

INTERNET SAFETY SURVEY: WHO WILL PROTECT THE CHILDREN?

Charlotte Chang

I. INTRODUCTION

The expansion of the Internet and its accompanying technologies has brought both increased efficiency and new methods of communication. However, the Internet also makes it easier for bad actors to harass and offend others. One form of online harassment is cyberbullying. Cyberbullying has become increasingly visible in the media, and concerns over online safety have prompted many state legislatures to take action. This Note will examine recent legislative attempts to make the Internet safer and explore the legal ramifications of implementing them.

Children and teenagers constitute a large portion of Internet users and are the focus of many recent statutory attempts to enhance online safety. According to an April 2009 study conducted by Pew-Internet & American Project, 74% of adults use the Internet.¹ A recent study found roughly 93% of Americans between the ages of twelve to seventeen use the Internet,² and youth Internet use is expected to increase. A 2009 study by Nielsen Research found an 18% increase in Internet use for children between the ages of two and eleven.³ Indeed, children are exposed to the Internet at the very young ages of two, three, and four as they sit on their parents lap.⁴ The increasing number of pre-teens who are online emphasizes the need to educate children about how to navigate the online world in a safe and moral manner. This Note construes “moral” and “ethical” Internet practices as not sending

© 2010 Charlotte Chang.

1. Pew Internet & American Life Project, Demographic of Internet Users, <http://www.pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx> (last visited Jan 23, 2010).

2. Sydney Jones & Susannah Fox, *Generations Online*, PEW RESEARCH CENTER PUBLICATIONS, Jan. 28, 2009, <http://pewresearch.org/pubs/1093/generations-online>.

3. Nielsen Wire, Growing Up, and Growing Fast: Kids 2–11 Spending More Time Online, Jan. 6, 2009, http://blog.nielsen.com/nielsenwire/online_mobile/growing-up-and-growing-fast-kids-2-11-spending-more-time-online.

4. Denise Chow, *Study: Children Ages 2 to 11 Make Up 9.5 Percent of Total Internet Users in the U.S.*, NY DAILY NEWS.COM, July 8, 2009, http://www.nydailynews.com/tech_guide/2009/07/08/2009-07-08_study_children_ages_2_to_11_make_up_95_percent_of_internet_users_in_the_us.html.

offensive or harassing messages through the Internet and not abusing social networking sites.⁵

The Internet can be an exciting place for children and teenagers because they are able to adopt different identities and interact away from adult supervision.⁶ Yet this same autonomy also makes the Internet dangerous. Just as teenagers can create personas that are different from their real world identity, so too can sexual predators⁷ and cyberbullies.⁸ High profile cases involving Internet safety, such as the Megan Meier suicide⁹ and the television show “To Catch a Predator,”¹⁰ have sparked legislative action.¹¹ Several states have proposed or enacted statutes designed to address internet safety.

Part II of this Note will discuss recent state legislative attempts to regulate social networking sites from sex offenders. Part III will examine state statutes addressing cyberbullying. Part IV will evaluate proposed solutions to online safety issues. Finally, Part V advocates that

5. For purposes of this Note Internet use considered not “moral” or “ethical” would include pretending to be someone else online, creating false personas to harass others, and posting and spreading false information using social networking capabilities.

6. ROBIN M. KOWALSKI, SUSAN P. LIMBER & PATRICIA W. AGATSTON, *CYBERBULLYING* 8 (2008).

7. Research has shown that the likelihood that a sexual predator will contact a child and exploit the child offline is very low. On the other hand, the likelihood of exposure to cyberbullying through social networking sites is much more likely and should be addressed. *See* SAMEER HINDUJA & JUSTIN W. PATCHIN, *BULLYING BEYOND THE SCHOOLYARD: PREVENTING AND RESPONDING TO CYBERBULLYING* 90 (2009).

8. Cyberbullying is difficult to define because it encompasses different communication technologies and involves different methods of bullying. At its core, cyberbullying involves “bullying through the use of technology such as the Internet and cellular phones.” KOWALSKI, LIMBER & AGATSTON, *supra* note 6, at 43.

9. Megan Meier was a thirteen-year-old girl from Missouri who committed suicide after she was cyberbullied by a classmate’s mother, Lori Drew. Drew created a MySpace account for the fictitious “Josh Evans” and used it to flirt with Meier to try and get information about Meier. Drew wanted retribution against Meier for perceived slights against her daughter. While pretending to be “Josh Evans” Drew allegedly told Meier that the “world would be a better place” without her. Meier committed suicide in her home. *See* Christopher Maag, *A Hoax Turned Fatal Draws Anger But No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23.

10. “To Catch a Predator” is an American reality television show that focuses on identifying would-be pedophiles through hidden camera investigations. The pedophiles make plans via internet chat to enter into sexual relations with a “minor,” who is actually a decoy. *See* To Catch a Predator Home Page, http://www.msnbc.msn.com/id/10912603/ns/datetime_nbc-to_catch_a_predator.

11. Larry Margasak, *House Members Seek Ways to Stop Internet Bullying*, THE WASHINGTON POST, Sept. 30, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/09/30/AR2009093004014.html> (last visited Oct 1, 2009).

comprehensive education is the best solution at this time to social networking safety and cyberbullying.¹²

II. SOCIAL NETWORKING SITES AND SEX OFFENDERS

This Part will first give a brief background of self-regulatory attempts by social networking sites. Next, this Part will analyze legislative attempts by Illinois, Georgia, Utah, and New Jersey to address social networking safety issues. Finally, this Part will examine studies about the actual threat of online predators.

A. BACKGROUND AND SELF-REGULATION

In recent years, social networking sites have grown in popularity and become the source of many online safety concerns. A social networking site is a “[w]eb site that provides a virtual community for people interested in a particular subject or just to ‘hang out’ together.”¹³ Social networking sites allow users to share their interests within online communities, meet new people, and interact with their real-life friends in the virtual world.¹⁴ For example, users can share their pictures with their friends and express themselves through online status updates.¹⁵ Users can also meet new friends through shared interests or mutual friends.

The anonymity of the Internet enables bad actors to create false identities on social networking sites and potentially harm other users. This danger is applicable to users of all ages, but this Note will focus on efforts that lawmakers have taken to protect children from bad actors, such as sexual predators. Social networking sites have taken steps to regulate sex offenders on social networking sites. In January 2008, the attorneys general from forty-

12. This Note is a survey of recent legislation and proposed solutions to address online safety. Therefore, the scope of the legislation that this Note will address is limited to the period directly before this piece was written in late 2009. The Note is not meant to be an exhaustive exploration of the topics of social networking or cyberbullying. Rather, the Note examines some of the latest efforts to address online safety issues for children.

Additionally, the Note discusses recent state statutes by grouping them into “social networking sites” and “cyberbullying.” These broad categories are for the convenience of this Note and do not represent an attempt to categorize all online safety measures into these two groupings.

13. Definition of Social Networking, PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=social+networking&ci=55316,00.asp (last visited Oct. 25, 2009).

14. HINDUJA & PATCHIN, *supra* note 7, at 188.

15. A user on Facebook, for example, can update their “status,” which is then distributed to all the user’s virtual friends. If the user entered “I had a rough day” as his status, his friends who log onto Facebook would be able to view that message.

nine states reached an agreement with the social networking site MySpace to protect children who used its platform.¹⁶ This agreement included age-protecting certain areas of MySpace and preventing users from changing their age to shift between the age-restricted areas.¹⁷ Therefore, a user would not be able to switch between the adult area and an area intended for children.

