

16. Tom Espiner, *ICANN: IPv4 Will Run Out by 2011*, ZDNET UK (May 12, 2008), http://www.zdnet.com.au/icann-ipv4-will-run-out-by-2011-339288828.htm.

17. *See Number Resources*, *supra* note 6; *What Is IPv6?*, *supra* note 15 ("IPv6 supports a theoretical maximum of 2128 [billion] addresses (340,282,366,920,938,463,463,374,607,431,768,211,456 to be exact!).").

18. Paul Meller, *European Commission Urges Rapid Adoption of IPv6*, Post to *Business Center*, PC WORLD (May 27, 2008, 12:00 PM), http://www.pcworld.com/businesscenter/article/146319/european_commission_urges_rapid_adoption_of_ipv6.html ("Most new computer and sever software sold by major manufacturers is already IPv6 compatible, but the computers and devices running this software are still only reachable through their old IPv4 addresses."). *See also IPv4-IPv6 Compatibility*, BGP EXPERT (June 6, 2006), http://www.bgpexpert.com/article.php?article=106.

19. *IPv6*, CYBERTELECOM, http://www.cybertelecom.org/dns/ipv6.htm (last visited Feb. 17, 2011) ("This large number of IPv6 addresses means that almost any electronic device can have its own address . . . . [T]he massive address space available in IPv6 will allow virtually any device to be assigned a globally reachable address. This change fosters greater end-to-end communication abilities between devices with unique IP addresses . . . .").

Telecommunications Act.[20] One part of the CDA, later found unconstitutional by the Supreme Court,[21] was intended to protect the public from indecent and obscene online material.[22] Section 230, which provides immunity to "interactive computer services," survived constitutional scrutiny.[23]

Congress enacted section 230 in response to two cases that discussed the distinction between a "distributor" and a "publisher," expressly overruling one of those cases.[24] A publisher is a person or entity that exercises editorial control over the content of a work, for example, newspapers.[25] Comparatively, a distributor makes content available to the public but exercises no editorial control, for example, newsstands.[26] The issue is substantial because under the law of most states, a publisher is strictly liable for defamatory statements, whereas a distributor is liable only for content it knew or should have known was defamatory.[27]

20. 47 U.S.C. § 230(a)–(d), (f)(2) (2006) ("The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.").

21. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 885 (1997) (holding that the CDA violated the First Amendment).

22. *See* Discussion of the CDA, CTR. FOR DEMOCRACY & TECH., http://cdt.info/grandchild/cda/ (last visited Feb. 17, 2011).

23. *See generally* John Nisbett, *Checkmate: How Sexual Predators in (Your) Space Have Strategically Employed Existing Cyber-Laws to Outflank Their Prey*, 28 MISS. C. L. REV. 181, 185 (2009); *see also* Madeline K. Rodriguez, Reexamining Section 230 of the CDA and Online Anonymous Speech: Defamation on the Internet and the Websites that Facilitate It 5 (May 2009) (unpublished Honors Thesis, Boston College) (on file with Department of Communication, Boston College), *available at* http://webcache.googleusercontent.com/search?q=cache:http://www.bc.edu/schools/cas/communication/meta-elements/pdf/thesis09.rodriguez.pdf.

24. H.R. Conf. Rep. No. 104-458, at 193–94 (1996).

25. John W. Dean, *Defamation Immunity on the Internet: An Evolving Body of Law Has Been Stretched Beyond Its Limits*, FINDLAW (July 4, 2003), http://writ.news.findlaw.com/dean/20030704.html.

26. *Id.*

27. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1367 n.10 (N.D. Cal. 1995). The *Religious Technology Center* court stated:

> Recent decisions have held that where a [bulletin board service] exercised little control over the content of the material on its service, it was more like a "distributor" than a "republisher" and was thus only liable for defamation on its system where it knew or should have known of the defamatory statements. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991). By contrast, a New York state court judge found that Prodigy was a publisher because it held itself out to be controlling the content of its services and

The first case discussing the difference between distributor and publisher with relation to the Internet was *Cubby, Inc. v. CompuServe, Inc.*, where CompuServe, an ISP, hosted an online news forum and was sued for defamatory comments posted by a user.[28] The *Cubby* court held that CompuServe was not liable as it was considered a distributor, not a publisher, under defamation law because it lacked editorial involvement.[29] The second case was *Stratton Oakmont v. Prodigy Services Co.*, where Prodigy, an ISP, was sued for defamatory comments posted by an unknown user on its "Money Talk" bulletin board.[30] The *Stratton* court held that Prodigy was liable as a publisher for content posted by its users because it took affirmative steps toward editorial control by attempting to screen offensive content.[31] As a result of these decisions, ISPs are less likely to screen content. Where screening might subject ISPs to liability as publishers, taking no action at all would classify ISPs as mere distributors, thereby facing limited liability.[32]

Congress's stated purpose in passing section 230 of the CDA was to "promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material."[33] Section 230 states that interactive computer services are not liable as publishers, and affords protection for "'Good Samaritan' blocking and screening of offensive material."[34] The plain

because it used software to automatically prescreen messages that were offensive or in bad taste. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *10 (N.Y. Sup. Ct. May 24, 1995).

Id. *See also* H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 373 (2008).

28. 776 F. Supp. 135, 137 (S.D.N.Y. 1991).

29. *Id.* at 140–41.

30. No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *1 (N.Y. Sup. Ct. May 24, 1995).

31. *Id.* at *10; Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 210–11 (2002).

32. Holland, *supra* note 27, at 372 ("Representatives of the online industry argued that the Prodigy decision placed service providers in an untenable position by 'creating a 'Hobson's choice' between creating 'child safe' areas that expose the ISP to liability as an editor, monitor, or publisher, and doing nothing in order to protect the ISP from liability.'" (quoting Robert Cannon, *The Legislative History of Senator Eon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 62 (1996))).

33. *See* 47 U.S.C. § 230 (2006); *see also* Carafano v. Metrosplash.com, 339 F.3d 1119, 1122 (9th Cir. 2003).

34. 47 U.S.C. § 230(c) (2006).

language of the statute provides that an interactive computer service would not be held liable as a publisher.[35] Notably, however, the Internet model at the time Congress enacted the CDA was very different than what has since evolved. Shortly after Congress passed the CDA, ISPs began to realize that greater profits could be made through Internet content rather than Internet services. This led to companies providing content while still seeking liability protection as ISPs.[36] It is uncertain whether Congress would have afforded the same protection at the time it enacted the CDA had it known that ISPs would deliver content in the future.

C. Judicial Expansion of Online Immunity

Courts have consistently given section 230 a broad reading by providing liability protection to ICPs even when the particular ICP knew, or should have known, the material was illegal.[37] In *Zeran v. America Online, Inc.*, Zeran sued America Online (AOL) for failing to remove a defamatory posting on its website after receiving notice.[38] Zeran contended that AOL had a "duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material."[39] The *Zeran* court found, however, that section 230 provided federal immunity for any cause of action originating from a third-party's use of the service.[40] In doing so, the *Zeran* court interpreted section 230 as a grant of distributor immunity. Section 230 states: "No provider or user of an interactive computer service shall be treated as the *publisher or speaker* of any information provided by another information

35. § 230(c)(1) ("Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the *publisher* or speaker of any information provided by another information content provider." (emphasis added)); *see* Holland, *supra* note 27, at 388.

36. *See* Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 984–85 (10th Cir. 2000) (finding that America Online was immune from liability as an ISP, in part because that it did not help create the inaccurate stock quotation even though the company provided the stock quotation); *see also* Blumenthal v. Drudge, 992 F. Supp. 44, 51–52 (D.D.C. 1998) (finding that America Online was immune from defamation liability as an ISP even though it had a licensing agreement with the author to provide the defamatory content).

37. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997).

38. *Id.* at 328.

39. *Id.* at 330.

40. *Id.* at 330–31.

content provider."[41]

Courts have also extended immunity to websites that knowingly profited from the illegal activities of their users.[42] For example, in *Doe v. Bates*, plaintiffs contended that Yahoo! knowingly profited from the trafficking of child pornography.[43] The *Bates* court found that Yahoo! was immune from any civil liability for third-party content on its website, even if the company had knowledge of the existence of the illegal content.[44] The *Bates* court reasoned that if Yahoo! could be held liable for allowing material it reviewed to be posted on the site, it would simply choose not to regulate at all, which would go against the Congressional purpose of section 230.[45] Nothing in the language of the statute, however, suggests that Congress intended to supersede traditional secondary liability analysis—holding an entity liable for knowledge of, promotion of, refraining to control, or profiting from illegal activity.[46]

Social networking websites are one of many beneficiaries of the judicial expansion of section 230. A social networking website is a service that provides its users with connectivity to friends and self-expression.[47] Although social networks target different audiences and offer varying services,[48] they all

41. 47 U.S.C. § 230(c)(1) (2006) (emphasis added).

42. *See, e.g.*, Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006); Voicenet Commc'ns, Inc. v. Corbett, 2006 WL 2506318 (E.D. Pa. Aug. 30, 2006).

43. 2006 WL 3813758, at *1.

44. *Id.* at *4. ("Section 230 does not . . . provide that an intentional violation of criminal law should be an exception to the immunity from civil liability given to Internet service providers.").

45. *Id.*

46. *Compare* § 230(c)(2) ("No provider or user of an interactive computer service shall be held [civilly] liable on account of . . . (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."), *with* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) (holding operators of a swap meet liable where they allowed vendors to sell counterfeit goods and they had knowledge of, control of, and profited from the infringing activity), *and* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 938, 941 (2005) (holding plaintiffs liable because they knew their software was used for copyright infringement, they promoted its use for copyright infringement, did not attempt to prevent the infringement, and profited from their users' copyright infringement).

