

2011

Social Networking Website Liability for the Illegal Actions of Its Users

Joseph Monaghan
Seton Hall Law

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Recommended Citation

Monaghan, Joseph (2011) "Social Networking Websites' Liability for User Illegality," *Seton Hall Journal of Sports and Entertainment Law*: Vol. 21: Iss. 2, Article 6. Available at: http://erepository.law.shu.edu/sports_entertainment/vol21/iss2/6

Social Networking Website Liability for the Illegal Actions of Its Users

By Joseph Monaghan

Part I: Introduction

The purpose of this article is to examine social networking sites' liability for the criminal actions of its users beyond copyright infringement. Specifically, the comment will illustrate that social networking websites are capable of providing more effective protection but have no incentive to do so because of the broad immunity granted to them through a combination of the Communications Decency Act and judicial interpretation of that Act. Therefore, legislation and increased liability is needed to bring about effective changes.

Part II provides necessary technical information which will be referenced and incorporated throughout the article. It also discusses necessary background on the origins of website immunity granted by Congress in section 230 of the Communications Decency Act and its expansion through judicial interpretation.

Part III discusses some of the societal problems associated with and facilitated by social networking websites, including sexual abuse, cyberbullying, and online gang activity. Part III also briefly discusses why social networking websites should be subject to increased liability over other websites.

Part IV discusses some currently implemented but ineffective solutions used by social networking websites such as age verification and banning of registered sex offenders. Part V discusses more effective solutions, some of which are being implemented by MySpace. Part V also discusses other possible solutions that have not been implemented at all. Part VI discusses why legislation is necessary to bring about effective security changes on social networking websites.

Part II: History and Context

A. Technical Background

An Internet Service Provider ("ISP") is a company that offers its customers access to the Internet (e.g. AT&T, Comcast, Sprint).¹ Basically, ISPs provide the "pipes" that the Internet travels through. Courts and academics may erroneously use the term ISP to cover websites as well. An Internet Content Provider ("ICP") is a party that provides or organizes or filters information on the Internet (Google, Amazon, Yahoo, Wikipedia, Facebook, MySpace). This is an important distinction because this paper is limited to increasing ICP liability, not ISP (and even then only for social networking websites, not for all websites). Part of the reason for increasing ICP liability, as explained below, is that ICPs are in a better position to monitor relationships among online identities and IP addresses.

An IP address is short for Internet Protocol address, and is vital in the composition and function of the Internet.² IP addresses are created and coordinated by Internet Corporation for Assigned Names and Numbers ("ICANN") and Internet Assigned Numbers Authority

¹ Boutell.com, *WWW FAQs: What is an ISP?* (Dec. 6, 2007), <http://www.boutell.com/newfaq/definitions/isp.html>.

² What Is My IP, *What is an IP Address*, <http://www.whatismyip.com/faq/what-is-an-ip-address.asp>.

(“IANA”).³ Under the control and supervision of ICANN,⁴ IANA distributes IP addresses to five Regional Internet Registries (“RIR”) that distribute IP addresses to ISPs in their specific geographical area.⁵ ISPs then assign an IP address to a device, usually a modem.⁶ If the modem is connected to a router, all of the devices connecting to the Internet through that modem share the same IP address.⁷

However, the IP address of a residential Internet connection (as well as some businesses and institutions) is not static.⁸ If device 1 disconnects, the ISP may reassign that IP address to device 2, and then assign device 1 a new IP address when it reconnects.⁹ This is why IP addresses have limited utility in tracking someone’s identity.¹⁰ The reason that ISPs recycle IP addresses is that there are not enough IP addresses to assign each device a different IP address.¹¹

The system currently used is IPv4, and provides 2^{32} (4.294×10^9) unique IP addresses.¹² However, ICANN is running out of IP addresses to distribute¹³ and is introducing a new system called IPv6, which provides 2^{128} (3.403×10^{38}) unique IP addresses.¹⁴ While computers are currently being built that incorporate IPv6 compatibility, very few use it.¹⁵ This means that monitoring capabilities and Internet security may change drastically with the new system.¹⁶

³ See Internet Corporation for Assigned Names and Numbers, <http://www.icann.org/>.

⁴ Contract Between ICANN and the United States Government for Performance of the IANA Function, Mar. 17, 2003, available at <http://www.icann.org/en/general/iana-contract-17mar03.htm>.

⁵ Kim Davies, *An Introduction to IANA*, Sept. 2008, available at <http://www.iana.org/about/presentations/davies-atlarge-iana101-080929.pdf>.

⁶ Speedguide.net, *What is the difference between dynamic and static IP addresses?*, http://www.speedguide.net/faq_in_q.php?category=88&qid=137 (last visited Jan. 19, 2010).

⁷ *Id.* (“The limited IP address space is one of the reasons for the wide use of NAT routers . . .”).

⁸ *Id.* (“Residential Internet connections, whether broadband or dialup usually use dynamic IP addresses . . .”).

⁹ *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.”)

¹⁰ Andy Johnson, *The IP Mystery: How Police Track Your Online Activity*, CTV NEWS, Sept. 12, 2007, http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070912/spying_background_070912/20070912/

¹¹ Speedguide.net, *supra* note 6 (“The need for dynamic IP addresses arises from the limited number of IP addresses available in IPv4. . . . This way, ISPs can have more subscribers than IP addresses . . . and ease IP maintenance.”).

¹² What Is My IP, *supra* note 2.

¹³ Tom Espiner, *ICANN: IPv4 Will Run Out by 2011*, ZDNET UK, May 12, 2008,

<http://www.zdnet.com.au/news/business/soa/ICANN-IPv4-will-run-out-by-2011/0,139023166,339288828,00.htm?omnRef=http://www.google.com/search?hl=en&client=safari&rls=en&q=ICANN%20IPv4&aq=f&oq=&aqi=g1>.

¹⁴ What Is My IP, *supra* note 2.

¹⁵ Paul Meller, *European Commission Urges Rapid Adoption of IPv6*, IDG NEWS SERVICE, May 27, 2008, 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.”). BGP Expert, *IPv4-IPv6 Compatibility* (June 6, 2006) <http://www.bgpexpert.com/article.php?article=106>.

¹⁶ Cybertelecom Federal Internet Law & Policy IPv6, <http://www.cybertelecom.org/dns/ipv6.htm> (last visited Jan. 19, 2010) (“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 . . .”).

B. Communications Decency Act

In 1996, Congress passed the Communications Decency Act (“CDA”) as part of the Telecommunications Act.¹⁷ One Part of the act, later found unconstitutional by the Supreme Court,¹⁸ was intended to protect children from online indecent and obscene material.¹⁹ The part of the act that survived was section 230, which provided greater immunity to “interactive computer services”.²⁰

Section 230 was enacted in response to two cases. The first was *Cubby, Inc. v. CompuServe, Inc.*, where CompuServe, an ISP, was sued for defamatory comments posted by a user in an online news forum it hosted.²¹ The court held that CompuServe was a distributor, not a publisher, under defamation law because it lacked editorial involvement, and therefore not liable.²² The second 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.²³ The court held that Prodigy was liable as a publisher for content posted by its users because it took affirmative steps towards editorial control by attempting to screen offensive content.²⁴ A publisher is a person or entity that has exercised editorial control over the content of a work (i.e. newspapers).²⁵ Comparatively, a distributor has exercised no editorial control (i.e. newsstands).²⁶ The issue was substantial because under the law of most states at the time (and as it remains today), a publisher was strictly liable for defamatory statements whereas a distributor was liable only for content they knew or should have known was defamatory.²⁷ As a result of these

¹⁷ 47 U.S.C. § 230(a)-(d), (f)(2) (1996), available at http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html (“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 education institutions.”).