The agreement was significant because cooperation between MySpace and governing bodies had once been tenuous. MySpace previously refused to give the names of users who were sex offenders to the attorneys general for fear of violating privacy rights, as well as the Electronic Communications Privacy Act of 1986, which technically prohibits private information from disclosure without a subpoena.¹⁸ However, MySpace later agreed to share with the attorneys general information that it retrieved from Sentinel Safe,¹⁹ a database that contains data aggregated from state sex offender registries.²⁰ MySpace also agreed to work within each state's specific process and requirements to ensure that the Sentinel Safe data was shared.²¹

Facebook, which has supplanted MySpace as the dominant social networking site,²² has also taken steps to stop sex offenders from lurking on its network. In May 2008, Facebook reached a similar agreement with the attorneys general from forty-nine states.²³ The agreement addressed automatic warnings when underage users are in danger of giving out personal

16. Texas was not part of the agreement. Proskauer Rose LLP Privacy Law Blog, State Attorneys General Announce Agreement with MySpace to Protect Children Online: Privacy Law Blog, Jan 15, 2008, <http://privacylaw.proskauer.com/2008/01/articles/childrens-online-privacy-prote/state-attorneys-general-announce-agreement-with-myspace-to-protect-children-online/> (last visited Sep 28, 2009).

17. *Id.*

18. Elizabeth Dunbar, *Citing Privacy, MySpace Won't Give Names of Sex Offenders*, USATODAY.COM, May 16, 2007, http://www.usatoday.com/tech/news/2007-05-16-myspace-sex-offenders_N.htm; Caroline McCarthy, *MySpace to Provide Sex Offender Data to State AGs*, CNET NEWS, May 21, 2007, http://news.cnet.com/MySpace-to-provide-sex-offender-data-to-state-AGs/2100-1030_3-6185333.html.

19. MySpace had announced its partnership with Sentinel to create a new technology to identify sex offenders in December of 2006. *See* Michael Calore, *MySpace Takes Steps to Stop Sex Offenders*, WEBMONKEY, Dec. 5, 2006, http://www.webmonkey.com/blog/MySpace_Takes_Steps_To_Stop_Sex_Offenders.

20. McCarthy, *supra* note 18.

21. *Id.*

22. Tony Bradley, *Facebook Skyrockets, MySpace Plummet, Twitter Grows*, PC WORLD, Oct. 12, 2009, http://www.pcworld.com/businesscenter/article/173476/facebook_skyrockets_myspace_plummet_twitter_grows.html (last visited Jan 26, 2010).

23. Texas was not a part of the agreement; Erick Schonfeld, *Facebook to Announce Safety and Privacy Deal with 49 States*, TECH CRUNCH, May 8, 2008, <http://www.techcrunch.com/2008/05/08/breaking-facebook-to-announce-safety-and-privacy-deal-with-49-states/>.

information and restricting the ability of users to change their age to under eighteen.²⁴ During the period between May 1, 2008 and January 31, 2009, Facebook removed more than 5,500 convicted sex offenders from its social networking website.²⁵ MySpace reported that over a two-year period it had removed 90,000 convicted sex offenders from its social networking site.²⁶

There have also been legislative efforts in addition to these self-regulating deals. Many of the legislative efforts present constitutional concerns and could be found void for vagueness. “Void for vagueness” is a legal concept that states that a given statute is void and unenforceable if it is too vague for the average citizen to understand and does not provide fair warning.²⁷ It would be unjust to punish a person without providing clear notice about what conduct is prohibited.²⁸ Also, if the contours and minimum guidelines of the laws are not objective, enforcement of the law may be uneven and prone to “personal predilections.”²⁹ Legislative efforts could run afoul of the Constitution if the statutory language is not clearly defined and a reasonable citizen would not know what conduct was permitted and what conduct was prohibited.³⁰ The next Sections will discuss recent legislative efforts by Illinois, Georgia, Utah and New Jersey.

B. ILLINOIS

In August 2009, Illinois Gov. Pat Quinn signed a bill that banned sex offenders from social networking sites.³¹ House Bill 1314 made it a felony for

24. Bradley, *supra* note 22.

25. *Facebook Has Removed 5,585 Sex Offenders*, CBSNEWS.COM, Feb. 20, 2009, <http://www.cbsnews.com/stories/2009/02/20/tech/main4815103.shtml> (last visited Sep 28, 2009).

26. *MySpace Kicks Out 90,000 Sex Offenders, Connecticut AG Says*, CNN.COM, Feb. 4, 2009, <http://www.cnn.com/2009/TECH/02/03/myspace.sex.offenders/index.html>; Erick Schonfeld, *Citing Progress, MySpace Says 90,000 Sex Offenders Blocked From Site*, TECH CRUNCH, Feb. 3, 2009, <http://www.techcrunch.com/2009/02/03/responding-to-subpoena-myspace-says-90000-sex-offenders-blocked-from-site>.

27. *See* Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926).

28. *Id.*

29. *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)(citations omitted).

30. *Grayned v. Rockford*, 408 U.S. 104, 108 (1972). In *City of Chicago v. Morales*, 527 U.S. 41 (1999), Chicago adopted an anti-loitering ordinance targeted at gangs. If a police officer reasonably believed that at least one person in a group of two or more loitering people was a gang member, the officer could order them to leave the area. Failure to leave was a misdemeanor offense. The Court found the definition of “loitering” to be vague and the requirements to avoid breaking the law unclear. *City of Chicago*, 527 U.S. at 59–60.

31. Sharon Gaudin, *Illinois Outlaws Sex Offenders from Using Facebook, MySpace*, COMPUTER WORLD, Aug. 14, 2009, http://www.computerworld.com/s/article/9136668/Illinois_outlaws_sex_offenders_from_using_Facebook_MySpace?source=CTWN_LE_nlt_security_2009-08-17.

a sex offender to access a social networking site for any purpose.³² The purpose of the law was to make it more difficult for sex offenders to meet new potential victims.³³ This law is one of the latest actions³⁴ by states to deal with the issue of sex offenders using social networking sites to interact with children and seek new victims.³⁵

The bill may be too broad to be workable. The bill fails to specify which social networks are covered and instead broadly defines “social networking website” as

an Internet website containing profile web pages of the members of the website that include the names or nicknames of such members, photographs placed on the profile web pages by such members, or any other personal or personally identifying information about such members and links to other profile web pages on social networking websites of friends or associates of such members that can be accessed by other members or visitors to the website. A social networking website provides members of or visitors to such website the ability to leave messages or comments on the profile web page that are visible to all or some visitors to the profile web page and may also include a form of electronic mail for members of the social networking website.³⁶

This definition is broad and may extend too far. For instance, professional networking sites such as LinkedIn would qualify under this definition. Thus, a sex offender conviction could take away one’s ability to post a resume in an attempt to secure employment—a result that seems unreasonable.³⁷ Forbidding sex offenders from using professional social networking sites would stunt their progress as they try to reintegrate into society. Thus, a careful balance must be struck between protecting potential sex offender

32. H.R. 1314, 96th Gen. Assem. (Ill. 2009).

33. Gaudin, *supra* note 31.

34. State attorneys general have previously created partnerships with two of the major social networking sites, MySpace and Facebook, to stop convicted sex offenders from using the social networking sites. See Richard M. Guo, Note, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 638 (2008).

35. In November 2009, an attempt by the United Kingdom government to keep sex offenders from social networking sites was halted because “such a move would breach human rights laws.” There were also concerns that the plan would be incompatible with the right to privacy. Jamie Doward, *Bid to Block Pedophiles from Facebook Fails*, THE OBSERVER, Nov. 8, 2009, <http://www.guardian.co.uk/technology/2009/nov/08/facebook-sex-offenders-law>.

36. H.R. 1314, 96th Gen. Assem. (Ill. 2009).

37. No Social Networking Web Site Use For Illinois Sex Offenders, cbs2chicago.com, Aug. 13, 2009, <http://cbs2chicago.com/topstories/sex.offenders.web.2.1127258.html> (last visited Sep 27, 2009).

victims and not overly restraining offenders so that they are unable to find employment or reintegrate into society.

Furthermore, there are many different types of crimes for which one will be labeled a sex offender, ranging from the serious sexual offenses³⁸ to non-dangerous crimes. As long as the crime is of a sexual nature or contains a sexual element, the conviction will result in the label of sex offender.³⁹ One example of a non-dangerous sexual offense is consensual sex between two teens whose ages are on different sides of the statutory rape line.⁴⁰ If one of the teenagers is eighteen, the other is seventeen, and the age of consent in that state is eighteen, then the eighteen-year-old would be guilty of statutory rape.⁴¹ However, the sexual interaction was consensual and it is only because one of them was eighteen and legally of age and the other was technically still a minor that the sex constitutes a crime. The eighteen-year-old is then labeled as a “sex offender” and will have all the corresponding restrictions and stigma placed upon him or her.