47. Richard M. Guo, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 619–20 (2008).

48. *See, e.g.*, FACEBOOK, http://www.facebook.com/facebook (last visited Mar. 23,

share two primary components: the profile and the community.[49] The user enters his or her own personal information into his or her profile, such as interests, birthday, hometown, and photos.[50] Users then create communities by mutually agreeing to link their profiles with one another.[51] As a result of judicially extended immunity to ICPs, these social networking websites have also been consistently granted broad section 230 immunity.[52] Most notably, in *Doe v. MySpace, Inc.*, a thirteen-year-old girl sued MySpace for "failing to implement basic safety measures to prevent sexual predators from communicating with minors . . . ."[53] The plaintiff misrepresented her age on her online profile and attracted the attention of a nineteen-year-old man.[54] The man allegedly assaulted the plaintiff when the two met in person for a date.[55] The *MySpace* court held that MySpace was immune from any liability as a result of the immunity granted by Congress under section 230.[56]

II. THE PROBLEM WITH ONLINE SOCIAL NETWORKS

Online social networking plays an increasingly dominant role in the lives of most people, regardless of nationality or

2011) ("Facebook helps you connect and share with the people in your life."); *About us*, MYSPACE, http://www.myspace.com/Help/AboutUs (last visited Mar. 23, 2011) ("Myspace, Inc. is a leading social entertainment destination powered by the passions of fans."); TWITTER, www.twitter.com (last visited Feb. 18, 2011) (microblogging and real-time short messaging service); DEVIANTART, www.deviantart.com (last visited Feb. 18, 2011) (online community of artists and their artwork); *About Us*, LINKEDIN, http://press.linkedin.com/about (last visited Jan. 18, 2010) (over 100 million professionals use LinkedIn to exchange information, ideas and opportunities").

49. Guo, *supra* note 47, at 619 ("While the various social networking services offer different features, they build around two basic elements: the profile and the community.").

50. *Id.* ("A profile is a webpage that allows a user to aggregate and present her personal information . . . .").

51. *Id.* at 620 ("Users create communities by linking their profiles with one another.").

52. *See, e.g.*, Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd* 528 F.3d 413 (5th Cir. 2008); Doe v. SexSearch, 502 F. Supp. 2d 719 (N.D. Ohio 2007).

53. 474 F. Supp. 2d at 848.

54. *Id.* at 846.

55. *Id.*

56. *Id.* at 850–52 (holding also that the plaintiff's state negligence claim failed because MySpace did not have a duty to protect minors or control conduct of third parties, and also MySpace was not required to implement safety measures to protect minors from sexual assault).

demographics. Social networking websites account for ten percent of all Internet time, the time spent on these websites is growing three times faster than the overall Internet rate, and using social networking websites is currently the fourth most popular online activity.[57] Although the Baby Boomer generation is the fastest growing age demographic,[58] and adults comprise the majority of social networking site users,[59] online social networking plays a more prevalent part in the lives of teens and young adults.[60]

Particularly worrisome is the dangerous appeal of social networking websites to young children. Children are becoming more tech-savvy at increasingly younger ages.[61] As a result, they are participating in social networking websites primarily aimed at teens and adults.[62] In response, some companies have created social networking websites directed specifically to children below the age of fourteen, some having a minimum age requirement as low as five years old.[63] As the

57. News Release, Nielson, Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email, Nielson Reports (Mar. 9, 2009), *available at* http://www.nielsen-online.com/pr/pr_090309.pdf; *see also Social Networking and Blog Sites Capture More Internet Time and Advertising*, Post to *Nielson Wire*, THE NIELSON CO. (Sept. 24, 2009), http://blog.nielsen.com/nielsenwire/online_mobile/social-networking-and-blog-sites-capture-more-internet-time-and-advertisinga/.

58. Steve Rubel, *Social Networking Demographics: Boomers Jump In, Gen Y Plateaus*, MICRO PERSUASION (Mar. 23, 2009), http://www.micropersuasion.com/2009/03/social-networking-demographics.html; *see also* Justin Smith, *Fastest Growing Demographic on Facebook: Women Over 55*, INSIDE FACEBOOK (Feb. 2, 2009), http://www.insidefacebook.com/2009/02/02/fastest-growing-demographic-on-facebook-women-over-55/.

59. *See Social Network User Demographics*, EMARKETER (Jan. 27, 2009), http://www.emarketer.com/Article.aspx?R=1006882.

60. *See Teens on Social Networks*, EMARKETER (Apr. 16, 2009), http://www.emarketer.com/Article.aspx?R=1007041 (stating that 75% of American teens use social networks, and predicting that number to increase to 79% by 2013); *see also* Mark Dolliver, *Take Care When Targeting Teens Online*, ADWEEK (Oct. 5, 2009), http://www.adweek.com/aw/content_display/news/agency/e3i505f5fdeedc76b42ca9d8d4695e83c6c (stating that 66% of teens said they use social networks when online); *see also* Amanda Lenhart, *Adults and Social Network Websites*, PEW INTERNET (Jan. 14, 2009), http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx (finding that 75% of adults, ages18–24, use online social networks).

61. *See Young People and Social Networking Sites*, CHILDNET INT'L (2010), http://www.childnet.com/downloads/blog_safety.pdf.

62. Jemima Kiss, *100,000 Kids Join CBBC Social Network*, GUARDIAN.CO.UK (July 10, 2008, 15.01 BST), http://www.guardian.co.uk/media/2008/jul/10/digitalmedia.web20 ("MyCBBC was launched shortly before an official report by media regulator Ofcom found that more than a quarter of eight- to eleven-year-olds in the UK regularly use social networking sites designed for older children and teenagers.").

63. Carolyn Jabs, *These 'Social Websites' Cater to Little Kids*, TECHNO FAM.,

amount of time spent and the number of users on social networking websites grow, a wide range of problems have been created and facilitated by these websites.[64]

A. Sexual Abuse

The online social networking problem garnering the most media attention is sexual abuse, with the victims ranging from young children to adults. An online social network's role in inadvertently facilitating sexual abuse varies from case to case. A large number of victims meet their assailants through online social networks. One out of seven children between the ages of thirteen and seventeen receive unwanted sexual solicitations online.[65] This problem is compounded by young Internet users' willingness to engage in online relationships.[66] Despite years of "awareness" programs and media coverage, the story generally remains the same: a young Internet user meets a "friend" over a social network, subsequently meets them in person, and is then sexually assaulted.[67] Fortunately,

http://mymetrokids.com/january08/technofamily0108.html (last visited Mar. 1, 2011) (naming Club Penguin, Imbee, Webkinz, Neopets, and Kidscom as social networks for children); Gina Chen, *Making Sense of Social-Networking Sites for Young Kids*, SYRACUSE.COM (Dec. 29, 2008, 4:00 AM), http://blog.syracuse.com/family/2008/12/making_sense_of_socialnetworki.html.

64. *See, e.g.*, TRENCH REYNOLDS' CRIME NEWS, http://thetrenchcoat.com/ (follows crimes facilitated by or committed through online social networks).

65. JANIS WOLAK, KIMBERLY MITCHELL & DAVID FINKELHOR, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, ONLINE VICTIMIZATION OF YOUTH: FIVE YEARS LATER vii (2006), http://www.unh.edu/ccrc/pdf/CV138.pdf.

66. *See id.* at 1 ("In YISS-2 there were also declines in the proportions of youth Internet users who communicated online with people they did not know in person (34% down from 40% in YISS-1 or who formed close online relationships with people they met online (11% down from 16%).").

67. Lori Fullbright, *Sapulpa Man Accused of Raping Teen After Meeting on MySpace,* NEWSON6.COM (Oct. 22, 2009, 1:41 PM) http://www.newson6.com/global/story.asp?s=11355491 (noting that a nineteen-year-old raped a fifteen-year-old girl he met over MySpace after he and a friend took her home and got her drunk); *Ex-Teacher's Aide Accused of Preying on Girls*, WFSB.COM (Oct. 10, 2006, 11:32 PM), http://www.wfsb.com/news/10047964/detail.html (a thirty-one-year-old pretending to be nineteen sexually assaulted teenage girls he met through MySpace); *Sex Offender Pleads Guilty to Having Sex with Teen MySpace Girl*, TRENCH REYNOLDS' CRIME NEWS (Oct. 10, 2009), http://mycrimespace.com/2009/10/10/sex-offender-pleads-guilty-to-having-sex-with-teen-myspace-girl/ (thirty-three-year-old lied about his age to a fourteen-year-old girl he met on MySpace and then had sex with her); *From the 15 Will Get You 20 Files: Joshua Britzman*, TRENCH REYNOLDS' CRIME NEWS (Sept. 27, 2009), http://mycrimespace.com/2009/09/27/from-the-15-will-get-you-20-files-joshua-britzman/ (twenty-three-year-old charged with having sex with a fifteen-year-old girl that he met

some criminals are caught before committing any physical harm.[68] An assailant, however, can cause harm or commit a crime without ever physically meeting the victim. There are a number of unfortunate stories involving older men and women who pose as someone they are not, enticing underage children to send them sexually explicit pictures of themselves.[69]

Due to the detail and breadth of personal information and preferences a user puts on his or her social networking profile, predators are able to feign common interests, allowing them to build online relationships very quickly.[70] Predators are able to use social networks for frequent, private exchanges outside of public view and parental supervision as a way to develop online relationships.[71]

---

on Facebook); *Brooklyn Man Charged with Having Sex with Upstate NY Teen He Met on Facebook*, TRENCH REYNOLDS' CRIME NEWS (Sept. 14, 2009), http://mycrimespace.com/2009/09/15/brooklyn-man-charged-with-having-sex-with-upstate-ny-teen-he-met-on-facebook/ (twenty-three-year-old accused of having sex with a fifteen-year-old girl he met on Facebook).

