STRANGER DANGER AND THE ONLINE SOCIAL NETWORK

By Richard M. Guo

> *The Internet has opened new channels of communication and self-expression. Countless individuals use message boards, date matching sites, interactive social networks, blog hosting services and video sharing websites to make themselves and their ideas visible to the world. While such intermediaries enable the user-driven digital age, they also create new legal problems.*[1]

I. INTRODUCTION

As poster children of the recent Web 2.0 movement, social networking services such as MySpace and Facebook redefine and change the way people—in particular, teenagers and young adults—interact. For example, many university campus organizations now advertise by sending invitations on Facebook instead of distributing paper fliers.[2] Advertising in this manner is quicker and cheaper. Moreover, invitees on Facebook can easily check which of their friends are attending a particular event, and accept or decline the invitation accordingly. Facebook has also found its way onto the dating scene. One undergraduate at the University of Michigan peruses the website when she has recently met a "cute guy."[3] She searches for his profile and gleans personal information such as what fraternity he is in and whether he is in a relationship.[4]

While the majority of online social network users frequent sites for these and other fairly innocent purposes, a nefarious few are beginning to infiltrate the sites in order to prey sexually on vulnerable youths. Although the problem of sexual predators over the Internet is not new (many predecessor services based on user developed content and communications have had similar problems), the sheer popularity and visibility of the online so-

---

1. Fair Housing Council v. Roommates.com, LLC, 489 F.3d 921, 924 (9th Cir. 2007) (citations omitted).

2. Cristian Lupsa, *Facebook: A Campus Fad Becomes a Campus Fact*, CHRISTIAN SCIENCE MONITOR, Dec. 13, 2006, at 13.

3. Matt Marshall & Anna Tong, *University Students Network's Biggest Fans*, SEATTLE TIMES, Sept. 19, 2005, at E1.

4. *Id.*

cial networks has caused widespread concern among the public, media, and lawmakers. In recent years, several news reports have illustrated instances where predators have propositioned youths over the online social networks.[5]

This Note explores the problem of sexual predators over online social networks. Part II describes the Web 2.0 phenomenon, provides a background on online social networks, and describes the structure and privacy protections of the two leading services, MySpace and Facebook. Part III examines the problem of online sexual predators infiltrating social networking communities, and the legal framework governing the services. Part IV argues that the online social networks confer several potential benefits that are worth preserving, and that the current, largely self-regulatory environment provides sufficient incentives for online social networks to protect children and also allows services to innovate and thrive. This Note concludes that lawmakers should avoid wholesale changes that might restrict the core attributes of online social networks such as limiting user-controlled content and communication. Instead, legislation at both federal and state levels should supplement the efforts of social networks through narrowly tailored procedural solutions.

II. THE RISE OF WEB 2.0 AND THE SOCIAL NETWORKING SERVICES

A. Web 2.0

Following the burst of the dot-com bubble in 2001, many concluded the web and its related services and products were "overhyped."[6] However, this conclusion was overly broad. While many dot-com based products and services premised on unviable business models failed in 2001, many others survived. Learning from the failures and survivors, a new group of web services began springing up as early as 2003 and have prevailed. Industry expert and analyst Tim O'Reilly described these new services as participants of a movement he coined "Web 2.0." As explained by O'Reilly, Web 2.0 embodies a set of core principles and practices that tie

5. See generally Pete Williams, MySpace, Facebook Attract Online Predators: Experts Say be Careful What You Post Online-Somebody is Always Watching, NBC NEWS, Feb. 3, 2006, http://www.msnbc.msn.com/id/11165576/; see also Kevin Poulsen, MySpace Predator Caught by Code, WIRED.COM, Oct. 16, 2006, http://www.wired.com/science/discoveries/news/2006/10/71948.

6. Tim O' Reilly, *What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, O'REILLY, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1.

"a veritable solar system of sites that demonstrate some or all" of the following principles:

1) Services, not packaged software, with cost-effective scalability
2) Control over unique, hard-to-recreate data sources that get richer as more people use them
3) Trusting users as co-developers
4) Harnessing collective intelligence
5) Leveraging the long tail through customer self-service
6) Software above the level of a single device
7) Lightweight user interfaces, development models, AND business models[7]

Social networking services are part of the Web 2.0 movement because they embrace the second, third, and fourth principles. Indeed, user content and activities almost entirely drive online social networks. A site becomes "richer" as more people add content and use its services. Online social networks also harness the collective intelligence of their members in developing their sites. A service does not create the majority of its communities. Instead, the service's users, through creating friendships, develop the bulk of communities that ultimately form the foundation of the social network.

B. Social Networking Services

1. Traits of the Social Networking Service

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, photos, web journals, favorite hyperlinks, and the like into one location.[8] Users input information through web-based questionnaires.[9] These questionnaires typically ask users to disclose descriptors

---

7. *Id.*

8. See generally David V. Richards, Note, Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act, 85 TEX. L. REV. 1321, 1323-1325 (2007) (characterizing such profiles as "digital dossiers").

9. *See* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. (2007), available at

such as interests, age, name, and location.[10] Once filled out, web servers take the user-supplied answers and generate the backend webpage code for the profile. As a result, users with little or no programming skills can create and maintain profiles without difficulty.[11] While this type of feature is not novel, it is one of the keys that have allowed social networks to proliferate.[12]

Following the creation of a profile, a user is then able to enjoy the second basic element of an online social network, the community. Unlike web-based communities organized by interest such as public discussion forums, the communities of online social networks are primarily structured around people.[13] Users create communities by linking their profiles with one another. This linking creates a "friendship" between any two users,[14] and generally allows each user to access the other's profile. Beyond the basic "friendship," some services such as Facebook automatically create communities by linking users if they are related in other ways.[15] Within communities, online social networks permit users to communicate in various ways. Most services employ commenting systems that allow a user to post messages directly on another user's profile in her community.[16] In addition to these commenting systems, services also include private messaging services that mimic e-mail.[17] Users can send personal messages to each other directly from links contained on profiles.

The two largest social networks currently are MySpace and Facebook. The slightly older MySpace service has an estimated active user base of 115 million.[18] MySpace is currently the most visited website in the United

---

http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (stating that individuals fill out forms containing questions).

10. *Id.*

11. See Sameer Hinduja & Justin W. Patchin, Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace, 31 J. ADOLESCENCE 125, 130 (2008).

12. See id.

13. Boyd & Ellison, *supra* note 9.

14. Although referred to here as a friendship relationship, Boyd and Ellison note that other terms such as contact or fan are also used to refer to such relationships. *Id.*

15. Some communities are based on geographic or institutional relationships. Facebook.com, About Facebook, http://www.facebook.com/about.php (last visited Dec. 21, 2007).

16. Boyd & Ellison, *supra* note 9.

17. Id.

18. Jon Swartz & Theresa Howard, *Facebook Plans to Offer Targeted Ads*, USA TODAY, Aug. 27, 2007, at B3, *available at* http://www.usatoday/money/advertising/2007-08-26-facebook_N.htm.