¹⁸ *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

¹⁹ Center for Democracy & Technology, *Communications Decency Act (CDA)*, <http://cdt.info/speech/cda/> (last visited Jan. 18, 2010).

²⁰ 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 (2009); Madeline K. Rodriguez, *Reexamining Section 230 of the CDA and Online Anonymous Speech: Defamation on the Internet and the Websites that Facilitate It* (2009), available at <http://www.bc.edu/schools/cas/communication/meta-elements/pdf/thesis09.rodriguez.pdf>.

²¹ *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 137 (S.D.N.Y. 1991).

²² *Id.* at 140.

²³ *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 N.Y. Misc. LEXIS 229, *1-2 (N.Y. Sup. Ct. 1995).

²⁴ *Id.* at *10; Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 210-11 (2002).

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 Comm’n*, 907 F. Supp. 1361, 1367 n.10 (N.D.Cal. 1995) (“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. 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 because it used software to automatically prescreen messages that were offensive or in bad taste.” (citing *Cubby*, 776 F. Supp.; *Stratton*, 1995 WL 323710)); H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 Kan. L. Rev. 369 (Jan. 2008).

decisions, ISPs became less likely to screen content out of fear that they would be liable as publishers, but if they took no action at all they would be merely distributors.²⁸

Congress' 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."²⁹ Section 230 provided that interactive computer services would not be held liable as publishers, and provided protection for "'Good Samaritan' blocking and screening of offensive material."³⁰ However, the Internet model at the time was very different than what has evolved. It is uncertain whether Congress would have afforded the same protection had it known that ISPs would provide content in the future.³¹

C. Judicial Expansion of Online Immunity

Courts have consistently given section 230 a broad reading in determining website liability by providing liability protection to ICPs (which Congress never explicitly authorized), even when the website knew, or should have known, the material was defamatory.³² In *Zeran v. America Online, Inc.*, Zeran sued America Online for failing to remove a defamatory posting on its site after receiving notice.³³ 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."³⁴ However, the court found that section 230 provided federal immunity to any cause of action originating with a third-party's use of the service.³⁵ In doing so the court interpreted section 230 to grant distributor immunity. The plain language of the statute explicitly provided only that an interactive computer service would not be held liable as a publisher.³⁶

Courts have also extended immunity to websites which knowingly profited from the illegal activities of its users. For example, in *Doe v. Bates*, Plaintiffs contended that Yahoo! knowingly profited from the trafficking of child pornography.³⁷ The court found that Yahoo! was immune from any civil liability for third-party content on Yahoo!'s website, even if Yahoo! had

²⁸ Holland, *supra* note 27 ("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.'" (citing 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)).

²⁹ 47 U.S.C. § 230 (1996), available at http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html.

³⁰ Schruers, *supra* note 24.

³¹ Shortly after the CDA was passed, ISPs began to realize that greater profits could be made in Internet content rather than Internet services, which led to companies providing content but then seeking liability protection as an ISP. *Ben Ezra, Weinstein, & Co. v. Am. Online, Inc.*, 206 F.3d 980, 984-85 (2000) (finding that American Online 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); *Blumenthal v. Drudge*, 992 F. Supp. 44, 47, 51-52 (1998) (finding that American Online was immune from defamation liability as an ISP even though it had a licensing agreement with the author to provide the defamatory content).

³² See *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

³³ *Id.* at 328.

³⁴ *Id.* at 330.

³⁵ *Id.*

³⁶ Holland, *supra* note 27.

³⁷ *Doe v. Mark Bates & Yahoo!, Inc.*, 35 Media L. Rep. 1435 (Dec. 27, 2006).

knowledge of the existence of the illegal content.³⁸ The 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 230.³⁹ However, this reasoning is inconsistent with traditional secondary liability analysis, which holds an entity liable for knowledge of, promotion of, refrain to control, or profit from an illegal activity.⁴⁰

A social networking website is a service that provides its users with connectivity to friends and self-expression.⁴¹ Although different social networking websites offer different services to different audiences,⁴² they all share two primary components: the profile and the community.⁴³ Unsurprisingly, social networking websites have also been consistently granted broad section 230 immunity. Most notably, in *Doe v. MySpace* the Plaintiff was a 13-year-old girl who had misrepresented her age on her online profile.⁴⁴ She was sexually assaulted by a 19-year-old male she had met through the website when they met for a date.⁴⁵ The Plaintiff sued MySpace for “failing to implement basic safety measures to prevent sexual predators from communicating with minors.”⁴⁶ The court, citing to section 230, held that MySpace was immune from any liability.⁴⁷

Part III: The Current Problem with Online Social Networks

Online social networking plays an increasingly more dominant role in the lives of all people regardless of nationality or demographic. The time spent on social networking sites is growing three times faster than the overall Internet rate; social networking accounts for 10

³⁸ *Id.* (“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.”).

³⁹ *Id.* (“The Zeran court also noted the Congressional purpose of removing disincentives to self-regulation by Internet service providers. If Internet service providers such as Yahoo! could be liable for reviewing materials but ultimately deciding to allow them, they would likely chose [*sic*] not to regulate at all.”).

⁴⁰ *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930, 938, 941 (2005) (plaintiffs held 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); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262-64 (1996) (operators of a swap meet were held liable where they allowed vendors to sell counterfeit goods and they had knowledge of, control of, and profited from the infringing activity).

⁴¹ Richard M. Guo, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 619-20 (2008).

⁴² *E.g.*, Facebook, www.facebook.com (last visited Jan. 19, 2010) (“Facebook helps you connect and share with the people in your life.”); MySpace Quick Tour, <http://www.myspace.com/index.cfm?fuseaction=userTour.home> (last visited Jan. 18, 2010) (Main categories and sub-categories: “(1) MySpace is a place for friends – Search friends, Find old friends, Make new friends, (2) MySpace is Your Space – Express who you are, upload pictures & videos, add music, your own web address”); Twitter, www.twitter.com (last visited Jan. 18, 2010) (microblogging and real-time short messaging service); DeviantART, www.deviantart.com (online community of artists and their artwork); LinkedIn About Us, <http://press.linkedin.com/about> (last visited Jan. 18, 2010) (“Your professional network of trusted contacts gives you an advantage in your career.”).

⁴³ Richard M. Guo, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 619 (2008) (“While the various social networking services offer different features, they build around two basic elements: the profile and the community. A profile is a webpage that allows a user to aggregate and present her personal information . . . Users create communities by linking their profiles with one another.”).

⁴⁴ *Doe v. MySpace*, 474 F. Supp. 2d 843 (W.D. Tex. 2007) *aff’d*, 2008 U.S. App. LEXIS 10612 (5th Cir. 2008).

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

percent of all Internet time and is currently the 4th most popular online activity.⁴⁸ While the baby boomer generation is the fastest growing age demographic,⁴⁹ and adults comprise the majority of social networking site users,⁵⁰ online social networking plays a more prevalent part in the lives of teens and young adults.⁵¹

Particularly worrisome is the dangerous lure and appeal of social networking sites to young children. Children are becoming increasingly more tech savvy at increasingly younger ages.⁵² As a result, these young children are participating in social networking sites primarily aimed at teens and adults.⁵³ In response, there are a number of social networking sites directed specifically to children below the age of 14, some having a minimum age requirement as low as 5 years old.⁵⁴

With the amount of users, and the time they spend, on online social networks, there is a wide range of problems facilitated by social networking websites.⁵⁵

A. Sexual abuse

One of the online social networking problems with the most media attention is sexual abuse, with the ages of victims ranging from young children to adults. The role an online social network takes when inadvertently facilitating sexual abuse varies from case to case.