Under the Illinois statute, a child or teenager convicted of a sex crime will not be able to access LinkedIn and other professional networking sites in his adult life. Though his crime was significantly less serious than other sex offenders, the online handicaps remain the same. The broad range of what constitutes a sex offender is hard to reconcile with the sweeping prohibition of accessing social networking sites. In an increasingly interconnected world,

38. For example, crimes such as sexually abusing children and rape would qualify as serious sex offenses.

39. Joseph L. Lester, *Off to Elba! The Legitimacy of Sex Offender Residence and Employment Restrictions*, 40 AKRON L. REV. 339, 342 (2007).

40. Another example is sexting. Sexting involves sexually explicit messages or photos that are electronically transmitted, most often through cell phones. Oftentimes the sexting involves teenagers taking nude pictures of themselves and sending the images via text message to their partner. The transmission of nude pictures over cell phones could constitute possession of child pornography, but the perpetrators are children themselves. The crime in this case is not the traditional sexual pervert who downloads child pornography, but is the transmission of one's own image to one's significant other. But, the treatment of both is the same—they are sex offenders if they are convicted. See “Sexting” Shockingly Common Among Teens, CBSEWS.COM, Jan. 15, 2009, <http://www.cbsnews.com/stories/2009/01/15/national/main4723161.shtml> (last visited Oct 25, 2009); See generally Elizabeth C. Eraker, *Stemming Sexting: Sensible Legal Approaches to Teenagers' Exchange of Self-Produced Pornography*, 25 BERKELEY TECH. L.J. ____ (forthcoming 2010) for more information about sexting.

41. Statutory rape is a term used to describe sexual relations that occur when one participant is below the age required to legally consent to the behavior. It usually refers to adults engaging in sex with minors under the age at which individuals are considered competent to give consent to sexual conduct. Kay L. Levine, *The External Evolution of Criminal Law*, 45 AM. CRIM. L. REV. 1039, 1058 (2008).

the role of social networks is growing at a rapid pace. To make it illegal for some sex offenders to participate is more punishment than is necessary.

Another important issue is the enforceability of banning sex offenders on social networking sites. The ability to create pseudonyms and varied email addresses that contain no identifying information means that just about anyone can create a social networking profile. It would be costly and time-consuming for the government to attempt to ensure compliance by every sex offender.

C. GEORGIA AND UTAH

Georgia recently revised its sex offender statute to increase the requirements for sex offender registration.⁴² In addition to the traditional home residence information, sex offenders must also register their email addresses and passwords.⁴³ The registration of email addresses is not novel; several states previously adopted provisions requiring sex offenders to provide email addresses.⁴⁴ However, only Utah had previously required disclosure of all Internet passwords.⁴⁵

1. *Utah*

The Utah sex offender registry statute required that sex offenders provide the Department of Corrections all Internet identifiers and the addresses the offender used for routing or self-identification in Internet communications or postings.⁴⁶ The sex offender also had to turn over the name and Internet addresses of the websites where he registered with an online identifier, as well as the passwords and user names associated with those websites. A related statute required sex offenders to give the Department of Corrections the password to an “online identifier,” which was defined as “any electronic mail, chat, instant messenger, social networking, or similar name used for Internet communication.”⁴⁷ The provisions in the Utah statute essentially meant that a majority of interactive Internet use by a sex offender would have to be disclosed, although the online identifier and password themselves would not be disclosed to the public.

42. GA. CODE ANN. § 42-1-12 (2009).

43. *Sex Offenders Must Hand Over Passwords*, MSNBC.COM, Dec. 30, 2008, <http://www.msnbc.msn.com/id/28437829> (last visited October 27, 2009).

44. *Id.*

45. H.R. 34, 2008 Gen. Sess. (Utah 2008), UTAH CODE ANN. § 77-27-21.5(12) (2008).

46. *Id.*

47. UTAH CODE ANN. § 77-27-21.5(2)(c).

In *Doe v. Shurtleff*, a man affected by the legislation challenged the Utah law on constitutional grounds.⁴⁸ Doe argued his First Amendment right to anonymous free speech was violated when he was required to hand over his passwords to the Utah Department of Corrections (UDOC).⁴⁹ The District Court judge found that the Utah statute violated plaintiff's right to free speech and that if "Doe provide[d] the UDOC with his Internet information and [knew] that there [were] no statutory limits on how that information [could] be used by the UDOC, or others, he [would be] less likely to engage in protected anonymous speech."⁵⁰ On May 12, 2009, amendments were made to the statute and the requirement to provide Internet passwords was removed.⁵¹ The scope of discretion was also limited so that the information could only be used to investigate sex-related crimes or to make disclosures permitted by Utah's Government Records Access Management Act (GRAMA).⁵²

Doe also argued the Utah statute resulted in unlawful and unreasonable search and seizure under the Fourth Amendment.⁵³ To establish a violation of the Fourth Amendment, a plaintiff had to show that he has a reasonable expectation of privacy. The court held that because Doe presumably accessed the Internet through an IP address linked to his subscriber information, and thus his identity, Doe would have no reasonable expectation of privacy in those user names.⁵⁴

2. Georgia

The Georgia statute adds "[e]-mail addresses, usernames, and user passwords" to the list of required registration information.⁵⁵ The Georgia statute defines "user password" to pertain to "e-mail messages and interactive online forums."⁵⁶ The Utah statute was very similar to Georgia's,

48. *Doe v. Shurtleff*, No. 1:08-CV-64, 2008 WL 4427594 (D. Utah Sep. 25, 2008), *rev'd*, 2009 WL 2601458 (D. Utah Aug. 20, 2009). The government defendant moved for, and was granted, a Rule 60(b) vacating order after the law was amended.

49. Susan Brenner, *Law Requiring Sex Offenders to Hand Over All Internet Passwords Going Too Far?*, CIRCLEID, Jan. 27, 2009, http://www.circleid.com/posts/law_sex_offenders_internet_passwords/ (last visited Jan. 24, 2010).

50. *Doe v. Shurtleff*, No. 1:08-CV-64, 2008 WL 4427594 at *4.

51. *Doe v. Shurtleff*, No. 1:08-CV-64, 2009 WL 2601458 (D. Utah Aug. 20, 2009).

52. *Id.* at *2; GRAMA is a statute that allows the public to obtain copies of government records. UTAH CODE ANN. § 63G-2-101, *et seq.*

53. *Doe v. Shurtleff*, 1:08-CV-64, 2009 WL 2601458, at *5.

54. *Id.*

55. S.B. 474, 2007–2008 Leg., Gen. Assem. (Ga. 2008), GA. CODE ANN. § 42-1-12(a) (2009).

56. *Id.*

but it also required disclosure of passwords for email, chat, social networking sites and other means of Internet communication. Given the similarity between the two laws, it is likely that the same or similar First and Fourth Amendment claims will be made in at least one pending challenge to the Georgia statute.⁵⁷ The results in Utah foreshadow the pending challenge to the Georgia statute. Accordingly, a court will possibly strike down the Georgia law.

Also, much like the Illinois statute, authorities will have difficulty monitoring offenders under the Georgia law. Sex offenders have a strong incentive to lie or disclose incomplete email and password information, and it would not be the best use of resources to attempt to track down every username and password owned by every sex offender. Even if a sex offender were to hand over all her passwords, the barrier to create a new username and password is very low—the sex offender could easily create a new name that the government would not have in its records.