States.[19] Facebook, started a year after MySpace, has experienced incredible growth, and estimates a membership of sixty million.[20]

2. MySpace

MySpace began its service on August 15, 2003, and expanded quickly thereafter.[21] One reason for the service's rapid growth is its openness. MySpace is premised on a model that encourages users to make friends with and view content from other users worldwide.[22] Anyone can use MySpace as long as that person has an e-mail address and claims to be over the age of fourteen.[23] The service also makes, by default, a vast amount of its users' profiles accessible to anyone, including non-members.[24]

MySpace users create profiles by filling out questionnaire-like web forms.[25] Users are then able to connect their profiles to those of other users and thereby form communities. MySpace profiles contain several informational sections, known as "blurbs." These include two standard blurbs: "About Me" and "Who I'd Like to Meet."[26] Users may supplement those blurbs with additional sections about their interests, general additional details, and other personal information.[27] MySpace profiles also incorporate several multimedia features.[28] For instance, users may post photos, music, videos, and web logs to their pages.[29]

With respect to privacy, the default setting for older users is to leave their profiles viewable to anyone.[30] Prior to 2008, users who were fourteen

---

19. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007).

20. Scott Spanbauer, *The Right Social Network for You*, PC WORLD, April 2008, at 106.

21. Brad Greenspan, MySpace History, FreeMySpace, http://freemyspace.com/?q=node/13.

22. Posting of Donna Bogatin to Insider Chatter by Donna Bogatin, MySpace to Facebook: Our Friends Rule, http://blog.insiderchatter.com/2007/06/15/myspace-to-facebookour-friends-rule/ (June 15, 2007).

23. MySpace, Terms & Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Mar. 10, 2008).

24. *See* Bogatin, *supra* note 22.

25. *See* Larry Magid, *Turn On MySpace Privacy Features*, CBS NEWS, April 25, 2006, http://www.pcanswer.com/articles/myspaceprivacy.htm.

26. MySpace, Profile Edit, http://www.myspace.com (follow "Home"; then follow "Edit Profile") (last visited Apr. 16, 2008).

27. *Id.*

28. MySpace, Home, http://home.myspace.com (last visited Apr. 16, 2008) (featuring links and buttons for viewing and adding photos, music, videos, and web logs).

29. *Id.*

30. Brian Stelter, *MySpace Agrees To Youth Protections*, N.Y. TIMES, Jan. 14, 2008, http://www.nytimes.com/2008/01/04/technology/14end-myspace.html.

or fifteen had their profiles automatically restricted to their friends.[31] In 2008, MySpace raised the age to eighteen.[32] In terms of privacy control, MySpace provides a few options to restrict exposure of a user's profile, such as limiting access to only a user's friends.

3. Facebook

Facebook, the second largest social networking service, was founded by Mark Zuckerberg[33] in 2004.[34] Facebook originally restricted its site to college students by requiring users to register with e-mail addresses associated with their college institutions.[35] While this requirement resulted in slower growth for Facebook as compared to MySpace, it also allowed Facebook to create a controlled environment and develop "marketing cachet."[36] In 2006, the service ranked as one of the top "in things on campus" along with iPods and text messaging.[37] In that same year, Facebook elected to open its services to anyone thirteen years or older[38] with an e-mail address.[39] The move helped Facebook increase new memberships by 200,000 per day and caused average page views to swell to fifty-four billion each month.[40]

Facebook, in contrast to MySpace, follows a "confirmed friendship" model that emphasizes users' "interact[ion] with their real friends, based on real relationships and the real world around them."[41] In fostering this

---

31. *Id.*

32. *Id.*; Anne Barnard, *MySpace Agrees to Lead Fight to Stop Sex Predators*, N.Y. TIMES, Jan. 15, 2008, at B3, *available at* http://www.nytimes.com/2008/01/15/us/15myspace.html.

33. Posting of Sid Yadav to Mashable, Facebook—The Complete Biography, http://mashable.com/2006/08/25/facebook-profile/ (Aug. 25, 2006, 09:28 AM PDT).

34. Spanbauer, *supra* note 20.

35. Yadav, *supra* note 32.

36. *MySpace, Facebook, and Other Social Networking Sites: Hot Today, Gone Tomorrow?*, KNOWLEDGE@WHARTON, May 3, 2006, http://knowledge.wharton.upenn.edu/article.cfm?articleid=1463.

37. Mike Snider, *iPods Knock Over Beer Mugs; College Kids Rank What's Most Popular*, USA TODAY, June 8, 2006, at D9, *available at* http://www.usatoday.com/tech/news/2006-06-07-ipod-tops-beer_x.htm.

38. Facebook, Customer Support | Facebook, http://www.facebook.com/help.php?safety (last visited Mar. 10, 2008).

39. About Facebook, *supra* note 15.

40. Daniel Lyons, *Party Crashers*, FORBES, Oct. 29, 2007, at 68, 70, *available at* http://www.forbes.com/forbes/2007/1029/068.html.

41. Posting of Donna Bogatin to Digital Markets, Facebook Talks "The Real Deal" In Exclusive Interview, http://blogs.zdnet.com/micro-markets/?p=533 (Oct. 12, 2006).

model, Facebook authenticates its users[42] and actively facilitates user privacy.[43]

Like MySpace, Facebook utilizes web-based questionnaires that permit users to create profiles containing photos and hosts of information including interests, work history, academic background, and user favorites.[44] The service also allows users to quickly add multimedia, articles, applets, and other things found around the site and the internet.[45] Communities or "networks" over Facebook are characterized by a user's relationships and also by the user's geographic location and affiliation to certain institutions such as a university or employer.[46]

With respect to privacy over the service as a whole, Facebook restricts profile views to only those within a user's communities.[47] Thus, the service's "networks" are fairly self-contained with most users having access to less than one-percent of the site's total number of profiles.[48] Minors must join the communities of their educational institutions.[49]

In terms of privacy control, Facebook permits its users to determine the privacy settings of nearly every aspect of their profiles.[50] Granting such control lets users individually decide the amount of information they wish to expose to their friends and to their geographic and institutional networks. For instance, Facebook allows a user to tell those at her school about her interests and activities, but at the same time to restrict avenues of contacting that user to only the user's friends. Contrast this with

---

42. With respect to authenticating users, Facebook generally requires its users to register an e-mail address distributed by their school or workplace institutions prior to joining that institution's community. With respect to communities based on region (such as for those living in the Los Angeles area), anyone with an e-mail can join. However, a user can only be registered in one region at a time. Changes to a user's region are limited to every few months. As a result, most users will accurately choose the region that is most relevant to them. *Id.*

43. Facebook suggests that user authentication and granular privacy controls enhance real world relationships. *Id.*

44. Facebook.com, Facebook | Site Tour, http://www.facebook.com/sitetour/profile.php (last visited Mar. 7, 2008).

45. *Id.*

46. Users enter these geographic or institutional communities by joining networks. *See* Facebook.com, About Facebook, http://www.facebook.com/about.php (last visited Dec. 21, 2007).

47. *Protect Your Privacy*, *supra* note 30.

48. Posting of Donna Bogatin to Digital Markets, Facebook Follows MySpace: Online Predator Risks, http://blogs.zdnet.com/micro-markets/?p=967 (Feb. 11, 2007).