68. Emily S. Achenbaum, *Facebook Child Porn Case Results in 35-year Federal Prison Term*, CHI. TRIB., Oct. 22, 2008, http://articles.chicagotribune.com/2008-10-22/news/0810210346_1_federal-prison-term-facebook-child (stating that Michael, a twenty-five-year-old was caught after he posed as a teenage girl, solicited a teenage boy, and tried to blackmail him for not posting sexual videos of himself on Facebook. Michael, posing as the teenage girl, told the boy that he could have sex with "her" only if the boy had sex with her male friend (Michael) first); *Boys' MySpace Prank Results in Sex Crime Arrest*, Post to *Security*, MSNBC (Mar. 8, 2006), http://www.msnbc.msn.com/id/11708746/ (teenage boys setup a fake profile as a fifteen-year-old girl and through coincidence helped police capture a forty-eight-year-old man trying to meet "her" for sex).

69. *Kansas Man Indicted on Facebook Child Porn Charges*, TRENCH REYNOLDS' CRIME NEWS (May 22, 2009), http://mycrimespace.com/2009/05/22/kansas-man-indicted-on-facebook-child-porn-charges/ (thirty-eight-year-old posed as a nineteen-year-old woman on Facebook to get teenage boys to send him sexual explicit photos of themselves); *More on Stickam's Latest Predator*, TRENCH REYNOLDS' CRIME NEWS (Oct. 21, 2009), http://mycrimespace.com/2009/10/21/more-on-stickams-latest-predator/ (father would pose as a seventeen-year-old boy on Stickam and convince underage girls to masturbate on webcam, sometimes by threatening to tell the girls parents if they did not do what he wanted).

70. VICTORIA BAINES, ECPAT INT'L, ONLINE CHILD SEXUAL ABUSE: THE LAW ENFORCEMENT RESPONSE 29 (2008), http://www.ecpat.net/worldcongressIII/PDF/Publications/ICT_Law/Thematic_Paper_ICTLAW_ENG.pdf ("Equal attention [ ] must be paid to the speed with which suspects are able to build online relationships with children and young people on the basis of positive feedback and the pretence of common interests or points of view – an observed offline grooming technique with a much wider application in those online environments where young people feel free to express themselves.").

71. Janis Wolak et al., *Online "Predators" and Their Victims: Myths, Realities, and*

Although better security measures may prevent some crimes,[72] this is not true of all crimes facilitated by social networking websites. For example, it would be nearly impossible for social networks to prevent certain crimes occurring between adults who merely meet through a social networking website.[73] Still, the inability to prevent all crimes does not mean social networking websites are helpless to prevent some of them.

B. Cyberbullying

Another problem associated with online social networks is cyberbullying,[74] defined as the "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices."[75] Although cyberbullying is not unique or exclusive to online social networks, social networks are one of its most prevalent virtual locations, and soon to be the most common source of cyberbullying worldwide.[76]

Implications for Prevention and Treatment, 63 AM. PSYCHOL. 111, 121 (2008), *available at* http://www.apa.org/pubs/journals/releases/amp-632111.pdf ("Online communications such as e-mail or instant messages allow frequent, swift, and private exchanges, which online molesters can use to develop relationships with and seduce victims outside of public view and parental supervision. Moreover, youths may be more willing to talk extensively and about more intimate matters with adults online than in face-to-face environments.").

72. *See* discussion *infra* Part IV.

73. *Woman Allegedly Raped After Meeting Someone on Tagged.com*, TRENCH REYNOLDS' CRIME NEWS (Sept. 5, 2009), http://mycrimespace.com/2009/09/06/woman-allegedly-raped-after-meeting-someone-on-tagged-com/ (fifty-one-year-old woman was drugged and raped after meeting a man from Tagged); *MySpace Rapists Get Slaps on the Wrists*, TRENCH REYNOLDS' CRIME NEWS (Oct. 8, 2009), http://mycrimespace.com/2009/10/08/myspace-rapists-get-slaps-on-the-wrists/ (two men plead guilty to raping a twenty-year-old woman that they met on MySpace); *MySpace Pants Robbers Busted*, TRENCH REYNOLDS' CRIME NEWS (Oct. 4, 2009), http://mycrimespace.com/2009/10/04/myspace-pants-robbers-busted/ (stating a man went to meet a woman he met over MySpace and had his pants stolen by her and an accomplice).

74. *See* CYBERBULLYING RESEARCH CTR., http://www.cyberbullying.us/ (last visited Mar. 19, 2011).

75. SAMEER HINDUJA & JUSTIN W. PATCHIN, CYBERBULLYING RESEARCH CTR., CYBERBULLYING FACT SHEET: WHAT YOU NEED TO KNOW ABOUT ONLINE AGGRESSION 1 (2009), http://www.cyberbullying.us/cyberbullying_fact_sheet.pdf.

76. *Cyber Bullying Statistics that May Shock You!*, CYBERBULLY ALERT (Aug. 27, 2008), http://www.cyberbullyalert.com/blog/2008/08/cyber-bullying-statistics-that-may-shock-you/ ("Currently, the most common virtual locations for cyberbullying are chat rooms, social networking web sites, email and instant message systems. . . . Social networking sites such as Facebook and MySpace are growing fast, and so are the cyberbullying incidents originating from them. Experts believe that they will soon

In 2006, cyberbullying gathered national media attention when thirteen-year-old Megan Meier committed suicide.[77] The cyberbully was "Josh Evans," a fictional sixteen-year-old boy created by Lori Drew, her daughter, and her assistant.[78] The purpose was to tease and humiliate Megan, with whom Lori Drew's daughter had a falling out.[79] At the time, no law existed specifically addressing cyberbullying for state or federal prosecutors to charge Drew.[80] The government unsuccessfully attempted to convince the fact-finder that "violating MySpace's terms of service was the legal equivalent of computer hacking."[81] In response, many states passed anti-cyberbullying laws,[82] and a federal bill is currently pending on the matter.[83]

overtake chat rooms as the top source of cyberbullying problems worldwide.").

77. Gina Keating, *MySpace Suicide Conviction Tentatively Dismissed*, REUTERS (July 2, 2009, 7:10 PM), http://www.reuters.com/article/technologyNews/idUSN029085920090702.

78. Tom McCarthy & Scott Michels, *Lori Drew MySpace Suicide Hoax Conviction Thrown Out*, ABC NEWS (July 2, 2009), http://abcnews.go.com/TheLaw/story?id=7977226&page=1.

79. Keating, *supra* note 77; *Cyber-Bullying Trial Opens in US*, BBC NEWS (Nov. 20, 2008, 8:27 GMT), http://news.bbc.co.uk/2/hi/americas/7738982.stm.

80. Frederick Lane, *Teen's Suicide Spurs Anti-Cyberbullying Law*, NEWSFACTOR (Nov. 24, 2007, 9:07 AM), http://www.newsfactor.com/story.xhtml?story_id=56869&full_skip=1.

81. Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED (July 2, 2009, 3:04 PM), http://www.wired.com/threatlevel/2009/07/drew_court/. *Accord* United States. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (acquitting Lori Drew after she was charged and found guilty by a jury under the Computer Fraud and Abuse Act).

82. *See, e.g.*, ARK. CODE ANN. § 6-18-514 (West 2010); A.B. 86 (Cal. 2008); DEL. CODE ANN. Tit. 14, § 4112D (West 2010); FLA. STAT. § 1006.147 (2010); IDAHO CODE ANN. § 18-917A (West 2010); IOWA CODE § 280.28 (West 2010); KAN. STAT. ANN. § 72-8256 (West 2010); H.B. 199, 2008 Gen. Assemb., Reg. Sess. (Md. 2008); E.O. 46 (Mich. 2007); MINN. STAT. ANN. § 121A.0695 (West 2010); S.B. 818, 94th Gen. Assemb., Reg. Sess. (Miss. 2008); L.B. 205, 2008 Leg. (Neb. 2008); N.J. STAT. ANN. § 18A:37-15 (West 2010); S.B. 1941, 51st Leg., 2d Sess. (Okla. 2008); OR. ADMIN. R. 581-022-1140 (2010); 24 PA. CONS. STAT. ANN. § 13-1303.1-A (West 2010); R.I. GEN. LAWS § 16-21-26 (2010); S.C. CODE ANN. § 59-63-120 (2010); WASH. REV. CODE § 28A.300.285 (2010). *See also* Ashley Surdin, *In Several States, a Push to Stem Cyber-Bullying*, WASH. POST, Jan. 1, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/31/AR2008123103067.html ("The [cyberbullying] phenomenon has led to a push among states to pass laws aimed at clamping down on the student-spun harassment, intimidation and threats coursing through the Web. Most of the laws are aimed at school districts, requiring them to develop policies on cyber-bullying – for example, how to train school staff members or discipline students. At least 13 states have passed such laws . . . .").

83. Megan Meier Cyberbulling Prevention Act of 2009, H.R. 1966, 111th Cong. (2009); Anna North, *Is Legislation the Way to Stop Cyberbullying?*, JEZEBEL (Oct. 1,

While most instances of cyberbullying do not have such drastic outcomes, it is still a growing problem with varying degrees of harm,[84] and social networking websites are the new favored forum of cyberbullies.[85] At the time of the Megan Meier incident, MySpace may not have had the technological means to prevent Lori's actions, nor the means to confirm the existence of "Josh Evans."[86] But with significant advances in the law, and with current technology, there may be a practical system available for identifying and monitoring cyberbullying.[87]

III. INCREASING SOCIAL NETWORKING WEBSITES' LIABILITY COMPARED TO OTHER TYPES OF WEBSITES

Social networking websites are unlike any other type of website, because users of social networking websites freely expose a tremendous amount of personal information.[88] As previously indicated, this liberal display of information results in a host of new problems, but it also provides a useful resource.

2009, 12:00 PM), http://jezebel.com/5371949/is-legislation-the-way-to-stop-cyberbullying.