⁴⁸ Nielsen News Release, *Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email*, NIELSON, Mar. 9, 2009, http://www.nielsen-online.com/pr/pr_090309.pdf. See also Nielsen, *Nielsen Reports 17 Percent of Time Spent on the Internet in August Devoted to Social Networking and Blog Sites, Up from 6 Percent A Year Ago*, NIELSON, Sept. 23, 2009, http://en-us.nielsen.com/main/news/news_releases/2009/september/nielsen_reports_17.

⁴⁹ 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/>.

⁵⁰ See EMarketer, *Social Network User Demographics*, EMARKETER, Jan. 27, 2009, <http://www.emarketer.com/Article.aspx?R=1006882>.

⁵¹ EMarketer, *Teens on Social Networks*, EMARKETER, Apr. 16, 2009, <http://www.emarketer.com/Article.aspx?R=1007041> (stating that 74% of US teens use social networks, and predicting that number to increase to 79% by 2013). See Mark Dolliver, *Take Care When Targeting Teens Online*, ADWEEK, Oct. 5, 2009, available at http://www.adweek.com/aw/content_display/news/agency/e3i505f5fdeedc76b42ca9d8d4695e83c6c (stating that 66 percent 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 18-24 use online social networks).

⁵² See Childnet International, *Young People and Social Networking Sites* (2009), http://www.childnet.com/downloads/blog_safety.pdf.

⁵³ Jemima Kiss, *100,000 Kids Join CBBC Social Network*, GUARDIAN.CO.UK, July 10, 2008, available at <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 11-year-olds in the UK regularly use social networking sites designed for older children and teenagers.”).

⁵⁴ Carolyn Jabs, *These ‘Social Websites’ Cater to Little Kids*, TECHNO FAM., Jan. 2008, <http://www.metrokids.com/january08/technofamily0108.html> (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, http://blog.syracuse.com/family/2008/12/making_sense_of_socialnetworki.html.

⁵⁵ E.g., Trench Reynolds’ Crime News, <http://crimene.ws/mycrimespace/> (follows crimes facilitated by or committed through online social networks).

A large number of victims have met their assailant through online social networks. It has been estimated that one out of seven children between the ages of 13 and 17 receive unwanted sexual solicitations.⁵⁶ This problem is compounded by a young Internet user's willingness to engage in online relationships.⁵⁷ Despite years of awareness programs and media coverage, the story generally remains the same: young Internet user meets a friend over a social network, eventually goes to meet him in person, and is then sexually assaulted (although sometimes the rape is statutory and not forceful).⁵⁸ Fortunately, some criminals are caught before any physical harm is done.⁵⁹

However, an assailant does not need to physically meet their victim in order to cause harm or commit a crime. There are a number of unfortunate stories of older men and women enticing underage children to send them sexually explicit pictures, usually by posing as someone they are not.⁶⁰ The oddest story was a father who propositioned his own 13-year-old daughter for sex over Facebook.⁶¹ He proposed "meeting the girl for sex and explained sex acts in graphic

⁵⁶ Janis Wolak, Kimberly Mitchell & David Finkelhor, *Online Victimization of Youth: Five Years Later*, NAT'L CENTER FOR MISSING & EXPLOITED CHILD., at vii (2006) available at <http://www.unh.edu/ccrc/pdf/CV138.pdf>.

⁵⁷ Id. at 1 ("In YISS-2 [*Online Victimization of Youth: Five Years Later* (2006)] there were [] 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 [*Online Victimization: A Report on the Nation's Youth* (2001)]) or who formed close online relationships with people they met online (11% down from 16%).").

⁵⁸ Trench Reynolds' Crime News, *Okla. Man Accused of MySpace Rape*, Oct. 27, 2009, <http://crimene.ws/mycrimespace/2009/10/27/okla-man-accused-of-myspace-rape.html> (19-year-old raped a 15-year-old girl he met over MySpace after he and a friend took her home and got her drunk); WFSB, *Ex-Teacher's Aide Accused of Preying on Girls*, Oct. 10, 2006, (31-year-old met teenage girls through MySpace and told them he was 19-years-old. They would then meet in person and he would sexually assault them.); Trench Reynolds' Crime News, *Sex offender pleads guilty to having sex with teen MySpace girl*, Oct. 10, 2009, <http://crimene.ws/mycrimespace/2009/10/10/sex-offender-pleads-guilty-to-having-sex-with-teen-myspace-g.html> (33-year-old lied about his age to a 14-year-old girl he met on MySpace and then had sex with her); Trency Trench Reynolds' Crime News, *From the 15 Will Get You 20 files: Joshua Britzman*, Sept. 27, 2009, <http://crimene.ws/mycrimespace/2009/9/27/from-the-15-will-get-you-20-files-joshua-britzman.html> (23-year-old charged with having sex with a 15-year-old girl that he met on Facebook); Trench Reynolds' Crime News, *Brooklyn Man Charged With Having Sex With Upstate NY Teen He Met on Facebook*, Sept. 14, 2009, <http://crimene.ws/mycrimespace/2009/9/15/brooklyn-man-charged-with-having-sex-with-upstate-ny-teen-he.html> (23-year-old accused of having sex with a 15-year-old girl he met on Facebook).

⁵⁹ Emily S. Achenbaum, *Facebook Child Porn Case Results in 35-year Federal Prison Term*, CHI. TRIB., Oct. 22, 2008, available at <http://archives.chicagotribune.com/2008/oct/22/local/chi-fox-lake-facebook-both-22-oct22> (stating that Michael, a 35-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.); The Associated Press, *Boys' MySpace Prank Results in Crime Arrest*, MSNBC, Mar. 8, 2006, available at <http://www.msnbc.msn.com/id/11708746/> (teenage boys setup a fake profile as a 15-year-old girl and through coincidence helped police capture a 48-year-old man trying to meet "her" for sex).

⁶⁰ Trench Reynolds' Crime News, *Kansas Man Indicted on Facebook Child Porn Charges*, May 22, 2009, <http://crimene.ws/mycrimespace/2009/5/22/kansas-man-indicted-on-facebook-child-porn-charges.html> (38-year-old posed as a 19-year-old woman on Facebook to get teenage boys to send him sexual explicit photos of themselves); Trench Reynolds' Crime News, *More on Stickam's latest predator*, Oct. 21, 2009, <http://crimene.ws/mycrimespace/2009/10/21/more-on-stickams-latest-predator.html> (Father would pose as a 17-year-old boy on Stickam and convince underage girls to masturbate on webcam, sometimes by threatening to tell the girls parents if they didn't do what he wanted);

⁶¹ Trench Reynolds' Crime News, *Man Accused of Propositioning His Own Teen Daughter on Facebook*, Oct. 10, 2009, <http://crimene.ws/mycrimespace/2009/10/10/man-accused-of-propositioning-his-own-teen-daughter-on-faceb.html>.

detail, telling her, ‘not many other fathers and daughters are this brave, so not many of them are so lucky to experience all these pleasures.’”⁶² Fortunately, the girl told her mother, who told the police, who set up an undercover sting, where they caught the father attempting to meet his daughter for sex with a camera, tripod, and an unopened box of condoms.⁶³

While these problems may have been prevented by better security measures (see Part III below), this is not true for all crimes facilitated by social networking sites. Specifically, it would be nearly impossible for social networks to prevent crimes between adults that occurred because they met through the social network.⁶⁴

B. Cyberbullying

Another problem associated with online social networks is cyberbullying.⁶⁵ Cyberbullying has been defined as the “willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.”⁶⁶ Although cyberbullying is not unique or exclusive to online social networks, social networks are one of its most popular virtual locations, with social networks to soon be the most common source of cyberbullying worldwide.⁶⁷