D. NEW JERSEY

New Jersey Assembly Bill 3757, proposed in February 2009, also targeted social networking sites. This bill introduced the “Social Networking Safety Act,” which was “intended to deter cyber-bullying and the misuse of social networking Web sites.”⁵⁸ The first piece would prohibit the use of social networks to transmit “sexually offensive communication” to minors in New Jersey.⁵⁹ The second piece proposes to make it illegal for a person to transmit a “harassing communication” through a social networking site to or about a person located in New Jersey.⁶⁰ “Sexually offensive communication” is defined as

any communication which a reasonable person would believe is intended to solicit or request a person to engage in sexual activity, and any communication depicting or describing nudity, sexual conduct or sexual excitement when it: (1) predominantly appeals to a prurient interest in sex; (2) is patently offensive to prevailing

57. Bill Rankin, *Judge Hears Challenge to Sex Offender Law*, ATLANTA JOURNAL-CONSTITUTION, Aug 25, 2009, <http://www.ajc.com/news/judge-hears-challenge-to-123557.html>. As of this writing, January 23, 2010, the case is currently before U.S. District Judge Bill Duffey in the Northern District of Georgia. Terrence White, a convicted sex offender in Georgia, has urged the judge to block the law because it violates his constitutional rights.

58. Wendy Davis, Proposed NJ Law Would Require Social Nets to Police Sites, Online Media Daily, March 31, 2009, http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=103115 (last visited Jan. 24, 2010).

59. A.B. 3757, 213th Leg. (N.J. 2009).

60. *Id.*

standards in the adult community as a whole with respect to what is suitable material or conduct for minors; and (3) taken as a whole, is without serious literary, artist, political or scientific value for minors.⁶¹

One who violates this statute and sends out a sexually offensive communication would be liable to the social networking operator as well as the recipient of the “sexually offensive communication.” The transmitter of the communication would be liable to the social networking site operator in a civil action for \$1,000 plus reasonable attorney fees for each violation.⁶² The transmitter would be liable to the recipient of the communication for damages of \$5,000 plus attorney fees, or actual damages, whichever is greater.⁶³

The definition of “sexually offensive communication” relies on standards that are not particularly clear. To determine what content is “suitable for minors,” the statute looks to “prevailing standards in the adult community.”⁶⁴ Every transmitter of a message will likely have a different definition of what that is appropriate. If the statute is too vague or unclear, it could be found void for vagueness.⁶⁵

The second piece of the statute appears to address cyberbullying. It prohibits the transmission of a “harassing communication,” which is defined as “any communication which is directed at a specific person, serves no legitimate purpose, and a reasonable person would believe is intended to threaten, intimidate or harass another person.”⁶⁶ No definition of “harass” or “threaten” is given, which could prove problematic in attempts to develop clear and objective boundaries for enforcement. Additionally, the phrase “serves no legitimate purpose” is indefinite as what is reasonably “legitimate” to one person may not be “legitimate” to another person. Further still, there are potential First Amendment issues, as this statute potentially infringes on the First Amendment right to speak one’s mind in an abrasive and harassing way. Courts have carved out exceptions to free speech laws in situations when there were threats of imminent unlawful violence, but it is very likely

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

65. *See supra* Part II.A for more on “void for vagueness.”

66. A.B. 3757, 213th Leg. (N.J. 2009).

that the First Amendment would protect harassing speech not accompanied by threats of imminent unlawful violence.⁶⁷

The statute also requires that a social networking website remove the “sexually offensive communication” or “harassing communication” without unreasonable delay.⁶⁸ If social networking sites do not comply, they would violate the New Jersey Consumer Fraud Act⁶⁹ and can be sued.⁷⁰ However, the statute provides a safe harbor for social networking sites that display buttons to report violations, conduct reviews in an expedient fashion of any report of violations, block violators when appropriate, and contact the police when appropriate.⁷¹

The Social Networking Safety Act was written to avoid conflict with Section 230 of the Communications Decency Act (“Section 230”).⁷² Section 230 grants protection for online intermediaries and states that “[n]o 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.”⁷³ Section 230 has been interpreted broadly and has granted immunity to Internet Service Providers (ISPs) even when the ISP had notice that the content was tortious.⁷⁴ The proposed statute states that the bill should not be “construed to permit a civil action against an interactive computer service that is inconsistent with the provisions of [Section 230].”⁷⁵ This attempt to avoid preemption by the federal statute renders the New Jersey bill relatively toothless. Section 230 would probably apply to most, if

67. *See* *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (holding that the government could not punish inflammatory speech unless it is likely to incite imminent lawless action); *see also* *Davis*, *supra* note 58.

68. A.B. 3757, 213th Leg. (N.J. 2009).

69. New Jersey Consumer Fraud Act, N.J. STAT. ANN. § 56:8-1 *et seq.* (2010), <http://www.state.nj.us/lps/ca/laws/ConsumerFraudAct.pdf>
70. *Id.*; Posting of Grayson Barber to Freedom to Tinker, A "Social Networking Safety Act", <http://www.freedom-to-tinker.com/blog/grayson/social-networking-safety-act> (Mar. 25, 2009, 14:44 EST) (last visited Sep 29, 2009).

71. A.B. 3757, 213th Leg. (N.J. 2009).

72. Codified at 47 U.S.C. § 230(c)(1)(2000).

73. 47 U.S.C. § 230(c)(1)(2000).

74. *See* *Zeran v. America Online, Inc.*, 129 F.3d 327, 332 (4th Cir. 1997) (holding that even notice of the content cannot serve as a basis for liability). Courts have found Section 230 to protect social networking sites from tortious actions. *See* *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008) (finding that a social networking site was under Section 230 and not liable for tortious actions based on user-generated content). *See generally* Shahrzad Radbod, *Craigslist – A Case for Criminal Liability for Online Service Providers?*, 25 BERKELEY TECH. L.J. ____ (forthcoming 2010).

75. N.J. A.B. 3757.

not all, civil suits brought under the statute thereby preempting the New Jersey bill.

The proposed New Jersey statute also puts a burden on a specific technology and type of website: the social networking site. Email providers, blogs, or wikis do not have the same burden.⁷⁶ The success and popularity that social networks have attained with youths in recent years has generated additional scrutiny.⁷⁷ These requirements represent an added cost and a higher barrier to entry for new social networking sites. If there are too many regulatory burdens on the social networking sites, then there may be fewer new social networking sites. This would result in a net loss to society as there would be fewer choices and less incentive for social networking sites to be innovative if there is little competition. A lack of innovative network development would hinder the hallmarks of social networking: individual expression and community building online.⁷⁸

The statutes of Illinois, Georgia, and New Jersey are problematic and unlikely to be effective. Notwithstanding the constitutional concerns, the success of the Illinois and Georgia statutes hinges on the sex offenders providing accurate and truthful information as well as voluntarily abstaining from creating further accounts. This is unlikely to occur. The New Jersey statute that addresses “sexually offensive communication” also may falter because of its vague standards. These statutes are unlikely to be effective against sexual predators. However, some evidence suggests that the sexual predator problem is not as big as the media portrays.

E. STATISTICS AND SOLUTIONS

The Crimes Against Children Research Center (CACRC) conducted a Youth Internet Safety Survey, which showed that the percentages of youth who received sexual solicitations declined from 19% in 2000 to 13% in 2006.⁷⁹ This decrease in reported sexual solicitations is significant given the increase of time young people spend on the Internet.⁸⁰ This decrease also

76. Barber, *supra* note 70.

77. *See supra* Part II.A.

78. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1151–60 (2009).

79. BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE TO THE MULTI-STATE WORKING GROUP ON SOCIAL NETWORKING OF STATE ATTORNEYS GENERAL OF THE UNITED STATES 14 (2008), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

80. NANCY E. WILLARD, CYBERBULLYING AND CYBERTHREATS 67 (2007).

suggests young people are “gaining greater skills in avoiding the online places where such contacts are being made.”⁸¹

Most of the recipients of sexual solicitation (81%) were between the ages of fourteen and seventeen.⁸² Other adolescents and young adults between eighteen and twenty-one, not older adults, were the source of most of the solicitations.⁸³ Furthermore, not all solicitations came from strangers; one detailed study found that about 14% came from offline friends or acquaintances.⁸⁴ More importantly, very few of the solicitations resulted in offline contact.⁸⁵ Also, teenagers seem to shrug off the solicitations without experiencing distress.⁸⁶ These statistics suggest that publicity about online predators preying on innocent children exaggerates the actual harm.⁸⁷ The lack of actual offline contact and the decreasing number of solicitations suggests that the likelihood of youths encountering online sexual predators is quite low.⁸⁸ Online predator arrests comprise only 1% of arrests for sex crimes against minors.⁸⁹ However, any online contact achieved by a sexual predator is a serious threat and children should be warned of the dangers that can result from offline contact. None of the state statutes previously discussed were proactive attempts to halt sexual solicitation by predators online.