84. Chris Matyszcyk, *Teen Sues Facebook, Classmates Over Cyberbullying*, CNET NEWS (Mar. 3, 2009, 4:37 PM), http://news.cnet.com/8301-17852_3-10187531-71.html (Teenager Denise Finkel sued her classmates, and Facebook, for creating a Facebook group forum containing posts claiming that she "had AIDS, was an intravenous drug user, and had 'inappropriate conduct with animals'"); Jim Staats, *MySpace.com: Why Parents and Cops Fear a Hot Site's Dark Side*, MARIN INDEP. J. (Mar. 27, 2006, 6:50 AM), http://www.marinij.com/ci_3643735 (thirteen-year-old had to switch schools after her friends started an "Olivia Haters" club on MySpace); Nadia Wynter, *Parents of Holly Grogan, 15, Blame Facebook for Teen's Suicide*, DAILY NEWS, Sept. 21, 2009, http://www.nydailynews.com/news/world/2009/09/21/2009-09-21_parents_of_holly_grogan_15_blame_facebook_for_teens_suicide.html (British fifteen-year-old Holly Grogan committed suicide in part from being the recipient of cyberbullying on her Facebook wall).

85. Arieanna, *Cyberbullying More Prevalent on Social Networking Sites*, ABSOLUTE SOFTWARE (July 4, 2007), http://blog.absolute.com/cyberbullying-more-prevalent-on-social-networking-sites/ (39% of social network users had been cyberbullied in some way, versus 22% of teens not using social networking sites).

86. *See* discussion *infra* Part IV (discussing the difficulty of identifying fake profiles).

87. *See* discussion *infra* Part V.

88. Jessica S. Groppe, *A Child's Playground or a Predator's Hunting Ground?: How to Protect Children on Internet Social Networking Sites*, 16 COMMLAW CONSPECTUS 215, 224–25 (2007) ("Interactive communication on social networking sites opens a virtually endless window for members to explore their creativity by being able to share interests, pictures, diaries, artwork, creative writing, music, and videos with other members.").

Compare the liability of a social networking site with that of a search engine (e.g., Google, Yahoo!, Bing). Twitter, one of the most popular social networking websites today,[89] has over fifty million unique accounts.[90] A person does not need a Twitter account to view most of Twitter's profiles.[91] These profiles are publicly accessible and can be located using search engines. This means a law holding Twitter liable for its users' activities, would require the company to actively police fifty million web pages.[92] Twitter is just one website of over 185 million websites.[93] This means that to hold search engines liable for the content of the web results they return, search engines would need to monitor fifty million of Twitter's pages, plus an additional 185 million websites,[94] each containing any number of web pages.[95]

A fairer comparison may be made to online auction and shopping websites (e.g., Amazon.com, eBay, Craigslist). The content of these websites is more similar to social networking websites than search engines because monitoring is limited to the company's own website. To put an item up for sale on eBay, a user writes a description and uploads a picture,[96] EBay takes measures to prevent fraudulent transactions, [97]

89. *Top 15 Most Popular Social Networking Websites | March 2011*, EBIZMBA, http://www.ebizmba.com/articles/social-networking-websites (last visited Mar. 31, 2011).

90. Robert J. Moore, *Twitter Data Analysis: An Investor's Perspective*, TECHCRUNCH (Oct. 5, 2009), http://www.techcrunch.com/2009/10/05/twitter-data-analysis-an-investors-perspective/.

91. *See generally* TWITTER, http://twitter.com/ (last visited Mar. 31, 2011).

92. *Website vs. Webpage*, INNOVATIONSIMPLE (Apr. 21, 2009), http://innovationsimple.com/web-design/website-vs-webpage/ (a website is composed of webpages).

93. *January 2009 Web Server Survey*, NETCRAFT (Jan. 16, 2009), http://news.netcraft.com/archives/2009/01/16/january_2009_web_server_survey.html.

94. *Id.*

95. *See We Knew the Web Was Big . . . ,* OFFICIAL GOOGLE BLOG (July 25, 2008, 10:12:00 AM), http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html (over one trillion unique URLs on the Internet).

96. *How Do I List an Item for Sale?*, EBAY, http://pages.ebay.com/help/sell/questions/list-item.html (last visited Mar. 27, 2011).

97. This is not to say that eBay's system is completely effective. *See* Tiffany, Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 477–78 (S.D.N.Y. 2008) ("For obvious reasons, the fraud engine could not determine whether a listed item was actually counterfeit. . . . Nevertheless, eBay's ultimate ability to make determinations as to infringement was limited by virtue of the fact that eBay never saw or inspected the merchandise in the listings. While some items-such as guns-were completely prohibited and thus required no judgment to remove, listings that offered potentially infringing and/or counterfeit items required a more in-depth review."). Although, eBay can, and does, take steps to

partly through identity verification by requiring a seller to use a PayPal[98] account or credit card, which is appropriate because a user must be over eighteen to use eBay.[99] This provides a buyer with judicial recourse for a fraudulent sale.[100]

Moreover, eBay has made substantial changes to its fraud prevention as a result of losing lawsuits in France.[101] Specifically in *LVMH v. eBay*, a French trade court found that eBay was responsible for counterfeit items sold on its website by third parties.[102] The new security measures implemented by eBay as a result of these suits[103] include proactive fraud protection on types of items more frequently targeted by scammers.[104] EBay has not made a full comprehensive release on how it checks for fraudulent items, so it is difficult

ensure that the user actually owns the object of the picture. *See* Ina Steiner, *eBay Restrictions on Apple iPhone Sales Remain in Place*, AUCTIONBYTES.COM (June 29, 2007), http://www.auctionbytes.com/cab/abn/y07/m06/i29/s01 ("Sellers must comply with the following rules in order to sell iPhones after they go on sale: The listing must include a unique photograph of the item or items. The seller's User ID must be clearly displayed within the photograph . . . .").

98. How PayPal Works, PAYPAL, https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing_CommandDriven/bizui/WhatIsPayPal-outside (last visited Mar. 25, 2011) (PayPal is a method for individuals and businesses to send and receive money online).

99. *Creating a Seller's Account*, EBAY, http://pages.ebay.com/help/sell/seller_account.html (last visited Mar. 31, 2011); *Underage User Policy*, EBAY, http://pages.ebay.com/help/policies/identity-underage-users.html (last visited Mar. 31, 2011); Ben Charny, *EBay Requires New Sellers to Use PayPal or Credit Card*, MARKET PULSE (Jan. 17, 2007, 8:15 PM), http://www.marketwatch.com/story/ebay-requires-new-sellers-to-use-paypal-or-credit-card.

100. *Rules for Buyers*, EBAY, http://pages.ebay.com/help/policies/buyer-rules-overview.html (last visited Mar. 22, 2011) ("[E]ach bid you make is a binding contract to buy the item.").

101. LVMH v. eBay, Tribunal de commerce [TCP] [court of trade] Paris, June 30, 2008 (Fr.).

102. *Id.*; Deidre Woollard, *EBay Loses Big French Lawsuit*, LUXIST (June 30, 2008, 6:01 PM), http://www.luxist.com/2008/06/30/ebay-loses-big-french-lawsuit/ ("[E]Bay has asserted that they are a host in the selling process and therefore not responsible [for counterfeit items sold] but a statement from [Louis Vuitton Moet Hennessy] counters that saying that eBay is not a host but is instead a broker for these goods and therefore responsible not just for counterfeits but for all the branded goods that are sold through eBay."); Ina Steiner, *EBay Loses Hermes Counterfeiting Case*, AUCTION BYTES (June 5, 2008), http://www.auctionbytes.com/cab/abn/y08/m06/i05/s01 ("[E]Bay was convicted by a French court Wednesday of selling counterfeit goods . . . .").

103. Steiner, *supra* note 102 ("Today's court ruling [against eBay] relates to past seller verification issues. The court acknowledged that eBay subsequently addressed these issues with its enhanced anti-counterfeiting measures . . . .").

104. Rob Chesnut, *Combating Online Fraud*, EBAY (Apr. 9, 2007, 9:21 AM), http://www2.ebay.com/aw/core/200704090921122.html.

to assess the effectiveness of such safety measures.[105]

Notably though, fraud is a direct harm to eBay's business, and the measures taken against fraud are directly linked to the success of eBay as a business; a fraudulent transaction is an unsuccessful transaction. Comparatively, the harms associated with social networking websites are not as damaging to the website's business, and therefore there is less monetary incentive to address or prevent those harms.

Additionally, one of the biggest differences between social networking websites and eBay is the type of harm encountered by their users. The information a user inputs into eBay is markedly limited and different from the information a user inputs into a social networking website. On eBay, the information's focus is on the product, and on social networking websites, the information's focus is on the actual person. For instance, a user on eBay creates a username such as eBayUser77, compared with most social networking websites where a user provides and is identified by his or her actual name. On eBay, when a fraudulent, damaged, and/or mislabeled item is sold, the resulting harm is limited to financial loss, dissatisfaction with the item, and/or a trademark violation. On social networking websites, the types of harm are much more serious and much more diverse.[106] Although social networking websites may seem to be disadvantaged by the sheer volume of information, this concern is largely alleviated by the ability to automate searches and filters through algorithms and coding.[107]

IV. INEFFECTIVE SOLUTIONS ENCOURAGE DECEPTION

There have been a wide variety of proposals and attempts to limit criminal activity facilitated by online social networks. Some have worked better than others. Generally, bad ideas encourage user deception and lies, making it harder for social

105. *Id.* ("Unfortunately, it's not possible for us to give you criteria [on what kinds of listings will be impacted], because that information could be used by scammers . . . .").

106. *See* discussion *supra* Part II.D.

107. *See* MICHAEL L. RUPLY, JR., IND. UNIV., INTRODUCTION TO QUERY PROCESSING AND OPTIMIZATION (2008), *available at* http://www.cs.iusb.edu/technical_reports/TR-20080105-1.pdf ("All database systems must be able to respond to requests for information from the user . . . . Obtaining the desired information from a database system in a predictable and reliable fashion is the scientific art of *Query Processing*. Getting these results back in a timely manner deals the technique of *Query Optimization*.").

networking websites to discover and identify abuse and potentially dangerous users.