49. Kim Komando, *Set Up a Safe Facebook Profile*, Komando.com, Feb. 2, 2008, http://www.komando.com/kids/tip.aspx?id=4455.

50. *Protect Your Privacy*, *supra* note 30.

MySpace, where limited privacy settings force members to choose either to expose their entire profiles or not.[51] As a result, a MySpace user cannot publicly share certain portions of her profile while limiting more personal portions to her friends.

4. The Benefits of Social Networks

While the social networking phenomenon is relatively new, interest in this area of growth has resulted in various studies attempting to understand the effects of online social networks on their users. With respect to minors, a recent study notes that far from acting solely as online places to hang out,[52] social networks provide younger users with valuable opportunities to express themselves and interact with their peers. These opportunities, in turn, help minors facilitate development of their identities, and refine their abilities to understand and interact with one another in healthy ways.[53] Researcher Danah Boyd, who did not take part in the aforementioned study but who was cited by its authors, explains that the "process of learning to read social cues and react accordingly is core to being socialized into a society."[54] Part of this learning experience is played out by attempting to communicate an impression of oneself through a performance, getting feedback on that performance from peers, and then adjusting one's approach accordingly to better relay the desired impression next time.[55] This process, defined as impression management, is "honed" through experience.[56] Online social networks provide an additional avenue for youths to further hone their impression management skills.[57] This is accomplished by permitting users to craft "digital bodies" through profiles and to display these "digital bodies" to peers.[58]

Apart from aiding social development, services also facilitate the sharing of web links, pictures, and stories.[59] Such facilitation often helps users

51. See id.
52. Hinduja & Patchin, *supra* note 11 at 131.
53. *Id.*
54. Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, in YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 129 (David Buckingham ed., John D. & Catherine T. MacArthur Found. Series on Digital Media & Learning, 2007), *available at* http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119.
55. *Id.* at 128.
56. Id.
57. See id.
58. See id.
59. Hinduja & Patchin, *supra* note 11 at 131.

to "remain intimately connected with friends regardless of spatial distance."[60]

III. SOCIAL NETWORKING AND ONLINE SEXUAL PREDATORS

A. The Online Sexual Predator Problem

Social networks are generally aimed at allowing users to develop communities of friends, and at facilitating communication within those communities. Indeed, the majority of teens use social networks to accomplish that very goal: to keep in touch with friends.[61] At the same time, social networks are also becoming forums where complete strangers meet.[62] In most instances, innocent friendships develop out of these online encounters. However, an unfortunate byproduct of the widespread usage of these social forums has been the increased presence of online sexual predators.

An online sexual predator is someone who uses the internet to sexually exploit vulnerable individuals, typically under-aged youths.[63] Predators approach and solicit sex from one out of five online youths.[64] These solicitations are typically done methodically. Most predators turn to the topic of sex early on, usually within three or four message exchanges.[65] While the majority of teens appear to ignore such advances,[66] for some unprepared minors, such situations can "get out of hand very quickly."[67] Predators,

---

60. *Id.*

61. *See* AMANDA LENHART & MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, TEENS, PRIVACY & ONLINE SOCIAL NETWORKS 31 (2007), http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (reporting that ninety-one percent of teenagers use social networking sites to stay in touch with friends they see frequently, while eighty-two percent use the sites to stay in touch with friends they rarely see in person).

62. See generally Janet Kornblum, Meet My 5,000 New Best Pals ; Does 'Friending' on a Social Site Make those Relationships Real?, USA TODAY, Sept. 20, 2006, at D1, available at http://www.usatoday.com/tech/news/2006-09-19-friending_x.htm.

63. See generally M. Megan McCune, Comment, Virtual Lollipops and Lost Puppies: How Far Can States Go to Protect Minors Through the Use of Internet Luring Laws, 14 COMMLAW CONSPECTUS 503, 505-07 (2006) (discussing online sexual predators).

64. *Id.* at 508.

65. M. Jane Brady, Symposium: Prosecution Responses to Internet Victimization: Keynote Address: Prosecution Responses to Internet Victimization, 76 MISS. L.J. 623, 633 (2007).

66. A Pew survey reports that nearly 65% of teens ignore or delete contact from strangers. LENHART & MADDEN, *supra* note 61 at 34.

67. Brady, *supra* note 65.

once detecting vulnerability, often start grooming a minor into trusting them and thinking that they are friends.[68] The prime targets of predators are frequently "'kids struggling with low self-esteem, or [those] that haven't found a place to belong and spend enormous amounts of time in isolation sitting at a computer.'"[69]

During the years prior to the explosive expansion of social networks, most online sexual predators attempted to contact youths through chat rooms and message boards.[70] In recent years, however, predators are increasingly targeting minors over social networking services. Two factors have contributed to this shift.

Arguably the primary factor is the escalating popularity of online social networks among teenagers. More than fifty-five percent of all American teenagers use and post profiles on these services.[71] The high number and high concentration of minors on both MySpace and Facebook, as one researcher describes, creates "target-rich environment[s]" for online sexual predators.[72] While a recent survey reveals that the majority of teens restrict their profiles to only their friends, a sizable forty percent allows anyone to view their information.[73] As a result, many teens remain contactable by strangers. Sexual predators have taken notice of this circumstance and have begun attempting to infiltrate social networking communities.[74]

The second factor involves the content that minors post on social networking profiles. Many members of social networks post seemingly trivial, yet significant, information such as their city of residence, age, and personal preferences.[75] Sexual predators often exploit this precise information to establish rapport with and acquire the trust of their victims.[76]

---

68. Chris Cobbs, Dangers of Online Networking; Protecting Kids From Predators; More and More Children Hang Out on Social-Network Sites—So Do Predators, ORLANDO SENTINEL, April 6, 2006, at A1.

69. *Id.*

70. In a report on online victimization by the Crimes Against Children Research Center in 2000, it was found that 65% of sexual solicitations of youths occurred in chat rooms. *See* DAVID FINKELHOR ET AL., CRIMES AGAINST CHILDREN RES. CTR., ONLINE VICTIMIZATION: A REPORT ON THE NATION'S YOUTH 4 (2000), http://www.missingkids.com/en_US/publications/NC62.pdf; *see also* McCune, *supra* note 63.

71. *See* LENHART & MADDEN, *supra* note 61 at 11.

72. *See* Cobbs, *supra* note 68 (quoting Secret Service special agent James Glendinning as stating that predators, "'go to these [social-networking] sites because they are a target-rich environment.'") (alteration in original).

73. LENHART & MADDEN, *supra* note 61 at 26.

74. *See* Cobbs, *supra* note 68.

75. LENHART & MADDEN, *supra* note 61 at 18.

76. Stephen T. Watson, *Online Site for Teens to Improve Security*, BUFFALO NEWS, March 5, 2006, at B1.

While both MySpace and Facebook have taken measures to enhance site safety and prevent sexual predators from browsing their sites, the improved sophistication of today's sexual predators[77] has meant that some have been able to get onto the sites and solicit minors. In some of these instances, victims and their parents have initiated civil actions against the social networking services. However, for the most part, social networking services are shielded from liability by the provisions of the Communications Decency Act.