A better solution is to educate children on safe Internet practices and on the realities of sexual predators. Teaching children about safe Internet practices and cautioning them against sharing too much information online will have lasting effects. Just as children learn to not take candy from

81. *Id.*

82. Janis Wolak, Kimberly Mitchell & David Finkelhor, National Center for Missing and Exploited Children, *Online Victimization of Youth: Five Years Later 17* (2006), available at <http://www.unh.edu/ccrc/pdf/CV138.pdf>. The Berkman report further detailed a study that found that younger age groups were not as likely to have experienced sexual solicitation. Two percent of fourth through six graders were asked about their bodies, compared with 11% of seventh through ninth graders and 23% of tenth through twelfth graders. In this study, 3% of the two older groups admitted to asking others for sexual content. Berkman Center, *supra* note 79.

83. BERKMAN CENTER, *supra* note 79.

84. *Id.*

85. *Id.*

86. *Id.*

87. See Janis Wolak et. al., *Online “Predators” and their Victims: Myths Realities and Implications for Prevention and Treatment*, 63 AM. PSYCH. 2, 111–28 (2008), available at <http://www.unh.edu/ccrc/pdf/Am%20Psy%202-08.pdf>.

88. Berin Szoka & Adam Thierer, *Cyberbullying Legislation: Why Education is Preferable to Regulation*, PROGRESS & FREEDOM FOUND. (2009), available at <http://www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf>.

89. *Id.*

strangers, they can also learn to not share personal information and about the wrongs of internet harassment. If children learn about ethical internet practices, it may become second nature to them and instances of severe cyberbullying may decrease.

III. CYBERBULLYING AND CYBERSTALKING

A. CYBERBULLYING STATISTICS⁹⁰

Statistics suggest that cyberbullying will impact a greater percentage of youth than sexual predators will in the United States. A recent report by the Internet Safety Technical Task Force⁹¹ concluded that bullying and harassment by peers “are the more frequent threats that minors face, both online and offline.”⁹² Nine studies done in 2006 found that the percentage of children who were cyberbullied ranged from 9% to as high as 53%.⁹³ The vast majority of these studies found that greater than 17% of children had been cyberbullied.⁹⁴ A 2006 nationwide survey conducted by the Opinion Research Corporation for Fight Crime found that cyberbullying occurs frequently. The study found that “31% of 12–14-year-olds and 40% of 15–17-year-olds reported that in the last year ‘mean, threatening or embarrassing [things were] said about [them] through email, instant messages, websites such as MySpace, Friendster, etc., chat rooms or text messages.’”⁹⁵ Most scholars agree that approximately 15–20% of students are regular victims of bullying behavior while about 10% of American children are subject to extreme victimization by bullying.⁹⁶ The aggregate numbers from the various

90. Cyberbullying statistics, like all research, must be evaluated in the correct context. Some cyberbullying statistics are gathered through online surveys and the online nature of the surveys might skew the results because those most likely to fill out the surveys are those who are already frequent Internet users. This caveat is not intended to diminish the studies’ results. As with all research, the context in which the data was gathered should be considered. *See* KOWALSKI, LIMBER & AGATSTON, *supra* note 6, at 69.

91. “The Internet Safety Technical Task Force (ISTTF) is a group of Internet businesses, non-profit organizations, academics, and technology companies that have joined together to identify effective tools and technologies to create a safer environment on the Internet for youth.” BERKMAN CENTER, *supra* note 82, at 4.

92. *Id.*

93. KOWALSKI, LIMBER & AGATSTON, *supra* note 6, at 71.

94. *Id.*

95. Darryn Cathryn Beckstrom, *State Legislation Mandating School Cyberbullying Policies and the Potential Threat to Students’ Free Speech Rights*, 33 VTLR 283, 288 (2008) (quoting Opinion Research Corporation for Fight Crime study).

96. Gia E. Barboza, *The Behavioral, Socio-Legal and Institutional Antecedents of Peer Harassment and Bullying in School: How Do Legal Norms Interact With Multiple Contexts of Childhood Aggression?*, 45 NO 3 CRIM LAW BULLETIN ART 8 (2009).

studies conducted in 2006 fall within this range, with some studies indicating much higher numbers for cyberbullying.⁹⁷

Hinduja and Patchin attribute the range of cyberbullying statistics to factors such as the varying ages of the respondents, the reporting periods of the different surveys, and the definition used for “cyberbullying.”⁹⁸ Hinduja and Patchin also point out that different methodologies might yield different results. For instance, the respondents could be questioned in-class, over the phone, or through the Internet. The Internet-based samples tend to report higher numbers of aggressors and victims because those respondents are more likely to use the Internet regularly and are most likely to experience cyberbullying.⁹⁹ An accurate evaluation of cyberbullying statistics will consider these factors. Regardless of the specific cyberbullying numbers, the effects of bullying on children are well documented.

1. *Effect on Children*

Bullying can have lasting psychological effects on children. For instance, bullied children are more likely to be anxious and to think about committing suicide.¹⁰⁰ Unfortunately, the problems are not only psychological and emotional; the effects can extend into the physical realm as well. In a study of Dutch schoolchildren aged nine to twelve, researchers found that bullied children were “approximately three times as likely to experience headaches, feel listless and wet their beds.”¹⁰¹ Studies have shown that the effects last into adulthood. One study found that male young adults who were bullied in junior high were likely to suffer from low self-esteem and depression a decade after the physical bullying had ended.¹⁰²

Bullying is damaging enough in its traditional schoolyard form, and the Internet only magnifies the effects. The breadth and reach of the Internet allows one’s humiliation at the hands of a bully to reverberate across cyberspace. Whereas only a handful of local students might witness a traditional bullying incident, YouTube and digital cameras make the spread of humiliation available to a much wider audience. Recent legislative efforts to address cyberbullying are discussed in Sections III.B and III.C.

97. KOWALSKI, LIMBER & AGATSTON, *supra* note 6, at 71.

98. HINDUJA & PATCHIN, *supra* note 7, at 49.

99. *Id.*

100. KOWALSKI, LIMBER & AGATSTON, *supra* note 6, at 26.

101. *Id.*

102. *Id.* at 27.

B. TELEPHONE HARASSMENT LAWS

In February 2009, Idaho H.B. 82 proposed to amend telephone harassment laws to apply to Internet communications.¹⁰³ The amendment would impose a misdemeanor on “every person who, with intent to annoy, terrify, threaten, intimidate, harass or offend, telephones or emails or sends a text message or posts on the internet to another” and with “obscene, lewd or profane language.”¹⁰⁴ The proposed statute defined “internet posts” as “use of internet sites including, but not limited to, social networking sites and personal blogs.”¹⁰⁵ The statute did not provide definitions of “annoy” and “terrify.”