In 2006, cyberbullying gathered national media attention when 13-year-old Megan Meier committed suicide.⁶⁸ The cyberbully was Josh Evans, a fictional 16-year-old boy created by Lori Drew, her assistant, and her daughter.⁶⁹ The purpose was to tease and humiliate Megan, with whom Lori Drew’s daughter had been fighting.⁷⁰ State and federal prosecutors were unable to find a law under which to charge Drew.⁷¹ Although the government did attempt, and ultimately fail, to argue that “violating MySpace’s terms of service was the legal equivalent of computer

⁶² *Id.*

⁶³ *Id.*

⁶⁴ Trench Reynolds’ Crime News, *Woman Allegedly Raped After Meeting Someone on Tagged.com*, Sept. 5, 2009, <http://crimene.ws/mycrimespace/2009/9/6/woman-allegedly-raped-after-meeting-someone-on-taggedcom.html> (51-year-old woman was drugged and raped after meeting a man from Tagged); Trench Reynolds’ Crime News, *MySpace Rapists Get Slaps on the Wrists*, Oct. 8, 2009, <http://crimene.ws/mycrimespace/2009/10/8/myspace-rapists-get-slaps-on-the-wrists.html> (two men plead guilty to raping a 20-year-old woman that they met on MySpace); Trench Reynolds’ Crime News, *MySpace Pants Robbers Busted*, Oct. 4, 2009, <http://crimene.ws/mycrimespace/2009/10/4/myspace-pants-robbers-busted.html> (stating a man went to meet a woman he met over MySpace and had his pants stolen by her and an accomplice).

⁶⁵ See Cyberbullying Research Center, <http://www.cyberbullying.us/>.

⁶⁶ Sameer Hinduja & Justin W. Patchin, *Cyberbullying Fact Sheet: What You Need to Know About Online Aggression*, Cyberbullying Research Center (2009) http://www.cyberbullying.us/cyberbullying_fact_sheet.pdf.

⁶⁷ CyberBully Alert, *Cyber Bullying Statistics that may Shock You!*, 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 overtake chat rooms as the top source of cyberbullying problems worldwide.”).

⁶⁸ Steve Gorman, *MySpace Suicide Conviction Tentatively Dismissed*, REUTERS, July 2, 2009, <http://www.reuters.com/article/technologyNews/idUSN029085920090702>.

⁶⁹ 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>.

⁷⁰ Steve Gorman, *MySpace Suicide Conviction Tentatively Dismissed*, REUTERS, July 2, 2009, <http://www.reuters.com/article/technologyNews/idUSN029085920090702>; Tina Kells, *Lori Drew Case Dismissed: MySpace Mom Caused Megan Meier Suicide*, NOWPUBLIC, July 2, 2009, <http://www.nowpublic.com/world/lori-drew-case-dismissed-myspace-mom-caused-megan-meier-suicide>.

⁷¹ Frederick Lane, *Teen’s Suicide Spurs Anti-cyberbullying Law*, NEWSFACTOR, Nov. 24, 2007, http://www.newsfactor.com/story.xhtml?story_id=56869&full_skip=1.

hacking.⁷² In response, many states passed anti-cyberbullying laws,⁷³ and there is currently a pending federal bill.⁷⁴

While it is generally true that most instances of cyberbullying do not reach such drastic outcomes, it is still a growing problem with varying degrees of harm,⁷⁵ and social networking sites are the new favored forum.⁷⁶ At the time of the Megan Meier incident, with no laws targeting cyberbullying, MySpace probably could not have done anything to prevent Lori's actions without infringing on free speech (nor did MySpace have any way to confirm the existence of Josh Evans). But that was then. With significant advances in the law, and with current technology, there may be a fair system available for identifying and monitoring cyberbullying.⁷⁷

C. Gang activity

A growing concern, but still one that has yet to reach the level of national media attention that cyberbullying and sexual abuse have, is gang activity on the Internet. Sometimes referred to as "net banging", gangs are using the Internet to recruit new members and intimidate rivals.⁷⁸ The issue is particularly concerning because of the new audience and range of influence that the Internet, social networking websites in particular, can give gangs.⁷⁹ Aside from recruitment, there

⁷² *U.S. v. Lori Drew*, 259 F.R.D. 449 (C.D.Cal. 2009) (court acquitted Lori Drew after she was charged and found guilty by a jury under the Computer Fraud and Abuse Act"); Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED, July 2, 2009, http://www.wired.com/threatlevel/2009/07/drew_court/.

⁷³ Ashley Surdin, *In Several States, A Push to Stem Cyber-Bullying*, WASHINGTON POST, Jan. 1, 2009, available at <http://privateschool.about.com/b/2008/02/10/7-states-pass-anti-cyberbullying-laws.htm> ("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 . . .").

⁷⁴ H.R. 1966, 111th Cong. (2009), available at <http://www.govtrack.us/congress/bill.xpd?bill=h111-1966>; Anna North, *Is Legislation the Way to Stop Cyberbullying*, JEZEBEL, Oct. 1, 2009, <http://jezebel.com/5371949/is-legislation-the-way-to-stop-cyberbullying>.

⁷⁵ Nadia Wynter, *Parents of Holly Grogan, 15, Blame Facebook for Teen's Suicide*, DAILY NEWS, Sept. 21, 2009, available at http://www.nydailynews.com/news/world/2009/09/21/2009-09-21_parents_of_holly_grogan_15_blame_facebook_for_teens_suicide.html (British 15-year-old Holly Grogan committed suicide in part from being the recipient of cyberbullying on her Facebook wall); Chris Matyszczuk, *Teen Sues Facebook, Classmates Over Cyberbullying*, CNET NEWS, Mar. 3, 2009, http://news.cnet.com/8301-17852_3-10187531-71.html (Teenager Denise Finkel has 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, http://www.marinij.com/ci_3643735 (13-year-old had to switch schools after her friends started an "Olivia Haters" club on MySpace).

⁷⁶ 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).

⁷⁷ See discussion *infra* Part V.

⁷⁸ Joe Vazquez, *Gangs Turn to Social Networking Sites to Recruit*, CBS5, Feb. 7, 2008, <http://cbs5.com/local/Internet.gang.recruiting.2.648038.html> ("It's really no different than the way Hitler recruited Hitler youth with the pageantry and the uniforms and the messages of unity and sacrifice and honor" said Vilchez. "It's the same messages that you seen [sic] on these gang websites."); Trendhunter, *Net Banging: Gangs Online for Recruiting and Intimidating* <http://www.trendhunter.com/trends/net-banging-gangs-online-for-recruiting-and-intimidating>.

⁷⁹ Shelly Mellot, *Can Social Networking Expose Your Children to Gangs*, YOUR SPHERE FOR PARENTS, Apr. 8, 2009, <http://internet-safety.yoursphere.com/tips/can-social-networking-expose-your-children-to-gangs> ("Teens who

is concern over the use of websites to incite violence on the street.⁸⁰ Gang activity has followed the trend that every societal problem will manifest itself on a social networking website.⁸¹

D. Why Should Social Networking Websites be More Liable than Other Websites?

Social networking websites are special. On no other website have users put on the Internet so much personal information so freely.⁸² As indicated above, this means a host of new problems associated with social networking websites, but it also means that those websites have at their disposal information unavailable on almost any other type of website.

Compare the liability of a social networking site with that of a search engine (Google, Yahoo!, Bing, etc.). Twitter, one of the most popular social networking websites today, has over 50 million unique accounts.⁸³ A person does not need a Twitter account to look at a Twitter profile,⁸⁴ so these profiles are publicly accessible and can be located using search engines. This means that to hold Twitter liable for its users, it would need to police 50 million web pages. Twitter is just one website of over 185 million.⁸⁵ This means that to hold search engines liable for the web results they return, search engines would need to monitor 50 million of Twitter's pages, plus an additional 184 million websites (not pages). The number is astronomical and beyond the practical technological ability of any search engine. Therefore, social networking sites are in a better position to monitor its users actions than search engines.