A. Banning Users

Banning IP addresses of consistent violators is, although seemingly a good idea, very ineffective and easily circumvented[108] because ISPs recycle IP address due to the nature of IPv4 and the limited number of IP addresses available.[109] Even users with broadband, who are always connected to the Internet, can still easily change their IP addresses.[110]

Recently, in response to a subpoena and increasing pressure from state attorneys general, MySpace announced that it had identified 90,000 registered sex offenders using its site.[111] The obvious choice of action taken by MySpace, and encouraged by the state attorneys general, was to remove the identified sex offenders from the site.[112] Despite appearances, this was the wrong course of action to take, because banning registered sex offenders from a website does not stop them from using another site, or from using the same website with a fake profile. MySpace may have superficially purged itself of sex offenders, but many of them migrated to Facebook.[113]

108. Adam Kalsey, *Why IP Banning Is Useless*, ADAM KALSEY (Feb. 10, 2004), http://kalsey.com/2004/02/why_ip_banning_is_useless/.

109. *See* discussion *supra* Part II.

110. *What Is the Difference Between Dynamic and Static IP Addresses?*, SPEEDGUIDE.NET, http://www.speedguide.net/faq_in_q.php?category=88&qid=137 (last visited Mar. 31, 2011) ("[Y]our IP address . . . can change any time you get disconnected, there is a power outage, ISP maintenance, etc.").

111. Press Release, Conn. Office of the Att'y Gen., CT, NC Attorneys General Say MySpace Response to Subpoena Revealed 90,000 Registered Sex Offenders with Profiles (Feb. 3, 2009), *available at* http://www.ct.gov/ag/cwp/view.asp?A=3673&Q=433228; Edith Honan, *MySpace: 90,000 Sex Offenders Removed in Two Years*, REUTERS (Feb. 3, 2009), http://www.reuters.com/article/technologyNews/idUSTRE51278C20090203.

112. *MySpace Kicks Out 90,000 Sex Offenders, Connecticut AG Says*, CNN (Feb. 4, 2009, 6:22 PM), http://www.cnn.com/2009/TECH/02/03/myspace.sex.offenders/index.html.

113. Erick Shonfeld, *Thousands of MySpace Sex Offender Refugees Found on Facebook*, TECHCRUNCH (Feb. 3, 2009), http://www.techcrunch.com/2009/02/03/thousands-of-myspace-sex-offender-refugees-found-on-facebook/; Daily Mail Reporter, *MySpace Removes 90,000 Sex Offenders . . . but Pedophiles May Be Turning to Facebook Instead*, MAILONLINE (Feb. 5, 2009, 1:48 AM), http://www.dailymail.co.uk/news/article-1135490/Myspace-removes-90-000-sex-offenders--paedophiles-turning-Facebook-instead.html.

Facebook, not wanting to be outdone by MySpace, followed suit and eliminated the registered sex offenders from its site.[114] States seem to share this mentality and are passing laws requiring sexual offenders to register any online screen names,[115] or banning them from social networking websites altogether.[116]

All of this means one of three things for MySpace and Facebook: (1) the websites evicted rehabilitated prior sex offenders,[117] (2) the websites evicted non-rehabilitated sex offenders who are now lurking on other social networking websites,[118] or (3) the websites have forced non-rehabilitated sex offenders to create fake profiles.[119] Similarly, state and local governments restrict the residency of prior sex

114. Caroline McCarthy, *Report: 5,585 Sex Offenders Purged from Facebook*, CNET NEWS (Feb. 20, 2009, 5:57 AM), http://news.cnet.com/8301-13577_3-10168255-36.html; *see* discussion *infra* Part IV (discussing alternative measures to eliminating users).

115. *Sex Offender Registries and Websites*, CYBER TELECOM, http://www.cybertelecom.org/security/child.htm (last visited Jan. 18, 2009); *Sex Offenders Must Register Online Screen Names*, N.Y. SUN, May 15, 2008, http://www.nysun.com/new-york/sex-offenders-must-register-online-screen-names/76433/.

116. Computerworld Staff, *Illinois Outlaws Sex Offenders from Using Facebook, MySpace*, NETWORK WORLD (Aug. 14, 2009, 2:00 PM), http://www.networkworld.com/news/2009/081409-illinois-outlaws-sex-offenders-from.html.

117. However rare it happens, public urination can put a person on the sex offender registry, and surely MySpace and Facebook are not trying to protect their users from the public urinators of the world. *See* Gordon Fraser, *Lawmakers: Public Urination Shouldn't Lead to Sex Offender Status*, EAGLE-TRIBUNE, Jan. 31, 2008, http://www.eagletribune.com/punewsnh/local_story_031093859.

118. Even if all social networking websites made it a policy to restrict access to registered sex offenders, that would only create a larger incentive for the offenders to create fake profiles. *See* discussion *infra* Part IV (discussing the difficulty of identifying fake profiles).

119. *See*, *e.g.*, Michael Seamark, *Paedophile Postman Used Facebook and Bebo to Groom Up to 1,000 Children for Sex*, MAILONLINE (May 28, 2010, 8:35 PM), http://www.dailymail.co.uk/news/article-1282157/Facebook-grooming-How-pervert-postman-used-site-groom-hundreds-children.html (creating at least eight fake profiles to target young children); Mark Williams-Thomas, *I Posed as a Girl of 14 Online. What Followed Will Sicken You*, MAILONLINE (March 11, 2010, 4:42 PM), http://www.dailymail.co.uk/news/article-1256793/I-posed-girl-14-online-What-followed-sicken-you.html ("The Government must provide police forces throughout Britain with the resources for covert policing, so they can lure men with fake teenage profiles before they ruin the lives of real children."); Leah Yahmshon, *How to Keep Your Kids Safe on Facebook*, PCWORLD (Sept. 30, 2010, 9:00 PM), http://www.pcworld.com/article/206683/how_to_keep_your_kids_safe_on_facebook.html (a registered sex offender created a fake profile of a seventeen-year-old to gain his victim's trust, who he subsequently kidnapped, raped, and murdered).

offenders,[120] but measures that socially isolate sex offenders are actually detrimental to the public's safety because they fuel sex offenders' cycles of abuse and create a false sense of security.[121] Although the numbers look good for MySpace and Facebook, the websites are probably less safe. Therefore, despite initial reactions, the best course of action would have been to keep the sex offenders on MySpace and monitor their behavior with police assistance.

While 90,000 profiles is a substantial number to monitor, it is harder to weed out 90,000 fake profiles. It can be very difficult to identify a fake profile, even using an algorithm, unless there are identity cross-check requirements for sign-up, such as providing a credit card.[122] Additionally, even assuming police can identify a fake profile, the only link from that fake profile to the real user is the IP address.[123] If the

120. *E.g.*, ALA. CODE § 15-20-26 (2010) (restricts sex offenders from living or accepting employment within 2000 feet of school or daycare); ARK. CODE ANN. § 5-14-128 (2010) (restricts certain level sex offenders from living within 2000 feet of school or daycare); CAL. PENAL CODE § 3003 (West 2010); FLA. STAT. ANN. § 947.1405(7)(a)(2) (West 2010) (restricts certain sex offenders from living within 1000 feet of a school, day care, park, playground); TENN. CODE ANN. § 40-39-111 (2010). *See also* Wendy Koch, *Homeless Sex Offenders' Isolation Can Add to Problem*, USA TODAY, Nov. 18, 2007, http://www.usatoday.com/news/nation/2007-11-18-InsideSexOffender_N.htm ("At least twenty-seven states and hundreds of cities have passed laws in the past decade to restrict where sex offenders live.").

121. Koch, *supra* note 120 ("The laws don't necessarily keep sex offenders away from kids, says [Jo Ellyn Rackleff, spokeswoman for the Florida Department of Corrections]. 'What people don't realize is these offenders are in our communities,' riding buses and walking around, she says. 'It's a waste of resources to check where they're sleeping,' says Corwin Ritchie, executive director of the Iowa County Attorneys Association. He says sex offenders may sleep in one place and spend their days elsewhere. He says it is better to monitor where they go."); *Our Mission and Deeper Purpose*, Post to *Sex Offender Reports, Charts and Other Papers*, SEX OFFENDER RES., http://sexoffender-reports.blogspot.com/2009/04/our-mission.html (last visited Mar. 2, 2011) ("Society in general, buried in hatred, is unaware of what is happening in the name of public safety. The hysteria caused by misinformation about sex offenders is fueling vigilantism, harassment, protests, media frenzy, and the feel-good legislation. This drives the untreated sex offender underground into deeper isolation and triggers cycles of abuse. Society feels it should, divide and isolate themselves from sex offenders. However, that act perpetuates the abuse cycle.").

122. *See generally* CATFISH (Rogue Pictures 2010) (documenting the accidental uncovering of a network of fake profiles fabricated by one woman).

123. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 146–47 (2007), *available at* http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm (discussing the ability of ISPs using IP addresses to trace anonymous Internet users). *See* Mark Tighe, *Biker Sues Bebo over Fake Profile*, SUNDAY TIMES, Feb. 14, 2010, http://www.timesonline.co.uk/tol/news/world/ireland/article7026292.ece ("[The police] were asked to investigate the fake

real user is accessing the Internet through someone else's Internet connection (and corresponding IP address), the fake profile will appear to belong to the owner of that Internet connection.[124] Social networking websites were in a unique position to help catch potential repeat offenders and make the Internet safer. For instance, the social networking websites could have been used to check compliance with required online identity registration for convicted sex offenders, and verify the accuracy of a user's purported age.[125] Even if the registered sex offenders had fake profiles before getting evicted from their real profiles, those fake profiles would still exist on the website. The purpose of keeping sex offenders on the website is to prevent the creation of fake profiles, and to prevent future harm.

B. Age Requirements

Age verification should be used on certain websites, but not when lying so easily circumvents it. Specifically, minors should be prohibited from using any of the adult dating websites now available.[126] SexSearch, a social network for people looking for sex, received media attention when one of its users was charged with statutory rape of a fourteen-year-

profile and it is understood Bebo gave officers the IP addresses used to set it up. The address indicated the culprit was an Eircom customer in south Dublin.").