The amendment of an existing telephone harassment law is not unprecedented. In January 2006, the federal government amended the Federal Telephone Harassment Statute¹⁰⁶ in an attempt to address the growing cyberstalking problem.¹⁰⁷ The pre-amendment statute outlawed anonymously and knowingly making a telephone call or using a “telecommunications device” to “annoy, abuse, threaten or harass” a person.¹⁰⁸ The phrase “telecommunications device” was amended to include “any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or part, by the Internet.”¹⁰⁹

The lack of definition for “annoy” was problematic. Words such as “annoy” are very difficult to define and use as a standard for enforcement. In *United States v. Bowker*, the Sixth Circuit examined the federal statute and found that the word “annoy” was constitutional because it upheld Congressional intent to protect individuals from fear, and the term did not chill political or free speech.¹¹⁰ The *Bowker* analysis preceded the amendment to “telecommunications device,” but the analysis for the newly amended statute might be the same. Naomi Harlin Goodno posits that “read in context, ‘annoy,’ like ‘threaten’ and ‘harass,’ is not unconstitutional because its purpose is to prohibit messages aimed at instilling fear, whether the

103. H.R. 82, 60th Leg., Reg. Sess. (Idaho 2009), available at <http://legislature.idaho.gov/legislation/2009/H0082.pdf>.

104. *Id.*

105. *Id.*

106. 47 U.S.C. § 223 (2006).

107. Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 148–49 (2007).

108. 47 U.S.C. § 223(a)(1)(c) (2006).

109. *Id.* (adding this language to 47 U.S.C. § 223(h)(1)(C)).

110. *United States v. Bowker*, 372 F.3d. 365 (6th Cir. 2004), vacated on other grounds, 543 U.S. 1182 (2005).

message is sent via the telephone or the Internet.”¹¹¹ The analysis in *Bowker* could apply to Idaho H.B. 82 and other similar legislative proposals. If these legislative efforts pass into law courts could find “annoy” or other similarly ambiguous words constitutional.

Ultimately, Idaho H.B. 82 was held in session and did not pass into law.¹¹² However, the above analysis could hold true for future legislative attempts to amend telephone harassments laws to fit Internet harassment.

C. TEXAS

Texas H.B. 2003 amended the penal code to create the crime of online harassment. Unlike the Idaho bill, Texas H.B. 2003 went into effect September 1, 2009 and there has already been at least one arrest of a teenager under the new law.¹¹³

The bill prohibits a social network user from using the name or persona of another to create a Web page or post comments within a social networking site without consent.¹¹⁴ The social network user must not have the intent to “harass, embarrass, intimidate or threaten” another on a “commercial social networking site.”¹¹⁵ The statute defines “commercial social networking site” as

[a]ny business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. *The term does not include an electronic mail program or a message board program.*¹¹⁶

The exclusion of email and message boards creates a dual system wherein one could harass through Facebook messages, which are delivered to users

111. Goodno, *supra* note 107, at 150.

112. See Hannah Saona, *2009 Legislative Session in Review*, IDAHO LIBERTY (ACLU of Idaho), Spring/Summer 2009, at 4, http://www.acluidaho.org/images/Idaho_Liberty_Spring_2009.pdf; see Bill Status House Bill 82, State of Idaho Legislature, <http://legislature.idaho.gov/legislation/2009/H0082.htm>.

113. James Muñoz, *Teen Arrested on Charges of Online Harassment*, KHOU.COM, Oct. 13, 2009, <http://www.khou.com/news/national/66205747.html> (last visited Feb. 1, 2010). The chargers were dropped two days later because the district attorney’s office determined there was not enough evidence to continue the case. James Muñoz, *Online Harassment Charges Dropped Against Texas Teen*, KHOU.COM, Oct. 17, 2009, <http://www.khou.com/news/national/66207272.html> (last visited Feb. 6, 2010).

114. H.B. 2003, 81st Leg., Reg. Sess. (Tex. 2009).

115. *Id.*

116. *Id.* (emphasis added).

via email, and could possibly be convicted of a felony, but send the same messages through email and not violate this law. In both cases, the recipient of the harassing message received and viewed the message through email, but the legal treatment would be different. The only difference is one is routed through a social networking site first, whereas the other is directly sent via email.¹¹⁷

H.B. 2003 also raises First Amendment issues. Similar to the First Amendment concerns with Idaho H.B. 82, the right to be annoying or to make unpopular comments online is protected by the First Amendment. Supporters of the statute say that it is narrow enough to avoid infringing free speech, while detractors point out that “harm” could be broadly interpreted and juvenile pranks or jokes could fall under the statute.¹¹⁸ Furthermore, opponents of the law suggest that current laws adequately protect against cyberstalking and impersonation.¹¹⁹ Opponents claim that identity theft laws could be used to prosecute those who impersonate and steal someone’s online identity and the current stalking laws could serve to protect against online stalking.¹²⁰

Another harassment law, Section 42.07(a)(7) of the Texas Penal Code was recently ruled unconstitutionally vague by the Texas Court of Criminal Appeals.¹²¹ Section 42.07(a)(7) read:

(a) A person commits an offense if, with intent to harass, annoy, alarm, abuse, torment, or embarrass another, he: . . . (7) sends repeated electronic communications in a manner reasonably likely to harass, annoy, alarm, abuse, torment, embarrass, or offend another.¹²²

117. Some scholars have found the focus on social networks untenable. When discussing Texas H.B. 2003, Professor Eric Goldman said, “The whole social networking exceptionalism is ridiculous” and that “[t]here’s no way to distinguish social networking sites from other sites.” Texas Passes Bill on Online Impersonation, NACS Online, June 10, 2009 <http://www.nacsonline.com/NACS/News/Daily/Pages/ND0610099.aspx> (quoting Prof. Goldman).

118. Criminal Jurisprudence Committee, House Research Organization Bill Analysis, May 8, 2009, available at <http://www.hro.house.state.tx.us/pdf/ba81r/hb2003.pdf#navpanes=0>.

119. *Id.*

120. *Id.*

121. *Scott v. State*, 298 S.W.3d 264 (Tex. Ct. App. 2009), *appeal docketed*, No. 04-08-501-CR, 2009 Tex. App. LEXIS 1806 (Dec. 16, 2009); *see also Karenev v. State*, 258 S.W.3d. 210, 214 (2008) (citations omitted), *rev’d on other grounds*, No. 2-05-425-CR, 2009 Tex. App. LEXIS 7533.

122. TEX. PENAL CODE ANN. § 42.07(a)(7) (Vernon 2003).

The court held that Section 42.07(a)(7) had First Amendment implications and if First Amendment freedoms are implicated “the law must be sufficiently definite to avoid chilling protected expression.”¹²³ The court found the words “annoy,” “alarm” and “embarrass” unconstitutionally vague; the statute did not establish an objective standard to measure the level of prohibited annoying or alarming behavior.¹²⁴ The lack of a clear standard for whose sensibilities must be offended and what level of annoyance was illegal did not afford a person of ordinary intelligence a “reasonable opportunity to know what was prohibited.”¹²⁵ Given that the Federal Telephone Harassment Statute¹²⁶ makes it a crime to use a telecommunications device to “annoy, abuse, threaten or harass” and uses “or” as a connector, it could be argued that the federal statute is also unconstitutional under the same analysis.¹²⁷ Texas H.B. 2003 is more definite than Section 42.07(a)(7) and is better equipped to withstand a constitutional challenge for vagueness, although the court may view the words “harm” or “intimidate” in a similar light as they are undefined in the statute.

Idaho H.B. 82 had fewer constitutional concerns than the Texas statute. The existing state statute that Idaho amended mirrors a federal statute, which was found constitutional. The Texas law, on the other hand, is closely related to another harassment statute that was previously found to be unconstitutional by the Texas state courts. Both proposals attempt to provide some legal recourse for those who have been cyberbullied or harassed online.

However, even if the statutes did not have potential constitutional issues, the statutes would not address the root of the cyberbullying problem. A more lasting solution would be to educate children on moral and ethical Internet use. With proper education, cyberbullying would be addressed before it escalates to the point where legal action is needed.

IV. PROPOSED SOLUTIONS

This Part will discuss various proposed solutions to the cyberbullying problem. Section IV.A will examine a proposed solution to decrease the immunity that intermediaries enjoy and increase their role in policing harassing internet speech. Section IV.B will discuss a proposal to reduce

123. Scott, 298 S.W.3d at 268.

124. *Id.* at 270.

125. *Id.* at 268.

126. 47 U.S.C. 223(a)(1)(c) (2006); *see supra* Part III.B.