A fairer comparison may be to online auction and shopping websites (Amazon.com, Ebay, Craigslist). The content of these websites is more similar to social networking sites than search engines because their liability and monitoring would be limited to their own website. Ebay has over 16 million new items listed on its website each day with no practical way to check for fraudulent items.⁸⁶ To put an item up for sale, a user writes a description and uploads a

would otherwise never come in contact with gang members are able to see their profiles, videos and photos online.”); *See also* Kevin Poulsen, *Pimps Go Online to Lure Kids Into Prostitution*, WIRED, Feb. 25, 2009, <http://www.wired.com/threatlevel/2009/02/pimping/> (“We’re seeing kids who are getting into this stuff [prostitution] that do not match society’s stereotype’ . . . ‘These are not just kids in poor families who have no other options. We’re seeing kids from the full spectrum of society, and a lot of that is due to recruitment over the Internet [sic].”).

⁸⁰ Robin I. Young, *Net Banging: Street Gangs Answer the Digital Craze*, NAT’L CRIME PREVENTION COUNCIL, 2008, <http://www.ncpc.org/programs/catalyst-newsletter/catalyst-newsletter-2008/volume-29-number-6/net-banging-street-gangs-answer-the-digital-craze> (“A random search on MySpace revealed a number of alleged gang member’s pages that were seemingly created just for the purpose of inciting conflict with their rivals . . . ‘[W]e’ll see something start on the Internet, and actually turn into an assault or a gang fight that actually results out of Internet profiling”).

⁸¹ Ashley Smith, *County, Schools Fighting ‘Online Generation’ of Gang Activity: Officials Say Tracking, Awareness, Anti-gang Programs are Crucial*, NEWS-SENTINEL, Mar. 19, 2009, <http://www.allbusiness.com/crime-law/criminal-offenses-property/12243358-1.html>.

⁸² 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 (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.”).

⁸³ 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/>.

⁸⁴ *See generally* Twitter, <http://twitter.com/>.

⁸⁵ Netcraft, *January 2009 Web Server Survey*, Jan. 2009, http://news.netcraft.com/archives/2009/01/16/january_2009_web_server_survey.html.

⁸⁶ The Auction Software Review, *Statistics You Won’t Find on eBay*, Oct. 12, 2007, <http://www.auctionsoftwarereview.com/articles/ebay-statistics.asp>.

picture.⁸⁷ Ebay has no way to verify that the picture listed is actually a picture taken by the user. Ebay does take measures to prevent fraudulent transactions through identity verification by requiring a seller to use a PayPal account or credit card (a user must be 18 or older to use Ebay).⁸⁸ This provides a buyer with judicial recourse for a fraudulent sale.⁸⁹

However, Ebay has made, and may make more, substantial changes to its fraud prevention as a result of losing lawsuits in France.⁹⁰ As a result of these lawsuits, Ebay created better security measures.⁹¹ Ebay has implemented proactive fraud protection on types of items more frequently targeted by scammers.⁹² Ebay has not released any details on how they check for fraudulent items, so it is very hard to assess the effectiveness of such safety measures.⁹³

The information a user inputs into Ebay is markedly limited and different from the information a user inputs into a social networking website. Therefore, with more personal information to work from, social networking websites are better able to prevent abuse than websites such as Ebay.

Additionally, one of the biggest differences between social networking websites and Ebay (and most other websites) is the type of harm that results. On Ebay, a fraudulent, or damaged, or mislabeled item is sold and the harm is either loss of money, dissatisfaction with the item, or a trademark violation. On a social networking website the types of harms are much more serious and much more diverse.⁹⁴

Part IV: Ineffective Solutions Encourage Deception

There have been a wide variety of proposals and implementations 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 networking websites to discover and identify abuse and potentially dangerous users.

⁸⁷ Ebay How Do I List an Item for sale?, <http://pages.ebay.com/help/sell/questions/list-item.html>.

⁸⁸ Ebay Creating a Seller's Account, http://pages.ebay.com/help/sell/seller_account.html; Ebay Underage Users, <http://pages.ebay.com/help/policies/identity-underage-users.html>; Ben Charny, *EBay Requires New Sellers to Use PayPal or Credit Card*, MARKET PULSE, Jan. 17, 2007, <http://www.marketwatch.com/story/ebay-requires-new-sellers-to-use-paypal-or-credit-card>.

⁸⁹ Ebay Rules for buyers – overview, <http://pages.ebay.com/help/policies/buyer-rules-overview.html> (“[E]ach bid you make is a binding contract to buy the item.”).

⁹⁰ Deidre Woollard, *EBay Loses Big French Lawsuit*, LUXIST, June 30, 2008, <http://www.luxist.com/2008/06/30/ebay-loses-big-french-lawsuit/> (“[A] French court ruled that eBay was responsible for counterfeit items sold on the site . . . Ebay 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> (“eBay was convicted by a French court Wednesday of selling counterfeit goods . . .”).

⁹¹ Ina Steiner, *eBay Loses Hermes Counterfeiting Case*, AUCTION BYTES, June 5, 2008, <http://www.auctionbytes.com/cab/abn/y08/m06/i05/s01> (“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 . . .”).

⁹² Posting by Rob Chesnut on eBay, *A Message from Rob Chesnut: Combating Online Fraud*, <http://www2.ebay.com/aw/core/200704090921122.html> (Apr. 9, 2007).

⁹³ *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 . . .”).

⁹⁴ See discussion *infra* Part III.D.

A. Banning Users

Although seemingly a good idea, banning the IP addresses of consistent violators is very ineffective and easily circumvented.⁹⁵ That is because ISPs recycle IP address due to the nature of IPv4 and the limited number of IP addresses available.⁹⁶ Even users with broadband, who are always connected to the Internet, can still easily change their IP address.⁹⁷

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 their site.⁹⁸ 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.⁹⁹ Despite appearances, this was the wrong course of action to take.

Banning registered sex offenders from a web site does not stop them from using another site. MySpace purged itself of sex offenders, but the offenders migrated to Facebook.¹⁰⁰ Facebook not wanting to be outdone by MySpace followed suit and kicked the registered sex offenders off of their site.¹⁰¹ States seem to share this mentality and are passing laws requiring sexual offenders to register any online screen names,¹⁰² or banning them from social networking sites altogether.¹⁰³ All of this means one of three things for MySpace and Facebook: (1) the websites kicked off rehabilitated prior sex offenders,¹⁰⁴ (2) the websites kicked off non-rehabilitated sex offenders who are now lurking on other social networking sites, or (3) the

⁹⁵ Adam Kalsey, *Why IP banning is Useless*, ADAMKALSEY, Feb. 10, 2004, http://kalsey.com/2004/02/why_ip_banning_is_useless/.

⁹⁶ Speedguide.net, *What is the Difference Between Dynamic and Static IP Addresses?*, http://www.speedguide.net/faq_in_q.php?category=88&qid=137.

⁹⁷ *Id.* (“[Y]our IP address . . . can change any time you get disconnected, there is a power outage, ISP maintenance, etc.”).

⁹⁸ Connecticut Attorney General’s Office, *CT, NC Attorneys General Say MySpace Response to Subpoena Revealed 90,000 Registered Sex Offenders with Profiles*, CT.GOV, 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>.