124. Rod Dixon, *White Nowhere to Hide: Workers Are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1, 41 n.96 (1999) ("Not only does every computer leave a trail of its IP address everywhere it goes on the Internet, but snifer programs, savvy computer users, untrustworthy computer hackers, website owners, and just about any employer can, with little difficulty, surreptitiously grab a computer's IP address."); *Securing Your Wireless Network and Why You Should Do It Now*, BULLDOG DATA SERVICES (Sept. 3, 2009), http://bulldogdata.com/securing-your-wireless-network-and-why-you-should-do-it-now ("Since the intruder is on your private network, any traffic between him and the Internet will appear to be coming from the public IP address the ISP assigned to the you. The ISP has no idea how many computers are behind the gateway, who they belong to, and what they are used for. If the criminal activity is discovered and investigated, the origin of the attack will be traced back to the your broadband account.").

125. Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (enacted) (requiring convicted sex offenders to register online identifiers).

126. *E.g.*, HORNYMATCHES, http://www.hornymatches.com/ (last visited Apr. 14, 2011); NAUGHTYCONNECT, http://www.naughtyconnect.com/ (last visited Apr. 14, 2011); ADULTFRIENDFINDER, http://adultfriendfinder.com/ (last visited Apr. 14, 2011); ADULTRATERS, http://www.adultraters.com/ (last visited Apr. 14, 2011); SEXSEARCH, www.sexsearch.com (last visited Apr. 14, 2011).

old minor who falsely claimed to be eighteen years old.[127] But finding shelter under the CDA, SexSearch was not held liable for the user's fraudulent statements regarding her age.[128]

Adult dating websites are in a better position to verify users' ages because the minimum age requirement is eighteen and not thirteen. Although this measure has been suggested for all social networking websites, requiring a credit card for site membership is better suited to adult dating websites because the minimum age for credit card ownership is already eighteen.[129] The website could require a prospective member's name to appear as it does on his/her credit card and charge a nominal fee to prevent minors from covertly using a parent's credit card.[130] This measure by itself, however, should not be sufficient to shield the website from all potential liability.[131]

Minimum age requirements are less practical for general social networking websites. Requiring a minimum age, below eighteen years old, is ineffective because age verification for minors is so difficult.[132] Minors lack a reliable source, such as a credit card, that can be used to cross-reference their information.[133] As a result, the current system to verify a user's age employed by most social networking websites is ineffective. Of the ten most popular social networking websites,[134] two do not have a minimum age requirement.[135]

127. Austin Modine, *SexSearch Not Responsible for Underage Hookup (Again)*, REGISTER (Dec. 31, 2008, 9:29 PM), http://www.theregister.co.uk/2008/12/31/sexsearch_v_johndoe_appeal_dismissed/.

128. Doe v. SexSearch.com, 502 F. Supp. 2d 719, 737 (N.D. Ohio 2007), *aff'd*, 2008 WL 5396830 (6th Cir. 2008) (affirming the lower court on alternative grounds without reading the issue of whether SexSearch was immune from liability under section 230).

129. Susan Hanley Duncan, *MySpace Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social-Networking Sites*, 96 KY. L.J. 527, 565 (2008).

130. *Id.*

131. *See* discussion *infra* Part IV.

132. Adam Thierer, et al., Panel at a Progress and Freedom Foundation Congressional Seminar: Age Verification for Social Networking Sites: Is It Possible? Is It Desirable?, at 5–6 (Mar. 23, 2007), *available at* http://www.pff.org/issues-pubs/pops/pop14.8ageverificationtranscript.pdf (expressing concerns that it is not possible and that the current sites that do have age verification are misleading in their security).

133. *Id.*

134. Andy Kazeniac, *Social Networks: Facebook Takes over Top Spot, Twitter Climbs,* COMPETE PULSE (Feb. 9, 2009, 2:01 PM), http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/.

135. Websites with a minimum age requirement include: *Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited Apr. 14, 2011); MYSPACE,

A child lying about his or her age to gain access to a social networking website may be seemingly innocuous but could have serious implications. Currently, when a ten-year-old girl is rejected from a social networking site due to a minimum age requirement, she goes right back onto the site and this time under "age" she puts thirteen instead of ten.[136] Now the social networking website has a ten-year-old user it thinks is thirteen years old.[137] While seemingly trivial, age can become a serious issue. For instance, assume a fifteen-year-old girl has lied about her age in the past so that her profile now claims she is eighteen, and that she sends naked pictures of herself to a nineteen-year-old through the social networking website. Now the website has unknowingly facilitated child pornography.[138] Of course if she is ever caught by the police, that fifteen-year-old girl may be charged with possession and distribution of child pornography,[139] while the social networking website would remain immune from liability.

Current legislation regarding minimum age requirements is ineffective because it is easily circumvented by website users. Social networking websites are not entirely to blame for setting minimum age requirements. The Children's

http://faq.myspace.com/app/answers/detail/a_id/237 (search "How can we help you?" for "minimum age requirement"; then follow "Minimum age for MySpace" hyperlink) (last visited Apr. 14, 2011); *Flixster Copyright Policy*, FLIXSTER, http://www.flixster.com/misc/copyrightprivacyterms (last visited Apr. 14, 2011); *User Agreement*, LINKEDIN, http://www.linkedin.com/static?key=user_agreement (last visited Apr. 14, 2011); *Terms of Service*, TAGGED, http://www.tagged.com/terms_of_service.html (last visited Apr. 14, 2011); *Terms of Service*, CLASSMATES, http://www.classmates.com/cmo/reg/terms.jsp (last visited Apr. 14, 2011); *Terms of Service*, MYYEARBOOK, http://www.myyearbook.com/terms.php (last visited Apr. 14, 2011). Sites that do not have a minimum age requirement include: *Terms of Service*, LIVEJOURNAL, http://www.livejournal.com/legal/tos.bml (last visited Apr. 14, 2011); *Terms of Service*, TWITTER, https://twitter.com/tos (last visited Apr. 14, 2011).

136. John Carvel, *Facebook: Children Evade Social Websites' Age Limits*, GUARDIAN.CO.UK (Aug. 7, 2008), http://www.guardian.co.uk/technology/2008/aug/07/socialnetworking.facebook.

137. *See* discussion *supra* Part II.

138. Dave Parrack, *Self-Taken Naked Photos of Teenagers Classified as Child Pornography*, TECH.BLORGE (Mar. 28, 2009), http://tech.blorge.com/Structure:/2009/03/28/self-taken-naked-photos-of-teenagers-classified-as-child-pornography/.

139. *See id.*; BJ Lutz, *Boy, Girl Charged with Child Porn*, NBC CHICAGO (Jan. 29, 2010, 9:05 AM), http://www.nbcchicago.com/news/local-beat/indiana-middle-school-sexting-82949612.html; Kim Zetter, *Child Porn Laws Used Against Kids Who Photograph Themselves*, WIRED (Jan. 15, 2009, 9:50 AM), http://www.wired.com/threatlevel/2009/01/kids/; *High Schoolers Accused of Sending Naked Pictures to Each Other*, WPXI.COM (Jan. 13, 2009), http://www.wpxi.com/news/18469160/detail.html.

Online Privacy Protection Act requires websites to take additional steps, such as seeking parental permission, before a child's personal information may be collected or subsequently disseminated.[140] But social networking websites easily sidestep this issue by requiring their users to be at least thirteen years old, having no effective means to verify their users' ages, and then subsequently enjoying full immunity from any resulting harm. The current age verification system employed by most social networking websites is too easily circumvented, and, as a result, either needs to be completely abandoned or completely revamped.[141]

V. EFFECTIVE ACTUAL AND POTENTIAL IMPROVEMENTS TO WEBSITE SECURITY AND SAFETY

Implementing effective solutions will encourage honesty among social network users. Social networking websites should seek to achieve security through profile tracking and cross-reference, IP tracking, and simple observation. Currently, social networking websites are not taking these steps to protect their users, and they have little, if any, incentive to do so because Congress and the courts have afforded them with such broad immunity.

A. Age Verification on Second Life

Second Life is an online virtual world, where the "virtual environment mimics the real world through an interactive body of residents called avatars."[142] After a scandal involving "depictions of or engagement in sexualized conduct with avatars that resemble children,"[143] Second Life banned that behavior and then created a community for minors called Teen Second Life.[144] Teen Second Life is open only to teens

140. 15 U.S.C. §§ 6501–6506 (2010).

141. *See* discussion *infra* Part V.

142. Melissa Ung, *Trademark Law and the Repercussions of Virtual Property (IRL)*, 17 COMMLAW CONSPECTUS 679, 680 (2009).

143. Kend Linden, *Clarification of Policy Disallowing "Ageplay"*, SECOND LIFE (Nov. 14, 2007, 12:10 AM), http://community.secondlife.com/t5/Features/Clarification-of-Policy-Disallowing-Ageplay/ba-p/599068.

144. Jacqui Cheng, *Second Life Now Like Real Life: Show Me Yer ID, Kid*, ARS TECHNICA (May 10, 2007, 12:43 AM), http://arstechnica.com/gaming/news/2007/05/second-life-to-segregate-users-by-age.ars.

between the ages of thirteen and seventeen.[145] The only adults allowed in Teen Second Life are members of the parent company, Linden Lab, who are "clearly identified as a 'Linden,'"[146] as well as "[e]ducators and youth non-profit organizations."[147] Any adult who is not a Linden Lab employee must go through a criminal and background check and is confined to certain areas of the website.[148]

As a means of age verification, Teen Second Life requires that a parent create his or her child's account so that it is tied to a cell phone account in their child's name or their child's PayPal student account.[149] Parents can set up a PayPal student account by providing their child's full legal name and their date of birth.[150] The student account is linked to the parent's banking account, but the student account has spending limits and parental controls.[151]

The solutions implemented by Second Life are all feasible steps for other social networking websites to take. It is possible that websites have not attempted those solutions because they are concerned that such protections would substantially decrease traffic and membership and in turn, decrease revenue. Profit maximization, however, cannot be the standard for determining whether to impose regulations. Movie theaters have maximum occupant capacities under fire code regulations,[152] businesses are required to have sprinkler systems,[153] and buildings are constructed to meet government safety specifications.[154] General societal norms mandate

145. *What Is Teen Second Life?*, TEEN SECOND LIFE, http://teen.secondlife.com/whatis (last visited Mar. 2, 2011).