B. The Regulatory Framework

1. Social Networking and the Communications Decency Act

a) The Communications Decency Act

The Communications Decency Act ("CDA"), Title V of the larger Telecommunications Act of 1996[78], attempted to regulate offensive material such as pornography over the internet.[79] In enacting the CDA, Congress chose to grant immunity to Internet Service Providers (ISPs) with regard to third-party usage in two key respects. Section 230(c)(1)[80] grants immunity to any "provider or user of an interactive computer service" from liability stemming from information "provided by another information content provider."[81] Section 230(c)(2) limits liability for a provider that removes or edits offensive content.[82] Together, these provisions remove liability concerns that might create a disincentive for a service provider to monitor its website.[83]

---

77. In the past, predators roamed largely open message boards and chat rooms. As a consequence, much of an online sexual predator's conversations with a minor unfolded in public. This allowed law enforcement to much more effectively monitor and hunt predators. However, today, most sexual predators conduct communications outside of public view. Although predators might make their own social networking profiles public, they generally avoid detection by sticking to private messages and hiding any comments posted by their potential victims from public view. *See* Poulsen, *supra* note 5.

78. Pub. L. No. 104-104, 110 Stat. 56 (codified throughout 47 U.S.C. (1996)).

79. Ken S. Myers, Wikimmunity: Fitting the Communications Decency Act to Wikipedia, 20 HARV. J. LAW & TECH. 163, 172 (2006).

80. Section 230(c) is also known as the Good Samaritan provision. 47 U.S.C. § 230(c) (2000).

81. 47 U.S.C. § 230 (2000).

82 47 U.S.C. § 230(c)(2) (2000).

83. 47 U.S.C. § 230(c)(2) (2000); *see* Jae Hong Lee, Note, Batzel v. Smith & Barrett v. Rosenthal: *Defamation Liability for Third-party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 472-73 (2004); *see* Myers, *supra* note 79 at 172.

Section 230 was enacted to directly address the problematic and odd situation created by *Stratton Oakmont, Inc. v. Prodigy Services, Co.*,[84] a New York state court decision. In that case, an investment banking firm, Stratton Oakmont, sued Prodigy over statements made by an unidentified poster over Prodigy's "Money Talk" message board.[85] The plaintiffs alleged that Prodigy was liable as the "publisher" of the statements.[86] The plaintiffs supported their view by pointing to statements made by Prodigy "likening itself to a newspaper."[87] The court ultimately sided with the plaintiffs. In its opinion, the court concluded that Prodigy's use of "technology and manpower" to delete offensive material demonstrated that the service "controlled decisions as to content" in a manner that warranted publisher liability.[88] The court noted that the benefits gained by Prodigy through asserting editorial control also subjected Prodigy to greater liability.[89]

For ISPs, *Stratton* produced a strong disincentive to monitor and remove offensive material from their sites.[90] Should a website decide to monitor third party content and unknowingly allow the posting of unlawful material, that website would be held strictly liable as a publisher.[91] However, if the same website elected not to monitor at all, a court would categorize the site as a distributor and determine liability based on a negligence standard.[92] As a consequence, electing to monitor one's site after *Stratton* actually increased the prospect of liability for ISPs.[93]

b) Subsequent Treatment of Section 230

In the years since the passage of the CDA, courts adjudicating Section 230 defenses have often looked to Congress's policy goals[94] for enacting the provision:

---

84. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 25, 1995).

85. *Id.* at *3.

86. *Id.* at *3.

87. *Id.* at *3-4.

88. *Id.* at *10.

89. *Id.* at *13.

90. Lee, *supra* note 83, at 472-73; Myers, *supra* note 79 at 172.

91. *See* Lee, *supra* note 83 at 472.

92. *Id.* at 470.

93. Cecilia Ziniti, Comment, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583.

94. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003); *see* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997); *see* Doe v. Bates, 2006 U.S. Dist. LEXIS 93348, at *8-9 (E.D. Tex. Dec. 27, 2006).

1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[95]

In light of these goals, courts have generally construed immunity under § 230 broadly. In terms of the range of internet services qualifying for immunity, courts have found § 230 "quite robust" with a "relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'"[96] Accordingly, most internet services meet the requirements for an interactive computer service. In terms of scope of protection from tort liability, most courts follow the Fourth Circuit's holding in *Zeran v. America Online, Inc.*, a decision that found that the CDA removes the "specter of tort liability" for internet intermediaries in relation to third party content.[97] In that case, the Fourth Circuit reasoned broad immunity was required because the imposition of tort liability on service providers would create a form of government regulation on speech that Congress expressly wanted to minimize.[98]

c) *Doe v. MySpace*

Congress designed Section 230 of the CDA during an era when the internet was burgeoning, and civil actions seriously threatened to curb online service providers. Section 230 allowed websites to develop without

96. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).
97. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).
98. *Id.*

fear of civil liability by granting immunity to the websites in legal actions stemming from content posted by service users.

Social networking services gained mainstream popularity more than half a decade after the CDA's passage. In 2007, the Western District of Texas squarely considered whether and to what extent online social networks qualified for protection under the CDA.[99]

In *Doe v. MySpace, Inc.*, the anonymous plaintiff, "Julie Doe," created a MySpace profile despite being only thirteen years old.[100] When she joined the website, Doe lied about her age and reported that she was in fact eighteen.[101] Peter Solis, a nineteen year-old man, later contacted Doe over the website and eventually, Doe provided Solis with her telephone number.[102] The two communicated over the telephone for several weeks before arranging to meet.[103] During the meeting, Solis allegedly sexually assaulted Doe.[104] Doe, along with her mother,[105] sued MySpace, claiming that the social network negligently failed "to take reasonable safety measures to keep young children off of its site."[106] MySpace moved to dismiss the lawsuit, asserting immunity under the Communications Decency Act.[107] The court ultimately found for MySpace and dismissed the case.[108]

The court considered MySpace's Section 230(c)(1) defense by first noting that neither party contested MySpace's role as an "interactive computer service," requisite for immunity under the CDA.[109] After making this observation, the court examined to what extent Julie Doe and the online sexual predator qualified as "information content providers" for the purposes of Section 230(c)(1). With little discussion, the court held that both parties clearly qualified as information content providers with respect to their MySpace communications.[110] Having settled these two requirements for Section 230(c)(1) applicability, the court subsequently spent the bulk of its analysis focused on the proper scope for CDA immunity, and whether the cause of action was rooted in MySpace's role as a publisher

99. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007).
100. *Id.* at 846.
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. Citizen Media Law Project, Doe v. MySpace, http://www.citmedialaw.org/doe-v-myspace (last visited Oct. 26, 2007).
106. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007).
107. *Id.* at 846.
108. *Id.* at 852.
109. *Id.* at 846.
110. *Id.* at 846-47.