⁹⁹ CNN, *MySpace Kicks Out 90,000 Sex Offenders, Connecticut AG Says*, Feb. 4, 2009, <http://www.cnn.com/2009/TECH/02/03/myspace.sex.offenders/index.html>.

¹⁰⁰ Erick Shonfeld, *Thousands of MySpace Sex Offender Refugees Found on Facebook*, TECHCRUNCH, Feb. 3, 2009, available at <http://www.techcrunch.com/2009/02/03/thousands-of-myspace-sex-offender-refugees-found-on-facebook/>; Tina Kells, *90,000 MySpace Sex Offenders Headed for Facebook? Does it Matter?*, NOWPUBLIC, Feb. 5, 2009 <http://www.nowpublic.com/tech-biz/90-000-myspace-sex-offenders-headed-facebook-does-it-matter>; Daily Mail Reporter, *MySpace removes 90,000 sex offenders... but paedophiles may be turning to Facebook instead*, MAILONLINE, Feb. 5, 2009, <http://www.dailymail.co.uk/news/article-1135490/Myspace-removes-90-000-sex-offenders--paedophiles-turning-Facebook-instead.html>.

¹⁰¹ Carline McCarthy, *Report: 5,585 Sex Offenders Purged from Facebook*, CNET NEWS, Feb. 20, 2009, http://news.cnet.com/8301-13577_3-10168255-36.html.

¹⁰² Cybertelecom Federal Internet Law & Policy, *Sex Offender Registries and Websites*, <http://www.cybertelecom.org/security/child.htm> (last visited Jan. 18, 2009); Melissa Mansfield, *Sex offenders required to register online screen names*, NEWSDAY, May 15, 2008, available at <http://www.allbusiness.com/crime-law/criminal-offenses-cybercrime/12104313-1.html>.

¹⁰³ Computerworld Staff, *Illinois Outlaws Sex Offenders from Using Facebook, MySpace*, NETWORKWORLD, Aug. 14, 2009, <http://www.networkworld.com/news/2009/081409-illinois-outlaws-sex-offenders-from.html>.

¹⁰⁴ 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. Gordon Fraser, *Lawmakers: Public Urination Shouldn’t Lead to Sex Offender Status*, EAGLE-TRIBUNE, Jan. 31, 2008, available at http://www.eagletribune.com/punewsnh/local_story_031093859.

websites have forced non-rehabilitated sex offenders to create fake profiles. Similarly, state and local governments restrict the residency of prior sex offenders,¹⁰⁵ but these measures that socially isolate sex offenders is actually detrimental to the public's safety.¹⁰⁶ So although the numbers look good for MySpace and Facebook, the actuality is that 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.

Despite gut reactions, the proper course of conduct would have been to keep the registered sex offenders on the site and monitor their behavior. While 90,000 profiles is a lot of profiles to monitor, it is harder to weed out 90,000 fake profiles. These 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 that the age purported in his or her online profile is accurate.¹⁰⁷ Instead, the websites tried to appease the media. Even if the registered sex offenders had fake profiles before getting kicked off of their real one, those fake profiles are still 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 in its current form. Specifically, minors should not be allowed on any of the many adult dating websites now available.¹⁰⁸ SexSearch received a lot of media attention when one of its users was charged with statutory rape of a minor who had lied in her profile and said she was 18 (she was 14).¹⁰⁹ But finding shelter under the CDA, SexSearch was not held liable for a user's false statement in her profile that she was over 18.¹¹⁰

¹⁰⁵ Wendy Koch, *Homeless Sex Offenders' Isolation Can Add to Problem*, USA TODAY, Nov. 18, 2007, available at http://www.usatoday.com/news/nation/2007-11-18-InsideSexOffender_N.htm ("At least 27 states and hundreds of cities have passed laws in the past decade to restrict where sex offenders live.").

¹⁰⁶ *Id.* ("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."); Sex Offender Reports, Charts and Other Papers by A Voice of Reason Our Mission and Deeper Purpose, <http://sexoffender-reports.blogspot.com/2009/04/our-mission.html> (last visited Feb. 18, 2010) ("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.").

¹⁰⁷ Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400 (enacted) (requires convicted sex offenders to register online identifiers).

¹⁰⁸ *E.g.* HornyMatches <http://www.hornymatches.com/>; NaughtyConnect <http://www.naughtyconnect.com/>; AdultFriendFinder <http://adultfriendfinder.com/>; AdultRaters <http://www.adultraters.com/>; SexSearch www.sexsearch.com.

¹⁰⁹ Austin Modine, *SexSearch Not Responsible for Underage Hookup (Again)*, REGISTER, Dec. 31, 2008, http://www.theregister.co.uk/2008/12/31/sexsearch_v_johndoe_appeal_dismissed/.

¹¹⁰ However, the 6th Circuit affirmed the lower court on alternative grounds and did not reach the issue of whether SexSearch was immune from liability under section 230. *Doe v. SexSearch.com*, 502 F. Supp. 2d 719 (N.D. Ohio 2007), *aff'd*, 2008 WL 5396830 (6th Cir. 2008).

Adult dating websites are in a better position to verify users' ages because the minimum age requirement is 18 and not 13. 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 18 anyway.¹¹¹ The website could require that your name appear as it does on your credit card, and the site can charge a nominal fee to prevent minors from using their parents credit card without their knowledge.¹¹²

Minimum age requirements are appropriate for adult websites because minimum age verification is practical, but this does not apply to general social networking sites. Of the ten most popular social networking sites two do not have a minimum age requirement.¹¹³ Requiring a minimum age below 18 years-old will never be completely accurate because age verification for minors is so difficult.¹¹⁴ Minors do not have any sort of paper trail (like a credit card) that can be used to cross-reference their information.¹¹⁵ As a result, the current system to verify a user's age employed by most social networking websites is completely ineffective.

Currently, when a 10-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 13 instead of 10.¹¹⁶ Now the social networking website has a 10-year-old user they think is 13 years old. While seemingly trivial, age can become a serious issue. For instance, assume a 15-year-old girl has lied about her age in the past so that her profile now claims she is 18, and that she sends naked pictures of herself to a 19-year-old guy through the social networking website. Now the website has unknowingly facilitated child pornography.¹¹⁷ Of course if she is ever caught by the police, that 15-year-old girl can be charged with possession and distribution of child pornography,¹¹⁸ while the social networking website would remain immune from liability.

The current age verification system employed by most social networking websites is too easily circumvented, and as a result, either needs to be completely scrapped or completely revamped.¹¹⁹

¹¹¹ 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 (2008).

¹¹² *Id.*

¹¹³ Posting of Andy Kazeniak to Compete, <http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/> (Feb. 9, 2009). Websites with a minimum age requirement: Facebook, <http://www.facebook.com/policy.php>; MySpace http://faq.myspace.com/app/answers/detail/a_id/237; Flixster, <http://www.flixster.com/misc/copyrightprivacyterms>; LinkedIn, http://www.linkedin.com/static?key=user_agreement; Tagged, http://www.tagged.com/terms_of_service.html; Classmates, <http://www.classmates.com/cmo/reg/terms.jsp>; MyYearBook, <http://www.myearbook.com/terms.php>; Imeem, <http://blog.imeem.com/legal/imeem-terms-of-use/>. Sites that do not have a minimum age requirement: LiveJournal, <http://www.livejournal.com/legal/tos.bml>; Twitter, <https://twitter.com/tos>.

¹¹⁴ Symposium, *Age Verification for Social Networking Sites: Is it Possible? Is it Desirable?*, PROGRESS & FREEDOM FOUND., at 5-6 (2007) available at <http://www.scribd.com/doc/2887394/Age-Verification-for-Social-Networking-Sites-PFF-event-transcript> (expressing concerns that its not possible and that the current sites that do have age verification are misleading in their security).