127. Susan Brenner, Texas Online Harassment Statute Held Unconstitutional, CYB3RCRIM3, May 6, 2008, 15:37 EST, <http://cyb3rcrim3.blogspot.com/2008/05/texas-online-harassment-statute-held.html>. *But see* Booker, *supra* note 110.

anonymity on the Internet. Section IV.C will then evaluate a proposed Federal statutory solution. Lastly, Section IV.D will discuss educating children on internet practices as a way to improve online safety and address cyberbullying.

A. REDUCE IMMUNITY AND INCREASE THE ROLE OF ISPs

One solution to the cyberbullying problem is to reduce the immunity from tort liability that intermediaries, such as Internet Service Providers (ISPs),¹²⁸ enjoy under Section 230 of the CDA.¹²⁹ The intermediaries bear no responsibility for the harassment that their users' experience at the hands of third-party actors and have no obligation to remove offensive materials from websites.¹³⁰

Bradley Areheart¹³¹ proposes that ISP immunity should be lessened and stripped for certain cyberwrongs.¹³² Areheart suggests a "notice and takedown" scheme similar to the one for copyright infringement under the Digital Millennium Copyright Act (DMCA).¹³³ Under Areheart's proposal, where an ISP has received notice of tortious cyberbullying from a victim, the ISP must remove the content or risk loss of immunity under the CDA. If the ISP refuses to remove the bullying material after receiving notice, then the intermediary could be held liable under tort law.

However, given the nature of cyberbullying, a takedown regime might prove difficult. Cyberbullying usually involves repeated acts or prolonged harassment and to prove that there were instances of cyberbullying the intermediaries would have to sift through a large amount of data to determine if there was a pattern of cyberbullying. This might make it more difficult for an intermediary to decide whether to take down information that allegedly constitutes cyberbullying.¹³⁴ Areheart acknowledges that his proposal could "require companies to make decisions about torts that are

128. Internet service providers (ISPs), such as AT&T or Comcast, provide access to the Internet. *See generally* Sara D. Sunderland, *Domain Name Speculation: Are We Playing Whac-A-Mole?*, 25 BERKELEY TECH. L.J. ____ (2010) for more information on how the Internet works.

129. *See supra* Part II.D for a discussion of Section 230 of the CDA.

130. Bradley A. Areheart, *Regulating Cyberbullying Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (2007), <http://thepocketpart.org/2007/09/08/areheart.html>.

131. Bradley A. Areheart is an attorney at DLA Piper LLP. Bradley Areheart Biography, DLA Piper, http://www.dlapiper.com/bradley_areheart (last visited Feb. 22, 2010).

132. Areheart, *supra* note 130.

133. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified in various sections of 17 U.S.C.).

134. Berin Szoka & Adam Thierer, *Cyberbullying Legislation: Why Education is Preferable to Regulation*, THE PROGRESS & FREEDOM FOUND., at 23 (June 2009).

notoriously ambiguous, such as negligence and intentional infliction of emotional distress.”¹³⁵ The intermediaries might then be inclined to take down all content that was complained about to avoid exerting the resources to determine which instances were truly tortious cyberbullying, and to avoid legal liability. Such an action would remove constitutionally protected speech along with potentially harassing speech.

By essentially deputizing the intermediary firms, Areheart’s proposal shifts regulation from the government to private firms whose interests may not be aligned with what is best for the public. Private firms will want to minimize their legal liability and satisfy their legal obligations at a low cost, which may end up limiting constitutionally protected speech. The possible infringement of protected speech by the takedown method makes Areheart’s proposal less attractive. The tradeoff to get better response to cyberbullying may not be worth the removal of legitimate speech.

B. REDUCING ANONYMITY

The easiest way to identify users over the Internet is by tracing the Internet Protocol (IP)¹³⁶ address through the ISP. But for the victim of sexual solicitation or cyberbullying to confront the harasser through the legal system they must have the cooperation of relevant ISPs or other intermediaries. The ISPs and other intermediaries possess identifying data, such as IP addresses, that would help identify harassers; Section 230 immunity, however, provides little motivation for the ISPs to voluntarily cooperate. In this manner, the broad protection under Section 230 serves to hinder individuals in their efforts to identify their online attackers.

Joan Lukey¹³⁷ proposes a system that would require an Internet intermediary, such as an ISP, to remove cyberbullying or cyberstalking material upon notice by a plaintiff, but only after an actual lawsuit has been filed.¹³⁸ Currently, an enforcement agency can only look for the IP address of

135. Areheart, *supra* note 130, at 44.

136. An Internet Protocol (IP) address is a numerical label assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. An IP address serves two principal functions in networking: host identification and location addressing. An IP address is unique to a computer and can be used to trace from where Internet comments were made. Definition of Internet Protocol Address, PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=IP+address&ti=45349,00.asp. See generally Sunderland, *supra* note 128.

137. Joan Lukey is a partner at Ropes & Gray LLP. Joan Lukey Biography, Ropes and Gray LLP, <http://www.ropesgray.com/joanlukey> (last visited Jan. 24, 2010).

138. Brian Baxter, *Tormented by Cyberstalking, Ropes Partner Drafts New Legislation on Online Libel*, LAW.COM, April 20, 2009, <http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202430012681>.

an offender if there is a criminal complaint.¹³⁹ Lukey's proposal would allow the enforcement agency to search for the IP address even without a criminal complaint, as long as a judge found reasonable cause that there were libelous or defamatory postings. Immunity would still be offered for third-party posted content, but if there is a court order at the outset of a criminal case, then the ISPs and search engines would be obligated to turn over whatever identifying information they have, "particularly the metadata necessary to track the IP address of the computer."¹⁴⁰

The Lukey proposal would only require action on the part of the ISP when it has been informed of some wrongdoing. This proposal expands the means to get IP addresses to include some civil actions.¹⁴¹ Lukey's proposal is less drastic than Areheart's and appears to be a reasonable attempt to open up more avenues for cyberbullying victims to identify their harasser. To fully evaluate the process and its effects, more details of this legislation are needed.¹⁴²

C. FEDERAL STATUTE CRIMINALIZING CYBERBULLYING

Another proposed solution would make cyberbullying a federal crime. In May 2008, Rep. Linda Sanchez (D-CA) introduced the "Megan Meier Cyberbullying Prevention Act" which would render cyberbullying a federal felony. The proposed legislation reads:

Whoever transmits in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support *severe, repeated, and hostile behavior*, shall be fined under this title or imprisoned not more than two years, or both.¹⁴³

The proposed bill would create a dual system where one could bully another on the playground and be free from federal repercussions, but not through the Internet. Sanchez wrote "Congress has no interest in censoring speech and it will not do so if it passes this bill. Put simply, this legislation would be

139. *Id.*

140. *Id.*

141. For instance, if there is a court order at the outset of a libel case, the intermediaries would be required to provide whatever identifying information they can about the poster. Baxter, *supra* note 138.

142. Szoka, *supra* note 134.

143. Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Congress, (April 2, 2009), available at <http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1966::>. The bill was originally introduced as H.R. 6123 on May 22, 2008, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6123ih.txt.pdf (emphasis added).

used as a tool for a judge and jury to determine whether there is significant evidence to prove that a person ‘cyberbullied’ another.”¹⁴⁴

Despite Rep. Sanchez’s assurances that the bill will only be used for cyberbullying, there is no way to know how the bill will be interpreted. Professor Eugene Volokh has said that the proposed law is clearly “facially overbroad (and probably unconstitutionally vague), and would thus be struck down on its face under the First Amendment.”¹⁴⁵ The proposed act is well meaning but is simply too vague as the standard for “severe, repeated, and hostile behavior” is unclear.¹⁴⁶ “Severe” and “hostile” are not defined by the statute, which gives this statute a very broad range of possible interpretations. The lack of clear definitions does not give notice to the public about what the prohibited behavior entails and makes the statute untenable and potentially constitutionally vague.