(the third requirement for a Section 230(c)(1) defense) with respect to Doe and Solis's communications. Specifically, the court examined the plaintiffs' arguments: (1) that CDA immunity did not apply in the case because it was applicable only to defamation or related actions, and (2) that the cause of action was "not based on MySpace's posting of third-party content [anyway], but rather on MySpace's failure to institute safety measures to protect minors."[111]

In reviewing the plaintiffs' first argument limiting CDA immunity to defamation or related actions, the court examined the policy underlying Section 230 and case law subsequent to the Section's enactment.[112] The court found that the CDA was intended to promote "the continued development of the Internet and other interactive computer services,"[113] and that courts dealing with Section 230 questions developed an expansive interpretation of its immunity provisions. Citing *Zeran*, the court rejected the plaintiffs' argument for a narrow interpretation of Section 230 and held that the CDA "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[114] The court further noted that courts in the past had granted Section 230 immunity against claims involving negligence, "negligence per se, intentional infliction of emotion distress, invasion of privacy, civil conspiracy," distribution of child pornography, and the Maryland Commercial Electronic Mail Act.[115]

Turning to the plaintiffs' assertion that their cause of action was based on MySpace's failure to institute safety measures and not in the site's capacity as a publisher, the court rejected the plaintiffs' stance and found that the claims were, despite artful pleading on the plaintiffs' part, directed toward MySpace in the service's "publishing, editorial, and/or screening capacities."[116] The court explained:

> It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs as-

111. *Id.* at 849.
112. Id. at 846-49.
113. *Id.* at 847.
114. *Id.* at 848.
115. *Id.* at 849.
116. *Id.* at 849.

> sert they never would have met and the sexual assault never would have occurred.[117]

Having found that MySpace met the requirements to qualify for immunity under Section 230(c)(1), the court absolved the service of liability.

In addition to applicability of Section 230(c)(1), the court also concluded that MySpace was exempted from liability under the CDA's provisions immunizing sites that make "efforts to self-regulate material."[118] Referencing Section 230(c)(2)(A), the court wrote:

> This section reflects Congress's recognition that the potential for liability attendant to implementing safety features and policies created a disincentive for interactive computer services to implement any safety features or policies at all. To the extent Plaintiffs seek to hold MySpace liable for ineffective security measures and/or policies relating to age verification, the Court alternately finds such claims are barred under § 230(c)(2)(A).[119]

After finding that MySpace was not liable under federal law, the court further found that the social networking service was not liable under Texas law either. The court began its analysis by observing that claims of negligence and gross negligence require the existence of an affirmative duty.[120] Since, as a general matter, "a person has no legal duty to protect another from the criminal acts of a third person or control the conduct of another," the court examined whether a special relationship between MySpace and the fourteen year-old plaintiff existed.[121] In the end, the court found no special relationship.[122] The court placed considerable weight on the fact that the plaintiff had lied about her age, communicated with an adult, and published her personal information.[123] The court explained that:

> To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks and close this avenue of communication, which Congress in its wisdom has decided to protect.[124]

---

117. Id.
118. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 850 (W.D. Tex. 2007).
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.*
124. *Id.* at 851.

Further, while the court acknowledged that premises owners had a duty to protect persons injured on their premises in certain situations, it declined to extend such a duty to ISPs and, in particular, to a defendant that "provide[d] its service to users for free."[125]

As a result of the court's holdings, MySpace was absolved from liability under the CDA and also under Texas law. The *MySpace* decision is significant because it directly considers Section 230's applicability with respect to social networking services. While not mandatory authority for future courts, it is likely to be influential. Although some critics argue that the decision's broad application of Section 230 makes online social networks unaccountable for bad behavior,[126] services are likely to act responsibly due to other external pressures.[127]

2. Other Federal and State Laws and Current Proposals on Online Social Network Regulation

While the *MySpace* court wrestled with the applicability and scope of section 230 immunity with respect to sexual predator cases involving online social networks, Congress and state legislatures proposed several measures specifically aimed at protecting minors over social networking sites. Several recent proposals address this issue by: (1) restricting child access to online social networks at institutions receiving government funding, (2) requiring sex offenders to register online identities and addresses, and (3) requiring minors to receive parental consent before accessing social networking services.

a) Restricted Access to Social Networks in Government Funded Institutions

The Deleting Online Predators Act of 2007 (DOPA II) seeks to restrict child access to online social networks at institutions receiving government funding.[128] In July 2006, the House of Representatives passed the bill's forerunner, the Deleting Online Predator Act of 2006 (DOPA I); but the bill did not become law because it stagnated in the Senate.[129] DOPA II

125. *Id.*

126. See Texas District Court Extends § 230 Immunity to Social Networking Sites—Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), 121 HARV. L. REV. 930 (2008).

127. *See infra* Part IV.

128. H.R. 1120, 110th Cong. (1st Sess. 2007); *see also* Eric Goldman, *Social Networking Sites and the Law*, TECHNOLOGY & MARKETING LAW BLOG, May 2007, http://www.ericgoldman.org/Resources/socialnetworkingsitesandthelaw.pdf.

129. Jacqui Cheng, *Deleting Online Predators Act Reappears for 2007*, ARS TECHNICA, Feb. 16, 2007, http://arstechnica.com/news.ars/post/20070216-8869.html.

would require schools receiving e-rate federal funding to prohibit access to commercial social networking websites and chat rooms unless those institutions use the services for an educational purpose under adult supervision.[130] The bill would also require libraries receiving e-rate federal funding to prevent minors without parental authorization from accessing the aforementioned services.[131] The definition of what constitutes a "social networking website" under the provisions of the bill is still unsettled.[132] The bill requires the creation of a definition within 120 days of enactment.[133] In developing the definition, the bill requires consideration of the extent to which a website:

(i) is offered by a commercial entity;

(ii) permits registered users to create an on-line profile that includes detailed personal information;

(iii) permits registered users to create an on-line journal and share such a journal with other users;

(iv) elicits highly-personalized information from users; and

(v) enables communication among users[134]

Supporters of DOPA II feel that the bill is necessary because "with the explosive growth of trendy chat rooms and social networking websites, it is becoming more and more difficult to monitor and protect minors from those with devious intentions, particularly when children are away from parental supervision."[135] Moreover, supporters note that the DOPA II does not create an outright ban of social networks and would allow children to use social networks under certain circumstances.[136]

Critics of DOPA II, however, fear that the bill might create an overly broad definition of a social network, and prevent access to "truly helpful and educational sites."[137] For example, critics fear that DOPA II may re-

130. H.R. 1120, 110th Cong. (1st Sess. 2007); *see also* Posting of Andy Carvin to Learning.now, Lifting the Hood on DOPA Jr., http:www.pbs.org/teachers/learning.now/2007/01//lifting_the_hood_on_dopa_jr.html (Jan. 26, 2007).

131. H.R. 1120, 110th Cong. (1st Sess. 2007).

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *See* Carvin, *supra* note 130.