¹¹⁵ *Id.*

¹¹⁶ John Carvel, *Facebook: Children Evade Social Websites' Age Limits*, THE GUARDIAN, Aug. 7, 2008, available at <http://www.guardian.co.uk/technology/2008/aug/07/socialnetworking.facebook>.

¹¹⁷ Posting of Dave Parrack to TechBlog, *Self-taken Naked Photos of Teenagers Classified as Child Pornography*, <http://tech.blorge.com/Structure:%20/2009/03/28/self-taken-naked-photos-of-teenagers-classified-as-child-pornography/> (Mar. 28, 2009).

¹¹⁸ *Id.*

¹¹⁹ See discussion *infra* Part V.

Part V: Effective Actual and Potential Improvements to Website Security and Safety

As a general rule, good and effective solutions encourage honesty. Social networking websites should seek to achieve security through profile tracking and cross-reference, IP tracking, and simple observation. Currently, social networking sites are not taking these steps to protect their users because they have no incentive to do so with the immunity Congress and the courts have afforded them.

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.”¹²⁰ After a scandal involving “depictions of or engagement in sexualized conduct with avatars that resemble children,¹²¹ which behavior was subsequently banned from the website,¹²² Second Life created a community for minors called Teen Second Life.¹²³ Teen Second Life is open only to teens ages 13-17.¹²⁴ The only adults allowed in Teen Second Life are members of the parent company, Linden Lab, who are “clearly identified as a ‘Linden,’”¹²⁵ and “[e]ducators and youth non-profit organizations.”¹²⁶ However, any adult who is not a Linden Lab employee must go through a criminal and background check and is confined to certain areas.¹²⁷

As a means of age verification, Teen Second Life requires that a parent create their 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.¹²⁸ PayPal is a method for individuals and businesses to send and receive money online.¹²⁹ Parents can set up a PayPal student account by providing their child’s legal full name and their date of birth.¹³⁰ The student account is linked to the parent’s banking account, but the student account has spending limits and parental controls.¹³¹

These are all steps social networking websites could take, but have not. The most likely reason is that to implement these protections would substantially decrease traffic and membership, and thereby revenue. Profit maximization cannot be the standard for determining whether to impose regulations. Movie theaters have maximum occupant capacities under fire

¹²⁰ Melissa Ung, *Trademark Law and the Repercussions of Virtual Property (IRL)*, 17 COMMLAW CONSPECTUS 679, 680 (2009).

¹²¹ Second Life, Clarification of Policy Disallowing “Ageplay”, <https://blogs.secondlife.com/community/features/blog/2007/11/14/clarification-of-policy-disallowing-ageplay> (last visited Jan. 18, 2010).

¹²² *Id.* (“[R]eal-life images, avatar portrayals, and other depictions of sexual or lewd acts involving or appearing to involve children or minors are not allowed within Second Life.”).

¹²³ Jacqui Cheng, *Second Life Now Like Real Life: Show Me Yer ID, Kid*, ARS TECHNICAL, May 10, 2007, <http://arstechnica.com/gaming/news/2007/05/second-life-to-segregate-users-by-age.ars>.

¹²⁴ Teen Second Life What is Teen Second Life?, <http://teen.secondlife.com/whatis>.

¹²⁵ Linda Zimmer, *A Second Life/Second Life Teen Primer for Parents*, WEBWISEKIDS available at http://www.webwisekids.org/Second_Life_Article.pdf.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Id.*; PayPal Student Accounts, <https://www.paypal.com/student/>.

¹²⁹ Paypal What is PayPal?, https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing_CommandDriven/bizui/WhatIsPayPal-outside.

¹³⁰ PayPal Student Accounts, <https://www.paypal.com/student/>.

¹³¹ *Id.*

code regulations,¹³² businesses are required to have sprinkler systems,¹³³ and buildings have to be built to meet government safety specifications.¹³⁴ Society has agreed that there has to be a balance between profits and safety, but social networking websites are oddly and unwarrantedly excluded from any substantial and meaningful imposition of safety requirements.

B. MySpace is finally heading in the right direction

After a multitude of state attorney generals put pressure on MySpace by threatening litigation and investigation,¹³⁵ the website took some action towards greater safety features.¹³⁶ Specifically, MySpace developed Zephyr, a parental-notification software to monitor their child's MySpace account.¹³⁷ Under Zephyr a parent would not have access to the content on their child's MySpace page, but would be able to establish whether their child has a MySpace profile and what age or address their child claims on that profile.¹³⁸ This is a good solution in that it encourages active parenting and provides a practical means for parents to obtain important basic information about their children without completely invading their privacy. However, the effectiveness of the tool 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.

Another idea MySpace has implemented is limiting the contact of minors with potential assailants by only allowing them to become friends with people they actually know.¹³⁹ Now users over 18 are required to know the full name or e-mail of a 15-year-old (or younger) before contacting them at all.¹⁴⁰ However, this implementation is still insufficient. First, it is not effective for young children who inflate their age on their profile.¹⁴¹ 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 have 15-year-olds and younger only be searched by full names, regardless of the age of the person conducting the search. This way, when a sexual predator searches for a specific name, his search results only reveal individuals over the age of

¹³² CITY OF SPARKS, NEV., MUNICIPAL CODE available at http://www.ci.sparks.nv.us/governing/muni_code/Title_5/75/100.php.

¹³³ Russell P. Fleming, *The Fire Sprinkler Situation* (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.").

¹³⁴ See Bureau of Labor Statistics, *Occupational Outlook Handbook* (2010) available at <http://www.bls.gov/oco/ocos004.htm>.

¹³⁵ See Posting by Proskauer Rose to Privacy Law Blog, *Social Networking Sites Feel the Heat from Law Enforcement*, <http://privacylaw.proskauer.com/2007/10/articles/childrens-online-privacy-prote/social-networking-sites-feel-the-heat-from-law-enforcement/> (Oct. 17, 2009).

¹³⁶ Caroline McCarthy, *MySpace Agrees to Social-Networking Safety Plan*, CNET NEWS, Jan. 14, 2008, 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.").

¹³⁷ Caroline McCarthy, *MySpace Developing Parental-Notification Software*, CNET NEWS, Jan. 17, 2009, http://news.cnet.com/MySpace-developing-parental-notification-software/2100-1032_3-6150824.html.

¹³⁸ *Id.*

¹³⁹ Jai Lynn Yang, *Can This Man Make MySpace Safe for Kids?*, CNN MONEY, June 30, 2006, http://money.cnn.com/magazines/fortune/fortune_archive/2006/07/10/8380854/index.htm.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

18. This also prevents victims of sexual predators who misrepresent their age to appear younger because the limitation applies to all users.

C. Steps not taken by social networking sites that should be

1. Systems to report abuse

Most social networking websites, but not all,¹⁴² have some sort of system in place to report abuse,¹⁴³ but to varying degrees. Facebook and MySpace both have a system in place to report abuse of photos or videos.¹⁴⁴ Specifically, on Facebook, the user can choose from one of several categories to explain why the photo or video is abusive.¹⁴⁵ Although Bebo has agreed,¹⁴⁶ both Facebook and MySpace have refused to implement a “CEOP report” button, which is provided for free by the Child Exploitation and Online Protection Centre of Britain (“CEOP”),¹⁴⁷ presumably because it would then lose advertising space.¹⁴⁸ The CEOP report button seems to be an effective step in Internet user protection¹⁴⁹ because by clicking the button users can get advice and get in instant contact with counselors and law enforcement officers concerning abusive content (such as posts or pictures) or abusive users.¹⁵⁰ 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 system.”¹⁵¹ One would assume that Facebook’s abuse reporting system is very good, but one would then be wrong.