146. Linda Zimmer, *A Second Life/Second Life Teen Primer for Parents*, WEBWISEKIDS, http://www.drrobertland.com/storage/second_life_article.pdf (last visited Apr. 1, 2011).

147. *Id.*

148. *Id.*

149. *Id.*; Student Accounts, PAYPAL, https://www.paypal.com/student/ (last visited Mar. 2, 2011).

150. Student Accounts, *supra* note 149.

151. *Id.*

152. SPARKS, NEV. MUN. CODE § 5.75.100 (2010), *available at* http://cityofsparks.us/governing/muni_code/Title_5/75/100.html.

153. RUSSELL P. FLEMING, NAT'L FIRE SPRINKLER ASS'N, THE FIRE SPRINKLER SITUATION IN THE UNITED STATES 1 (2002), *available at* www.sprinklerworld.org/vds.doc ("Originally installed to reduce property insurance premiums, fire sprinkler systems are now installed mainly to meet the requirements of building codes for new construction.").

154. *See* BUREAU OF LABOR STATISTICS, OCCUPATIONAL OUTLOOK HANDBOOK

corporations maintain a balance between profits and safety, but social networking websites are oddly excluded from any substantial and meaningful imposition of safety requirements.

B. MySpace Headed in the Right Direction

After a multitude of state attorneys general put pressure on MySpace by threatening litigation and investigation,[155] the website took some action towards implementing greater safety features.[156] Specifically, MySpace started development of Zephyr, a parental-notification software used to monitor a child's MySpace account.[157] Under Zephyr, parents would not have access to the content on their children's MySpace page, but would be able to establish whether a child has a MySpace profile and what age or address the child lists on that profile.[158] This is a good solution because it encourages active parenting and provides a practical means for parents to obtain important basic information about their children's account without completely invading their privacy. But the effectiveness of this type of software is questionable because the number of parents that actually use it is unclear, and whether it really prevents sexual abuse or other problems associated with social networking is unknown. Since MySpace's announcement, IMSafer beat Zephyr to the market[159] and Zephyr seems to have been abandoned by

(2010).

155. Kristen J. Matthews, *Social Networking Sites Feel the Heat from Law Enforcement,* Post to *Privacy Law Blog*, PROSKAUER (Oct. 17, 2007), http://privacylaw.proskauer.com/2007/10/articles/children-online-privacy-prote/social-networking-sites-feel-the-heat-from-law-enforcement/.

156. Caroline McCarthy, *MySpace Agrees to Social-Networking Safety Plan*, CNET NEWS (Jan. 14, 2008, 9:51 AM), http://news.cnet.com/8301-13577_3-9849909-36.html ("MySpace has pledged to work with the attorneys general on a set of principles to combat harmful material on social-networking sites (pornography, harassment, cyberbullying, and identity theft, among other issues), better educate parents and schools about online threats, cooperate with law enforcement officials around the country, as well as develop new technology for age and identity verification on social-networking sites.").

157. Caroline McCarthy, *MySpace Developing Parental-Notification Software*, CNET NEWS (Jan. 17, 2009, 9:22 AM), http://news.cnet.com/MySpace-developing-parental-notification-software/2100-1032_3-6150824.html.

158. *Id.*

159. IMSAFER, http://www.imsafer.com (last visited Jun. 3, 2011); Kristen Nicole, *IMSafer Beats MySpace Zephyr to the Punch*, MASHABLE (Apr. 11, 2007), http://mashable.com/2007/04/11/imsafer-myspace-zephyr/

MySpace.

Another safeguard MySpace implemented to limit the contact of minors with potential predators is allowing them to become friends only with people they actually know.[160] Now users over eighteen are required to know the full name or e-mail of a user fifteen years old and younger before contacting them at all.[161] But this implementation is still insufficient. First, it is not effective for young children who inflate their age in their profile.[162] Second, it may encourage sexual predators to lower their own age in their profile in order to avoid this limitation.

A better implementation is to allow children fifteen years old and younger to search, and be searchable by, only full names, regardless of the age of the person conducting the search. This way, when anyone over eighteen or a potential sexual predator searches for a specific name, his search results only reveal individuals over the age of eighteen. This also prevents sexual predators that misrepresent their age from contacting children because all users, regardless of age, would only be able to search for children by their full names. This is not a complete solution to the problem because it does not prevent contact if the minor lies about his or her age, but it would provide protection for those users who do not lie about their age.

C. Steps Not Taken by Social Networking Websites to Report Abuse

Many social networking websites have some sort of scheme in place to report abuse, but the comprehensiveness of these schemes vary.[163] Facebook and MySpace both have a system

160. Jai Lynn Yang, *Can This Man Make MySpace Safe for Kids?*, FORTUNE (June 30, 2006, 7:24 AM), http://money.cnn.com/magazines/fortune/fortune_archive/2006/07/10/8380854/index.htm.

161. *Id.*

162. *Id.*

163. Sean Poulter, *Children 'Exposed to Pornography, Prostitution and Drugs on Twitter*,, MAILONLINE (Feb. 26, 2009, 12:55 PM), http://www.dailymail.co.uk/news/article-1156136/Children-exposed-pornography-prostitution-drugs-Twitter.html ("[Twitter] state[s] users must be [thirteen] or over, but it doesn't offer a 'report abuse' button or explicit ways to flag offensive material or monitor sexually explicit and racist behaviour [sic] and links to adult sites."); *Community Standards*, TEEN SECOND LIFE, http://teen.secondlife.com/corporate/cs.php (last visited Mar. 2, 2011).

to report photos or videos that violate the websites' terms of use, including harassing material.[164] On Facebook, the user can choose from one of several categories to explain why the photo or video is abusive.[165] Although Bebo has agreed,[166] both Facebook and MySpace have refused to implement a "CEOP report" button, which is provided free by the Child Exploitation and Online Protection Centre of Britain (CEOP),[167] presumably because it would then lose advertising space.[168] The CEOP report button seems to be an effective step in Internet user protection[169] because a click of the button provides users with instant contact with counselors and law enforcement officers for advice and assistance concerning abusive content—such as posts or pictures—or abusive users.[170] In response, Facebook said that it had tested similar systems and found that such systems were "ineffective and actually reduced the reporting of abuse, and that as an international site, it preferred to have its own global

164. *See* Mercedes Bunz, *How Easy Is It to Report Abuse on Facebook?*, GUARDIAN.CO.UK (Nov. 18, 2009, 3:44 PM), http://www.guardian.co.uk/media/2009/nov/18/facebook-reporting-abuse; *Report Abuse*, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=help.reportabuse (last visited March 22, 2011).

165. Jessica Ghastin, *Responding to Abuse Reports More Effectively*, FACEBOOK BLOG (Oct. 14, 2009, 1:43 PM) http://blog.facebook.com/blog.php?post=144628037130 ("[W]hen reporting an offensive photo, you can select from the following reasons why it may violate our Statement of Rights and Responsibilities: nudity or pornography, drug use, excessive gore or violence, attacks individual or group, advertisement or spam or infringes on your intellectual property. Keep in mind that we won't remove a photo or video just because it's unflattering.").

166. *See* BEBO, www.bebo.com (last visited Apr. 1, 2011) (a general social networking website); Nic Fleming, *Social Networking Sites: Why No Abuse Report Button?*, NEW SCIENTIST (Nov. 18, 2009, 1:43 AM), http://www.newscientist.com/blogs/shortsharpscience/2009/11/social-networking-sites-why-no.html.

167. *Id.*; *see generally* CHILD EXPLOITATION & ONLINE PROT. CENTRE, http://www.ceop.police.uk/ (last visited Mar. 2, 2011).

168. Adam Fresco, *Networking Sites Fail to Protect Children from Abuse, Says CEOP Head*, TIMES ONLINE (Nov. 18, 2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6920945.ece.

169. CHILD EXPLOITATION & ONLINE PROT. CENTRE, CEOP ANNUAL REVIEW 9 (2009). ("Since CEOP launched in April 2006, more than 340 children have been safeguarded, over 700 offenders apprehended and over four million children educated, empowered and protected by our Thinkuknow safety training . . . .").

170. *Id.*; *More Than 8 Million Young Users Get Added Safety Support as Bebo Adopts 'CEOP Report' Button*, CEOP (Nov. 17, 2009), http://www.ceop.gov.uk/mediacentre/pressreleases/2009/ceop_17112009.asp ("Around 10,000 people a month are already pressing the button for advice and help across other online services.").

system."[171] While Facebook currently employs an improved reporting system,[172] it is worthwhile to implement a report abuse button for easy access to professional help and free third party support, even if used sporadically by Facebook users.

D. Use of the Inherent Nature of Social Networking Websites

Social networking websites should take advantage of the ease of aggregating information on the Internet. The purpose of social networking websites is to "connect and share with the people in your life."[173] Social networking websites should cross-reference information posted by the user in order to check a profile's validity, or to raise red flags. Social networking website database queries are easy to implement,[174] so social networking websites are capable of taking a proactive approach to Internet safety. For instance, age verification could be assisted by cross-referencing information provided by the user. If a girl claims to be eighteen years old in 2010, but is a member of the network "Suburban High School 2014," she is probably younger. If someone claims to be fifteen, but has a graduate degree, it should raise a red flag. Automated queries monitoring behavior, in conjunction with age verification cross-referencing techniques, could help prevent the sexual abuse of minors by preventing contact with suspicious adults. A social networking website is capable of checking if a forty-year-old man is attempting to friend a group of unrelated fifteen-year-olds,[175] and should be required to bring it to the attention of

171. Fleming, *supra* note 166.

172. Facebook's prior implementation required that a user remove the alleged violator as a friend before reporting the abuse, thereby ruining anonymity and any follow up to ensure compliance. *See* Sweta, *Facebook Makes 'Report Abuse' More Efficient*, GLOBAL THOUGHTZ (Oct. 15, 2009), http://socialmedia.globalthoughtz.com/index.php/facebook-makes-report-abuse-more-efficient/ ("[T]here is no report link on a person's profile anymore in a shocking attempt to claim that Facebook has less reports than other users." (quoting response by David)).