D. EDUCATION

1. School Regulation

Another proposed solution is to allow the schools and school districts to regulate the cyberbullying. The ability of schools to administer punishment for offsite cyberbullying behavior has yet to be fully decided by the Supreme Court. However, the Court has examined whether a school has the authority to regulate and punish off-campus behavior.¹⁴⁷ If the Court ultimately determines that schools have the authority to regulate off-campus

144. Rep. Linda Sanchez, *Protecting Victims, Preserving Freedoms*, HUFFINGTON POST, May 6, 2009, http://www.huffingtonpost.com/rep-linda-sanchez/protecting-victims-preser_b_198079.html.

145. Posting of Eugene Volokh to The Volokh Conspiracy, Federal Felony To Use Blogs, the Web, Etc. To Cause Substantial Emotional Distress Through “Severe, Repeated, and Hostile” Speech?, <http://volokh.com/posts/1241122059.shtml> (Apr. 30, 2009, 16:07 PST).

146. Steven Kotler, *Cyberbullying Bill Could Ensnare Free Speech Rights*, FOXNEWS.COM, May 14, 2009, <http://www.foxnews.com/politics/2009/05/14/cyberbullying-ensnare-free-speech-rights/>.

147. *See Morse v. Frederick*, 551 U.S. 393 (2007) (holding that the First Amendment does not require schools to tolerate student speech that could contribute to the dangers of drug use); *Hazelwood Sch. Dist. v. Kuhlmeier*, 484 U.S. 260 (1988) (finding that a court must be able to set standards for student speech that originates with school resources); *Bethel Sch. Dist. No. 403 v. Fraser*, 478 U.S. 675 (1986) (holding that a “plainly offensive” speech by a student in a school environment infringed upon the rights of other students); *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969) (holding that the First Amendment prevented school authorities from disciplining students for peacefully wearing armbands to protest the Vietnam War). *See generally* Darryn Cathryn Beckstrom, *State Legislation Mandating School Cyberbullying Policies and the Potential Threat to Students’ Free Speech Rights*, 33 VT. L. REV. 283 (2008).

cyberbullying, or if there is legislative action granting schools authority, schools are the logical choice to regulate both traditional bullying and cyberbullying.

A singular source of authority over bullying would be ideal because it would ensure continuity and would make the punishment and enforcement regime clear to the children. Just as teachers and principals regulate traditional bullying at school, schools officials would have authority to discipline offsite cyberbullying. One tool that the schools could use to help monitor offsite cyberbullying is an anonymous reporting system where students could report instances of cyberbullying without fear of retribution.¹⁴⁸

In the absence of explicit authority from the courts to exert power over all off-campus cyberbullying, parents are charged with the task of monitoring and disciplining their children's internet activities. The result has been uneven enforcement; some parents are unaware, too busy, or unwilling to discipline their children and curtail their Internet use. Schools can serve as an impartial governing body to protect the educational interests of the students. Children spend a great deal of time in school, and teachers with the authority to regulate and punish bad internet behavior will help to ensure the educational experience of students is not weighed down by cyberbullying.

2. *Education Beyond School*

Another suggested approach focuses on Internet education instead of changing laws or creating a new regulatory regime. In May 2009, Senator Robert Menendez (D-NJ) introduced the School and Family Education about the Internet (SAFE Internet) Act.¹⁴⁹ The SAFE Internet Act would allocate \$175 million over five years to educate children on Internet safety issues.¹⁵⁰ The education grant program would be administered by the Department of Justice, which would work with the Department of Education and the Department of Health Services to determine how to administer the money to state and local education agencies that would educate children on how to use the Internet safely and ethically.¹⁵¹ Senator Menendez stated on his website:

148. HINDUJA & PATCHIN, *supra* note 7, at 167.

149. SAFE Internet Act, S. 1047, 111th Cong. (2009).

150. *Id.*

151. Press Release, Senator Menendez Newsroom, Keeping Children and Teens Safe Online: Sen. Menendez, Rep. Wasserman Schultz Propose National Grant Program for Internet and Wireless Safety Education (May 13, 2009), *available at* <http://menendez.senate.gov/newsroom/press/release/?id=2c8c04c7-8997-4efb-bbc1-e1504a865ea6>.

The way to meet the challenges and opportunities the Internet presents isn't to deny our children access to this great resource but to make sure they know how to use it wisely. Just as we make sure our children know not to talk to strangers, not to bully kids on the playground, and not to give out their personal information, we have the same responsibility to teach them to apply these values online.¹⁵²

The grant money can be used in a variety of ways, including educating parents and teachers about how to better teach children about the dangers of online use as well as how to ethically and morally use the Internet.¹⁵³

Educating children on safe and ethical use of the Internet could have a positive, lasting impact on the next generation. The SAFE Internet Act lists as one of its findings the promising success of a mandated internet education program in Virginia, wherein “according to an empirical study of 1,379 fourth grade students in Virginia, the first State to mandate Internet safety education in its schools, the students improved their responses to eight of ten questions after completing an Internet safety education program, especially in 2 major areas, uncomfortable content and cyberbullying.”¹⁵⁴ Parents, teachers, law enforcement officers, other community leaders, and children all must work together to create a baseline of Internet safety knowledge for the next generation of Internet users.¹⁵⁵ Much like teaching children to look both ways before crossing the street, a concerted effort from many different sources to educate children on limiting the amount of personal information displayed on social networks and humanizing cyberbullying victims could drive home safe and moral internet practices.

Integrating educational materials into the registration process for social networking sites could also provide value. Children often do not understand the true impact of what they are doing in the name of fun. Through education programs and parental guidance the impact of these behaviors will be relayed to the children.¹⁵⁶ Empathy is one of the keys to fight cyberbullying; once children understand the harmful effects of their actions they will be less inclined to continue.¹⁵⁷ An educational video on Internet best practices, followed by a quiz, could be required when children attempt to

152. *Id.*

153. For the statutorily approved uses see the SAFE Internet Act, S. 1047, 111th Cong. (2009).

154. SAFE Internet Act, § 2(a)(4).

155. HINDUJA & PATCHIN, *supra* note 7, at 130.

156. MELINE KEVORKIAN & ROBIN D'ANTONA, 101 FACTS ABOUT BULLYING 85 (2008).

157. *Id.* at 87.

sign up for Facebook or similar sites. The video could inform them that posted pictures and comments made in cyberspace are available to the whole world, and can be used against them by cyberbullies or be seen by college admissions officers.¹⁵⁸ The registration process could also educate children about the lasting and damaging effects of cyberbullying. Real life stories about suicides, such as Megan Meier's, might provide some context for children. There will undoubtedly be cheating and people will find ways to not pay attention or bypass the training, but there will also be people who will learn something from the training and will walk away with better practices.

Of course, education is best when it starts early.¹⁵⁹ Parents can go online with their children at a young age and instill safe and moral practices. One problem is that many parents may themselves need education. The gap in technical prowess between parents and children could be very wide. Training sessions held at local schools to educate parents on how to monitor and teach safe online use would be an appropriate and productive use of the grant money. When armed with the knowledge of safe Internet practices, parents can pass along that knowledge to their children at an early age. These educators would then pass on the information to students.

V. CONCLUSION

At this time, education is the best legal avenue to instill a culture of online safety in children. Creating new crimes and deputizing intermediary firms are problematic because they raise constitutional concerns. The SAFE Internet Act is a positive step in the attempt to educate parents and teachers so they can in turn educate children. As children learn about safe Internet practices at home, the benefits are more likely to multiply and grow through peer sharing. Peer education is important because children are more likely to listen to their peers than an authority figure.¹⁶⁰

Still, education must start at home. If parents start early and teach their children at a young age about the dangers of using the Internet, as well as respectful and ethical Internet practices, those lessons are likely to stay with them. Ideally, schools would be able to regulate off-campus cyberbullying, creating a consistent regime for traditional bullying and cyberbullying. However, even in the absence of school authority over offsite cyberbullying, if parents, teachers, and the children themselves all work together to educate and build awareness, then there can be lasting effects.

158. HINDUJA & PATCHIN, *supra* note 7, at 101.

159. *Id.* at 148.

160. *Id.* at 137.