Facebook’s current abuse reporting system is logically cyclical and difficult to use, which may have been done in an attempt to claim that Facebook has less abuse reports than other social

¹⁴² Sean Poulter, *Children ‘Exposed to Pornography, Prostitution and Drugs on Twitter’*, MAILONLINE, Feb. 26, 2009, <http://www.dailymail.co.uk/news/article-1156136/Children-exposed-pornography-prostitution-drugs-Twitter.html> (“[Twitter] state users must be 13 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 and links to adult sites.”).

¹⁴³ Teen Second Life Community Standards, <http://teen.secondlife.com/footer/cs>.

¹⁴⁴ Mercedes Bunz, *How Easy is it to Report Abuse on Facebook?*, GUARDIAN.CO.UK, Nov. 18, 2009, <http://www.guardian.co.uk/media/2009/nov/18/facebook-reporting-abuse>; MySpace Report Abuse, <http://www.myspace.com/index.cfm?fuseaction=help.reportabuse>.

¹⁴⁵ Posting of Jessica Ghaslin to Facebook, <http://blog.facebook.com/blog.php?post=144628037130> (Oct. 14, 2009) (“[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.”).

¹⁴⁶ Nic Fleming, *Social Networking Sites: Why No Abuse Report Button?*, SHORT SHARP SCI., Nov. 18, 2009, <http://www.newscientist.com/blogs/shortsharpscience/2009/11/social-networking-sites-why-no.html>.

¹⁴⁷ *Id.*; Child Exploitation and Online Protection Centre <http://www.ceop.gov.uk/>.

¹⁴⁸ 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.

¹⁴⁹ *CEOP Annual Review*, at 9 (2009) available at http://www.ceop.gov.uk/downloads/documents/CEOP_Annual_Review_2008-09.pdf (“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 . . .”).

¹⁵⁰ *Id.*; CEOP, *More Than 8 Million Young Users Get Added Safety Support as Bebo Adopts ‘CEOP Report’ Button*, 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.”).

¹⁵¹ Nic Fleming, *Social Networking Sites: Why No Abuse Report Button?*, SHORT SHARP SCIENCE, Nov. 18, 2009, <http://www.newscientist.com/blogs/shortsharpscience/2009/11/social-networking-sites-why-no.html>.

networking websites.¹⁵² While there is a “report abuse” link for an offensive video or photo posted by a friend, there is not a link for an offensive wall post. So if a user wants to report offensive content on a person’s profile, he or she can use the “Report this Person” link located at the bottom of the offender’s profile page.¹⁵³ The problem is that this link only appears on the profiles of people the user is not friends with. Most people, notably founder Mark Zuckerberg himself,¹⁵⁴ set most of their profile content to private, so that only friends can see the content. Facebook has essentially set up a reporting system where users can easily report offensive material on profiles that they cannot see and do not have access to. If a user wants to “anonymously” report an offensive profile of a friend, he or she has to first remove them from friends, which makes any sort of follow up, or future abuse reporting on that profile, impractical if not impossible (aside from ruining part of the anonymity of the reporting to begin with).

There is little, if any, downside to implementing a report abuse button for easy access to help, especially when that button puts the user in contact with free third party support.

2. Use of the inherent nature of social networking sites

The purpose of social networking websites is to “connect and share with the people in your life.”¹⁵⁵ Social networking websites should cross reference information posted by the user to check a profile’s genuineness, or to check for red flags. Social networking website database queries are easy to implement,¹⁵⁶ so that 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 in 2010 a girl claims to be 18 years-old, but is a member of the network “Suburban High School 2014”, she is probably not 18. If someone claims to be 15, but has a graduate degree, it should raise a red flag.

Automated queries monitoring suspicious behavior would help prevent the sexual abuse of minors by preventing contact with suspicious adults, and age verification prevents them from potentially precarious situations. A social networking website is capable of checking if a 40 year-old man is attempting to friend a bunch of 15 year-olds, and should probably be required to bring it to the attention of law enforcement officials.

Many societal problems that are finding their ways 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. These would be better assisted, and may necessarily have to be assisted, by police cooperation.

¹⁵² 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/> (quoting response David “[T]here is no report link on a persons profile anymore in a shocking attempt to claim that Facebook has less reports than other users.”).

¹⁵³ Facebook Safety, <http://www.facebook.com/help/?safety>.

¹⁵⁴ Mark Zuckerberg’s Facebook profile,

<http://www.facebook.com/zuck?ref=search&sid=24801168.998771791..1#/zuck?v=wall&ref=search>.

¹⁵⁵ Facebook Home Page <http://www.facebook.com/>.

¹⁵⁶ E.g., SQL Wildcards, http://www.w3schools.com/SQL/sql_wildcards.asp (explaining how to code for a database query).

For those with concerns that the average criminal is more intelligent than to put obvious and incriminating information on a social networking websites, rest assured that he is not.¹⁵⁷ For those concerned that intelligent people will easily circumvent these kind of security protections, it is important to note that even intelligent people who engage in online criminal activity are easily caught.¹⁵⁸

Part VI: Legislation is necessary

Real substantial change in the safety of social networking websites has to come from legislation or a change in judicial interpretation of the scope of section 230.¹⁵⁹ 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 the website may lose as a result. However, legislation 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 them by inadvertently increasing the traffic of potential users to Facebook or Bebo.

Congress should 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 legislation¹⁶⁰ that would impose certain safety requirements on social networking websites,¹⁶¹ but the harms associated with social networks is on a national scale, and requires national coordination. Interestingly, the New Jersey bill would give social network providers some bite by allowing them to “sue customers who post ‘sexually offensive’ or ‘harassing’ communications.”¹⁶²

¹⁵⁷ Melissa Grace & Wil Cruz, *MySpace Brags Spur Gang Busts of Crips, Bloods Who Terrorized Manhattan Housing Project*, DAILY NEWS, Jan. 14, 2010, available at 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 . . .”).

¹⁵⁸ Andrew Scott, *Sex Sting in Poconos Nets Former Chief U.N. Weapons Inspector*, POCONO REC., Jan. 14, 2010, available at <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 what he thought was a 15-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 16-year-old girl,” but was actually} an undercover policewoman.).

¹⁵⁹ McCarthy, *supra* note 133 (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.”).

¹⁶⁰ Assem. B. 3757, 2009 Leg., 213th Sess. (N.J. 2009) available at http://www.njleg.state.nj.us/2008/Bills/A4000/3757_R1.HTM.

¹⁶¹ Posting of Grayson Barber to Freedom to Tinker, <http://www.freedom-to-tinker.com/blog/grayson/social-networking-safety-act> (March 25, 2009) (“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 ‘appropriate’ and banish offenders . . . Finally, if the social network provider fails to take action, it can be sued for consumer fraud.”).

¹⁶² *Id.*

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.¹⁶³ Also, there should be regulations dictating minimum requirements for a social networking website's abuse reporting system. However, social networking websites should not be liable for any harm that results from the good faith operation of an abuse reporting system. Social networking websites are not be 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.

However, 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 engaging in offensive activity or content that was not illegal out of fear of liability.¹⁶⁴ Additionally, there may be first amendment concerns with requiring websites to implement certain kinds of safety measures.¹⁶⁵

Part VII: 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, technology has progressed, and social networking websites have the means, but not the will to implement effective change.¹⁶⁶ 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.

¹⁶³ Declan McCullagh, *Congress Targets Social-Networking Sites*, CNET NEWS, June 29, 2006, 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, 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.").

¹⁶⁴ 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.").

¹⁶⁵ *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); *U.S. v. Playboy Entm't Group, 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).

¹⁶⁶ McCarthy, *supra* note 133 ("[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.").