173. *See* FACEBOOK, http://www.facebook.com/ (last visited Mar. 2, 2011).

174. *See, e.g.*, *SQL Wildcards*, W3SCHOOLS.COM, http://www.w3schools.com/SQL/sql_wildcards.asp (last visited Mar. 2, 2011) (explaining how to code for a database query).

175. *See, e.g.*, Tiffany, Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 477 (S.D.N.Y. 2008) ("The fraud engine uses rules and complex models that automatically search for activity that violates eBay policies.").

law enforcement officials.[176] Additionally, Facebook and other major social networks with consistently large traffic often use data gathered from users to increase usage and thereby increase revenue.[177] These same websites could easily discover trends, associations, and correlations between content and reports of abuse to prevent future harm.

Many societal problems finding their way onto social networks may be deterred by developing a point system to "wall" posts and profile content. Such a point system would enable a social networking website to monitor, through automated queries, the frequency of derogatory or offensive language used by a user or directed at a specific user. The website is also capable of checking posts and profile content for words commonly associated with gangs, drugs, or sex trafficking. Police intervention or assistance may be necessary to achieve this goal, as the police could provide the proper keywords from their own experience and expertise. For those with concerns that the average criminal is too intelligent to put obvious and incriminating information on a social networking websites, rest assured that he is not.[178] For those concerned that intelligent people will easily circumvent these kinds of security protections, even intelligent cyber-criminals are often, and sometimes easily, caught.[179] Even so,

176. *See, e.g.*, 18 U.S.C.A. § 2258A(a) (2008) (requiring electronic communication service providers and remote computing service providers to report any material related to child pornography); Doe v. XYC Corp., 887 A.2d 1156, 1166–69 (N.J. Super. Ct. App. Div. 2005) (holding that an employer had a duty to investigate employee's Internet use after being put on notice that he was visiting child pornography websites at work); *Child Pornography Reporting Requirements (ISPs and IT Workers)*, NCSL (Sept. 2010), http://www.ncsl.org/default.aspx?tabid=13460 (noting that seven states require and the federal government require computer technicians and ISPs to report child pornography if they encounter it).

177. *Data, Data Everywhere*, ECONOMIST, Feb. 25, 2010, http://www.economist.com/node/15557443 ("'Looking at large data sets and making inferences about what goes together is advancing more rapidly than expected.' . . . Facebook regularly examines its huge databases to boost usage.").

178. Melissa Grace & Wil Cruz, *MySpace Brags Spur Gang Busts of Crips, Bloods Who Terrorized Manhattan Housing Project*, DAILY NEWS, Jan. 14, 2010, http://www.nydailynews.com/news/ny_crime/2010/01/14/2010-01-14_myspace_brags_spur_gang_busts.html ("Crips and Bloods drug dealers who terrorized a Manhattan housing project and boasted of their gang ties on MySpace were busted Wednesday . . . .").

179. Andrew Scott, *Sex Sting in Poconos Nets Former Chief U.N. Weapons Inspector*, POCONO REC., Jan. 14, 2010, http://www.poconorecord.com/apps/pbcs.dll/article?AID=/20100114/NEWS/1140319 (Former chief U.N. inspector is accused of engaging in sexual conversation and showing himself masturbating on a webcam to

the aforementioned measures are not anticipated to completely solve the problems on social networking websites, only to significantly reduce them.

VI. LEGISLATION IS NECESSARY

Significant substantial change in the safety of social networking websites requires a change in legislation or in judicial interpretation of the scope of section 230.[180] Social networking websites have little, if any, incentive to implement measures that might decrease traffic or revenue. Even now, social networking websites may not be implementing effective protective measures due to the amount of traffic or revenue they may lose as a result. Legislation, however, would level the playing field by requiring all social networking websites to meet certain minimum safety requirements. This way, if MySpace implements a system that requires parental consent to open an account, either through phone number registration or a PayPal account, the website does not have to worry that implementing this safety measure may adversely affect it by shifting potential users to Facebook or Bebo.

Congress should either decrease the immunity currently extended to social networking websites or impose minimum safety requirements in exchange for limited liability protection. New Jersey currently has pending legislation that would impose certain safety requirements on social networking websites.[181] Although state legislatures, such as

what he thought was a fifteen-year-old girl in an Internet chat room, but was actually an undercover officer. He had been previously charged in 2001 with "attempted child endangerment after arranging to meet what he thought was a sixteen-year-old girl," but was actually an undercover policewoman).

180. McCarthy, *supra* note 156 (explaining that under pressure of the attorneys general, MySpace agreed to "an extensive new plan for ensuring the safety of minors on the Internet." The new plan consists of MySpace's chief security officer and the attorneys general of 49 total U.S. states. "Texas Attorney General Greg Abbott said . . . that his office declined to participate because he didn't consider the proposed safety measures to be strong enough.").

181. Social Networking Safety Act, 2009 N.J. Laws A-3757, *available at* http://www.njleg.state.nj.us/2008/Bills/A4000/3757_R1.HTM. *See* Grayson Barber, *A "Social Networking Safety Act"*, FREEDOM TO TINKER (Mar. 25, 2009, 2:44 PM), http://www.freedom-to-tinker.com/blog/grayson/social-networking-safety-act ("The bill requires social network providers to design their user interfaces with icons that will allow customers to report 'sexually offensive' or 'harassing communications.' . . . Moreover, the social network provider must investigate complaints, call the police when

New Jersey,[182] may be acting to prevent harm, the harms associated with social networks are on a national scale, and require national coordination.[183]

Moreover, Congress should pass legislation that forces social networking websites to work in greater collaboration with law enforcement in order to ensure a safer community for adults and children alike.[184] Regulations should dictate minimum requirements for a social networking website's abuse reporting system. Social networking websites should not, however, be liable for any harm that results from the good faith operation of the resulting *heightened* abuse reporting system. Social networking websites are not able to avoid every harm a user experiences, but they should be required to take steps to ensure some acceptable level of safety and prevention.

Any legislation that passes has to be reasonably flexible in the degree of requirements and liability it would impose on social networking websites, otherwise social networking websites may remove users who were not engaged in offensive activity or for content that was not illegal out of fear of liability.[185] Additionally, requiring websites to implement certain kinds of safety measures may raise First Amendment

'appropriate' and banish offenders . . . . Finally, if the social network provider fails to take action, it can be sued for consumer fraud.").

182. Interestingly, the New Jersey bill would give social network providers some force by allowing them to "sue customers who post 'sexually offensive' or 'harassing' communications." Barber, *supra* note 181.

183. Any federal or state legislation, however, would have to be consistent with section 230 of the Communications Decency Act to avoid preemption, which is admittedly not an insubstantial hurdle. *See* U.S. CONST. art. VI, § 2; 47 U.S.C. § 230(e)(3) (2006) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section.").

184. Declan McCullagh, *Congress Targets Social-Networking Sites*, CNET NEWS (June 29, 2006, 11:38 AM), http://news.cnet.com/Congress-targets-social-networking-sites/2100-1028_3-6089574.html (proposed Congressional legislation that would have require social networking websites to retain activity logs to aid in criminal investigations); Declan McCullagh, *Bill Proposes ISPs, Wi-Fi Keep Logs for Police*, CNET NEWS (Feb. 19, 2009, 10:45 PM), http://news.cnet.com/8301-13578_3-10168114-38.html ("Republicans . . . called for a sweeping new federal law that would require all Internet providers and operators of millions of Wi-Fi access points . . . to keep records about users for two years to aid police investigations.").

185. Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 104–05 (2007) ("The overall effect is a set of "safe harbors" that provides something less than perfect safety for intermediaries, and that gives intermediaries incentives to take down any doubtful content as soon as they receive a complaint about it.").

concerns, such as overbreadth.[186] For instance, legislation that requires instant messaging filters to block certain words may be overbroad because it may filter out potentially offensive words that are not used in an abusive context.[187] As such, Congress must carefully craft the legislation so as to avoid constitutional concerns while also successfully protecting the users of social networking websites.

CONCLUSION

Ten years ago, social networking websites may not have had the technology or the resources to implement effective safety measures and prevent criminal actions of its users. In the last ten years, however, technology has progressed, and social networking websites now have the means, but not the will to implement effective change.[188] The number of users of social networking websites continues to increase, and as a result the number of victims of crimes facilitated by these websites, specifically, the cyberbullying and sexual abuse of minors. Congress needs to recognize this technological progress and the increased dangers associated with social networking websites, and pass legislation to force social networks to implement more effective safety measures.

186. *See* Ashcroft v. Am. Civil Liberties Union, 542 U.S. 656, 668–69 (2004) (finding unconstitutional a law requiring pornographic websites to use credit card verification to confirm a viewer's age because private blocking or filtering technology provides a less restrictive means); United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 804 (2000) (finding unconstitutional a law that prevents cable television operators from showing pornographic programs during the day because private blocking technology provided a less restrictive means).

187. For instance, legislation that requires instant messaging filters to block certain words may be overbroad because it may filter out potentially offensive words that are not used in an abusive context. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 863–64 (1997) (finding that the Communications Decency Act's provisions attempting to regulate indecency were over inclusive because they criminalized unprotected sexually explicit indecent speech as well as legitimate protected speech).

188. McCarthy, *supra* note 156 ("[MySpace] acknowledged that law enforcement officials still don't see eye-to-eye with social-networking sites on a variety of issues, namely the feasibility of identity and age verification. The attorneys general believe it's technologically possible; [MySpace's chief security officer] and the rest of MySpace say it needs more development.").