137. Cheng, *supra* note 129.

strict websites such as Wikipedia and Amazon.[138] Consequently, critics are concerned that some children who lack access to the internet at home might miss out on "an extended sphere of contacts."[139] Moreover, while DOPA II permits schools and libraries to allow access to social networks, some critics argue that most schools and libraries would simply "lock down their computers" and "walk away."[140] In addition, adult supervisors such as teachers who wish to use social networks for educational purposes might be dissuaded by increased scrutiny and pressure.[141]

b) Registration of Sex Offender Online Identities

With respect to the second category of proposals, which requires sex offenders to disclose online identities, Virginia became the first state to enact such a proposal when it recently passed a bill requiring sex offenders to register e-mail addresses and screen names.[142] Legislators envision that the state will use the collected information to build a database accessible to website operators for the purpose of locating registered sex offenders on their sites.[143]

At the federal level, the Keeping the Internet Devoid of Sexual Predators Act (KIDS),[144] introduced by U.S. Senators Charles E. Schumer and John McCain, parallels the Virginia statute by requiring "registered sex offenders to submit e-mail addresses, instant message addresses or other identifying internet information to law enforcement to be placed on the National Sex Offender Registry."[145] Commercial social networking sites would then have access to this information to prevent registered sex offenders from using their services.[146]

---

138. *Id.*

139. Interview by Sarah Wright with Henry Jenkins, Director of the Comparative Media Studies Program at M.I.T., and Danah Boyd, Ph.D. Student at U.C. Berkeley School of Information, conducted via e-mail (May 26, 2006), http://www.danah.org/papers/MySpaceDOPA.html. While Jenkins and Boyd discuss DOPA I, their concerns are also applicable to DOPA II.

140. *Id.*

141. *Id.*

142. H.B. 2749, 2007 Sess. (Va. 2007); VA. CODE ANN. § 9.1-903 (2007).

143. Kevin Fayle, *Understanding the Legal Issues for Social Networking Sites and Their Users*, FINDLAW, 2007, http://technology.findlaw.com/articles/00006/010966.html.

144. S. 431, 110th Cong. (1st Sess. 2007).

145. Press Release, Press Office of U.S. Senator John McCain, Senators McCain and Schumer Introduce KIDS Act of 2007 (Jan 30, 2007), http://mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=B81BC365-6A58-4425-B170-99E85F0E85D4.

146. Jennifer Parker, *Congress, MySpace Team Up to Fight Sexual Predators*, ABC NEWS, January 30, 2007, http://abcnews.go.com/Politics/story?id=2835135&page=1.

Supporters of such measures argue that sexual predators "'have no business joining social networking communities," and need to be kept out of the "online neighborhoods" that children frequent.[147] Critics, however, argue the proposal would do little to directly prevent a sexual predator from soliciting minors.[148] The anonymity of the internet and the ease in which it allows people to create multiple e-mail addresses, they contend, make it easy for a sexual predator to avoid detection and infiltrate online social networks with unregistered identities.[149]

c) Age Verification

Finally, the third category of proposals would require minors to obtain parental consent and have their age verified prior to using social networking services. The North Carolina State Senate incorporated such a requirement in a bill introduced in 2007.[150] The requirement, which was ultimately removed while the bill was being considered in the North Carolina State House of Representatives,[151] required online social networks to verify parental identity and age[152] before allowing minors site access. While the requirement did not specify how sites would verify parental consent and age, one proposed method included using public records to check a parent's identity, and then later placing a follow up phone call or postcard to confirm parental approval and the minor's age.[153]

Advocates for such verification proposals argue that requiring parental consent and age verification at least will give parents the chance to see what their children post.[154] Critics, however, counter that requiring parental approval creates an "ineffective and unworkable" solution in the long run, pointing out that parental approval and an age-verification system

147. *Senators Introduce KIDS Act of 2007*, GOVERNMENT TECHNOLOGY, Feb. 1, 2007, http://www.govtech.com/gt/articles/103705.

148. *See Editorial: KIDS Act of 2007*, CALIFORNIA AGGIE, Feb. 8, 2007, http://media.www.californiaaggie.com/media/storage/paper981/news/2007/02/08/Opinion/Editorial.Kids.Act.Of.2007-2706532.shtml; *see also* Catherine Rampell, *Registry May Soon Add Sex Offenders' Web IDs*, WASH. POST, Dec. 15, 2007, at D02, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/12/14/AR2007121401734.html (quoting Law Professor David Filler).

149. *See* Rampell, *supra* note 148.

150. S. Res. 132, Sess. 2007 (N.C. 2007) (edition 3); *see also* Fayle, *supra* note 143.

151. *See* S. Res. 132, Sess. 2007 (N.C. 2007) (edition 4).

152. S. Res. 132, Sess. 2007 (N.C. 2007) (edition 3).

153. *See* Press Release, North Carolina Department Of Justice, Protecting Children from Sexual Predators: SB 132 (July 24, 2007), http://www.ncdoj.com/DocumentStreamerClient?directory=WhatsNew/&file=S132%20Summary%20final.pdf.

154. *Id.*

would be difficult to implement technically.[155] In addition, a parental verification requirement, critics assert, would make the internet less safe by creating a false sense of security.[156]

3. Self-Regulation Through Initiatives and Technical Safety Mechanisms

The CDA, in theory, creates an environment where social networks can routinely ignore concerns regarding offensive content. Such a theory seems plausible because the CDA removes tort liability, and thus eliminates a strong incentive to patrol one's site. While such a scenario might conceivably occur in environments where governments are the sole regulators, in the case of safety over social networks, the existence of other external forces creates a strong incentive for services to monitor their sites and enhance safeguards.

Specifically, media attention and public pressure continuously remind the social networks that they must be extra mindful of the sexual predator problem. Over the past two years, the media has detailed several incidents where sexual predators targeted minors over the online social networks. For example, in 2006, journalist Kevin Poulsen conducted an investigative report that helped law enforcement apprehend a thirty-nine year old convicted sex offender who had been using MySpace to contact and proposition a fourteen-year-old teen.[157] Reports like Poulsen's have created public concern[158] that in turn has caused many online social networks to carefully examine their services and act towards creating safer environments for their members.

---

155. Posting of Braden Cox to Netchoice, The Achilles Heel of Social Networking Age Verification in the Tar Heel State, http://blog.netchoice.org/2007/05/the_achilles_he.html (May 15, 2007).

156. *Id.*

157. *See* Poulsen, *supra* note 5.

158. Such concern had prompted some state attorney generals to initially use the threat of litigation to push social networks to enhance site safety. Currently, however, a situation has developed where state attorney generals and the social networks are operating in a cooperative manner to combat the danger of online sexual predators. *See* Brad Stone, *States Fault MySpace on Predator Issues*, N.Y. TIMES, May 15, 2007, at C2, *available at* http://www.nytimes.com/2007/05/15/technology/15myspace.html; *see also* Catherine Louisa Glenn, Note, *Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records*, 53 VAND. L. REV. 1605, 1631-32 (2000) (discussing how the threat of liability makes self-regulation more effective); Juan Carlos Perez, *Facebook, MySpace Join NY AG in Pushing E-safety Bill*, INFOWORLD, Jan. 29, 2008, http://www.infoworld.com/article/08/01/29/NY-AG-pushes-e-safety-bill-Facebook-MySpace-back-it_1.html.

Generally, safety initiatives are directed at improving public awareness, enhancing complaint intake and monitoring, and improving safety through technical means.

a) Non-Technical Initiatives

With respect to improving awareness, both MySpace and Facebook have taken steps to improve public consciousness of the online predator issue. MySpace, for instance, recently started displaying public-service announcements on its website promoting safe online practices.[159] Facebook, in an agreement with the New York State Attorney General, began disclosing information about the site's safety measures, and also issued sterner warnings about the dangers of online sexual predators.[160] Facebook's chief security officer Chris Kelly recently described educational initiatives as the best way to protect minors in online communities.[161]

Both MySpace and Facebook have also made directed efforts at improving their procedures for locating and handling problematic profiles. Facebook, also in its agreement with the New York Attorney General, has implemented monitoring guidelines that include making it easier for users to complain about problematic profiles and addressing user complaints within twenty-four hours.[162] MySpace, for its part, allocates a third of its customer service force to monitoring for and removing problematic profiles.[163] The service has also taken steps to strengthen coordination with law enforcement including establishing a twenty-four hour hotline.[164]

b) Technical Safety Mechanisms

In addition to the aforementioned initiatives, MySpace and Facebook have implemented technical safety mechanisms. These mechanisms come in the form of additional, independent safety measures as well as in the form of safeguards developed through site design.

---

159. Maria Newman, *Internet Site Hires Official To Oversee Users' Safety*, N.Y. TIMES, April 12, 2006, at 3, *available at* http://www.nytimes.com/2006/04/11/technology/11cnd-myspace.html.

160. *Facebook Agrees to Police For Predators, Content*, NORTH COUNTRY GAZETTE, Oct. 16, 2007, http://www.northcountrygazette.org/news/2007/10/16/facebook_ agrees/.

161. Erica Ogg, *RSA Panel Addresses Net Threats to Children*, NEWS.COM, Feb. 7, 2007, *http*://www.news.com/2100-7348_3-6157399.html.

162. Facebook Agrees to Police for Predators, Content, supra note 160.

163. Jenn Shreve, *MySpace Faces a Perp Problem*, WIRED.COM, April 18, 2006, http://www.wired.com/news/culture/0,70675-0.html.

164. January W. Payne, Invitation to Harm; Some Minors Find MySpace.com a Hospitable Home for Traffic in Illegal Pills and Promotion of Self-Destructive Behaviors, WASHINGTON POST, July 4, 2006, at F01, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/07/03/AR2006070300788.html.

MySpace has added several technical safety mechanisms independent of their social networking system. In late 2006, the website announced the development of an automated system that would compare user profiles to a database containing the names and physical descriptions of convicted sex offenders.[165] The system is currently in operation. A recent report shows the system has helped MySpace find and remove more than 29,000 sex offender profiles.[166] Aside from this major initiative, MySpace is planning to make monitoring software available to users' parents. The software, currently in testing,[167] operates from a user's personal computer and provides her parent with the user's profile name, reported age, and location. Such information, MySpace's chief security officer Hemanshu Nigam notes, helps parents validate their children's self-reported information and determine whether too much personal information is being revealed.[168] Nigam further explains that the age validation feature is of particular importance because many of MySpace's technical safety features are built around age.[169]

MySpace also incorporates safety measures into the design of their system. For example, as mentioned previously, MySpace limits access to profiles of users under eighteen.[170] Moreover, users that are eighteen and over are blocked from contacting a fourteen or fifteen year old user unless they can verify that user's last name and e-mail address.[171]

Facebook incorporates many of its protections through the design of its service. As previously mentioned, member profiles, unlike those in MySpace, are viewable only to a user's friends and those within a user's institutional or geographic networks. Such a design decision reduces the number of strangers granted access to any given profile from the outset of

---

165. The database maintains information on the United States' 550,000 registered sex offenders, and is maintained by ID verification firm Sentinel. Robert Lemos, *MySpace Teams to Create Sex-Offender Database*, SECURITYFOCUS, Dec. 5, 2006, http://www.securityfocus.com/news/11428.

166. Audrey Barrick, *29,000 MySpace Sex Offenders Removed*, CHRISTIAN POST, July 25, 2007, http://www.christianpost.com/article/20070725/28604_29,000_MySpace_Sex_Offenders_Removed.htm.

167. MySpace.com, ParentCare Beta, http://myspace.com/parentcare (last visited Dec. 18, 2007).

168. Caroline McCarthy, *MySpace Developing Parental-Notification Software*, NEWS.COM, Jan. 17, 2007, http://www.news.com/MySpace-developing-parental-notification-software/2100-1032_3-6150824.html?tag=item.

169. *Id.*

170. Stelter, *supra* note 32.

171. Jessica S. Groppe, Comment, A Child's Playground or a Predator's Hunting Ground?-How To Protect Children on Internet Social Networking Sites, 16 COMMLAW CONSPECTUS 215, 238-39 (2007).

that profile's creation. While such a distinction might seem trivial because MySpace already limits access to the profiles of minors, consider situations such as that of the plaintiff in *MySpace* who had lied about her age. For those minors, Facebook's design at least provides a bit more protection.

In addition to greater structural privacy protections, Facebook also gives its users enormous control in tweaking their privacy settings. Facebook's design choices, in this respect, permit users to very precisely select an appropriate level of information disclosure for each group of possible profile viewers. As a result, Facebook users are not faced with an all or nothing proposition in terms of profile information dissemination. Such privacy control comes in handy when a minor wants to reveal her interests and favorites to her friends, but not to the stranger living across town.

Along with aiding in curbing the unwanted proliferation of information, Facebook also makes it much more difficult to access minor-populated communities. High school aged students can only sign up by either using a school-issued e-mail or through invitation.[172] After registration, Facebook associates the profiles of these students with their high school networks, and makes their profiles private to non-network members. For minors this is generally not a great issue because most minors use online social networks to interact with people that they personally know offline anyway.[173] Users without an invitation[174] or school issued e-mail address are not allowed access to the high school networks. As a result, Facebook creates a virtual boundary that helps prevent online sexual predators from locating and contacting minors.

Lastly, Facebook actively uses "algorithms [to] detect possibly problematic situations."[175] Algorithms, for example, flag users that make "too many friend requests to members younger than [eighteen], [who have] denials of friend requests and [who have] reports of inappropriate photos."[176]

---

172. Ogg, supra note 161.

173. *See* Amanda Lenhart & Mary Madden, Pew Internet & Am. Life Project, Social Networking Websites and Teens: An Overview 2 (2007), http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf.

174. In order to join a high school network through invitation, people within the network will need to accept a friend request from the user wanting to join the network and check that the requestor attends the high school in question. Facebook notes that sometimes more than one friend is required to confirm network status. Facebook.com, Networks and Network Pages, http://www.facebook.com/help.php?page=2 (last visited Dec. 18, 2007).

175. Ogg, *supra* note 161.

176. *Id.*

IV. DISCUSSION

The rich experiences available to minors over social networks are worth preserving despite potential dangers. In order to maintain such experiences and at the same time offer safer environments, lawmakers should retain the current legal regime and permit the services to spearhead safety efforts through self-regulatory means.

A. Advantages of the CDA/*Zeran* Framework

With respect to social networking services, the current legal regime is necessary for a robust market. The regime allows web-based services—particularly those that heavily rely on third party posted content like online social networks—to thrive.[177] The CDA permits online social networks to accomplish its most fundamental functions. Under this current regime, and the broad scope of immunity ushered in by *Zeran*, social networks are able to organize profiles into communities, provide search engines to categorize and publish profiles, and ask questions during the input process to facilitate the creation and development of profiles without the fear of lurking liability.[178] Arguably, without such broad immunity, online social networks might have limited their design choices and service offerings. For example, Professor Mark Lemley recently argued that the absence of any safe harbor immunity would cause internet intermediaries[179] to respond by "inefficiently restricting the uses that third parties can make of the Internet."[180] Lemley foresees absence of immunity leading to a scenario where the only internet intermediaries that exist are those that transmit "pre-approved content" similar to cable networks.[181]

If such a scenario is to unravel, social networks might disappear and take with them the "largely uncontrolled, unregulated, [and] unconstrained public space[s]"[182] that, at present, support numerous vibrant and diverse

177. *See generally* Ziniti, *supra* note 93 (describing ways the CDA has helped Web 2.0 services thrive).

178. Landry-Bell v. Various, Inc., 2005 U.S. Dist. LEXIS 38471, at *6 (W.D. La. Dec. 27, 2005).

179. Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101 (2007). While Lemley's paper directs its analysis to "service providers, Web hosting companies, Internet backbone providers, online marketplaces, and search engines," online social networks are applicable to Lemley's analysis because the sites share the same attribute that Lemley initially uses to tie his set of intermediaries—that is all use automated processes to handle volumes of data transfers, and to "host or link" large amounts of third part content.

180. *Id.* at 112.

181. *Id.*

182. Hinduja & Patchin, *supra* note 11 at 131.

communities. For minors, these communities create important experiences that make valuable contributions to identity formation and development.[183]

B. Why Self-Regulation Works for Child Safety Over Online Social Networks

Turning to the goal of child safety, online social networks are likely to develop the best solutions through self-regulation. They have the incentive and means to aggressively protect users as well as to minimize disruptions in content development and user interactions.

As a general matter, self-regulation has the potential of being ineffective where active consumer and citizen participation is absent.[184] However in this particular area, self-regulation works because sites have strong incentives from the public and media to improve safety. Steps taken by social networks already show that they are willing to improve safety because they are pushed by an interested public that expects safe internet experiences for children.[185] As in other areas of the internet, pleasing the marketplace has proven to be one of the strongest incentives for service providers to self-regulate.[186] Ultimately, among all stakeholders, online social networks are the most likely to cautiously weigh the benefits and risks when imposing limitations on its users. Sites are also likely more inclined to find means of effectively improving safety that completely avoid restricting service functionality. Indeed, when it comes to regulating user content and communications, laws in the past have created "overinclusive" effects that precluded non-injurious content, and impinged on the Constitution.[187] The Supreme Court invalidated portions of the CDA for such a reason in *Reno v. ACLU*.[188]

Online social networks are also inclined to produce the best solutions for at least two other reasons. First, sites benefit from the fact that they

---

183. *Id.*; *see also supra* Section II.B.4.

184. *See* Monroe E. Price & Stefaan G. Verhulst, Self -Regulation and the Internet 10 (2005).

185. *See* Lemos, *supra* note 165.

186. *See* Malcolm Maclachlan, *Self-Regulation Needed to Ensure Privacy*, TECHWEB NETWORK, March 13, 1998, http://www.techweb.com/wire/story/TWB19980313S0018; *see also* Glenn, *supra* note 158 at 1630-31.

187. *See* Monroe E. Price & Stefaan G. Verhulst, *The Concept of Self-Regulation and the Internet*, in PROTECTING OUR CHILDREN ON THE INTERNET 164 (Jens Waltermann & Marcel Machill eds., 2000).

188. Reno v. ACLU, 521 U.S. 844, 880 (1997) (striking down provisions as overly suppressive of communications when less restrictive alternatives existed); *see also* ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 221 (2007) (commenting on the Supreme Court's assessment of the CDA's constitutionality).

have extensive experience with both their own services and users.[189] Accordingly, services are in the strongest position to realize and attack areas of potential weakness on their sites. Second, as a general matter, online social networks are able to develop and implement measures more quickly than lawmakers are able to enact statutes through the political process.[190] This consideration is particularly important in a constantly evolving internet sphere where speedy reaction is essential.[191] For example, while the KIDS Act was still not law as of March 2008,[192] MySpace's sex offender identification system (announced only a few months prior to the introduction of KIDS) had already matched thousands of offenders to their online personas.[193]

C. Appropriate Areas for Legislative Action

Lawmakers, for their part, should work with online social networks to implement measures that affect procedures for obtaining service access. Such measures, that leave site functionality to the discretion of the online social networks, will tend to promote service innovation.

An appropriate role for legislatures is evident in KIDS. KIDS and its enacted and proposed state counterparts impose hefty penalties on sex offenders who use unregistered online identities on social networks.[194] By doing so, these statutes and proposals aid social networks by helping sites reduce the number of online predators accessing their services. KIDS and its brethren accomplish this in two ways. First, they create strong disincentives for at least some risk adverse sex offenders from venturing onto social networks. Second, they collect the information necessary for online social networks to actively monitor and prevent access to their sites by sex offenders. In this instance, the proposals enhance site safety while leaving intact the features that add to the richness of social networks.

---

189. *See* PRICE & VERHULST, *supra* note 184 at 9 (referencing former FTC chairman Robert Pitofsky's assertion that self-regulation is sometimes more "prompt, flexible, and effective than government regulation," and that "the judgment and experience of an industry" is of great benefit).

190. *See generally id.*; TAMBINI ET AL., CODIFYING CYBERSPACE: COMMUNICATIONS SELF-REGULATION IN THE AGE OF INTERNET CONVERGENCE 31 (2008) (noting, with respect to Europe, technology is changing fast and that regulation is too subject to procedural constraints to keep pace).

191. *See* Monroe E. Price & Stefaan G. Verhulst, *In Search of the Self: Charting the Course of Self-Regulation on the Internet in a Global Environment*, in REGULATING THE GLOBAL INFORMATION SOCIETY 75 (Christopher T. Marsden, ed., 2000).

192. OpenCongress.com, H.R.719 KIDS Act of 2007, http://www.opencongress.org/bill/110-h719/show (last visited Mar. 31, 2008).

193. Barrick, *supra* note 166.

194. Senators McCain and Schumer Introduce KIDS Act of 2007, *supra* note 145.

V. CONCLUSION

Online social networks create an avant-garde participatory culture that, among other great goals, supports the developmental growth of youth.[195] The user-driven interactive experiences fostered by social networks are worth preserving. While the danger of online sexual predators does exist, media attention and public pressure will continue to encourage social networks to make their sites safer for minors. As such, Section 230 of the Communications Decency Act works as Congress had intended. The CDA has permitted services to thrive while at the same time allowing sites to protect minors through self-regulation. Therefore, the current regime does not require wholesale modification. At most, lawmakers should create narrowly tailored statutes that support the safety measures already implemented by the online social networks.

195. *See* Hinduja & Patchin, *supra* note 11 at 131-32.