Kentucky Law Journal

Volume 97 | Issue 3 Article 6

2009

The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet

Samantha L. Millier
University of Kentucky

The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet

Samantha L. Millier[1]

INTRODUCTION

NOT long after Amy Polumbo was crowned Miss New Jersey in June of 2007, she was allegedly blackmailed using photos found on her Facebook profile.[2] Through a highly publicized confrontation with her blackmailer, Polumbo told NBC's *Today* show that the pictures were "meant to be private," that they were "supposed to be between my friends and I [sic]."[3] Luckily, the pageant board decided that although the photos were in "poor taste," they did not feature nudity and were not serious enough to strip Polumbo of her crown.[4]

The Polumbo incident epitomizes the first-person problem of online social networks. Presumably, these pictures were taken with Polumbo's knowledge, much like many of the pictures users place on their Facebook profiles. Either one of Polumbo's friends or a third party acquired the pictures and decided to blackmail her. This sort of problem is the type of privacy invasion online social network users face on a daily basis. Many users fail to realize the import of their decisions to pose for a picture or post personal information on their online profiles.

In the digital world of online social networks, users have grown accustomed to the free flow of information and expansive opportunities for self-expression. One of the most popular networks, Facebook, began as a networking tool on Harvard University's campus.[5] The site was created by Mark Zuckerberg, and was originally intended to serve as the online version of Harvard's paper publication of pictures and information about

1 B.A. from Colgate University, 2006; J.D. expected from University of Kentucky College of Law, 2009. The author would like to thank Professor Mark Kightlinger for his comments on and guidance with earlier drafts of this Note. All errors and omissions are the author's alone.

2 Wayne Parry, *'Private' Online Photos Really Aren't*, SFGATE, July 12, 2007, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/07/12/national/a135131D11.DTL&tsp=1.

3 *Id.*

4 *Id.*

5 John Cassidy, *ME Media: How Hanging Out on the Internet Became Big Business*, NEW YORKER, May 15, 2006, at 50, *available at* http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy?currentPage=1.

enrolling freshman.[6] The site quickly caught on at Harvard and rapidly expanded to other college campuses.[7] In the fall of 2006, Facebook opened to the public, and the privacy risks posed to users skyrocketed.[8]

From its inception, Facebook has appealed to "a powerful yearning: the desire of hundreds of ambitious and impressionable young people to establish themselves and make friends in an unfamiliar environment."[9] Working in tandem with this social desire, users have a sense of privacy in the information they post because their profiles are associated with particular social groups, like one's university, high school, or town, and only users in that social group may see members' profiles. This sense of privacy and familiarity encourages users to post personal information, pictures, and update their "status" to let friends know exactly what they are doing on a daily basis.[10] Though users have the means to limit public access to their profiles, some do not to realize they have this option or fail to activate available privacy restrictions.[11] Additionally, users frequently do not account for unknown third parties that have access to this information. Many users also fail to understand the "data mining" of personal information that is conducted by the private sector with permission from the network itself and, unknown to them, with the users' consent.[12]

Consider the example of Freddi Staur, a toy frog with a Facebook account. In a recent study conducted by Sophos, a Boston-based Internet security company, Freddi "friended" 200 Facebook members.[13] Of the 200, 82 accepted the frog's friendship request, and Freddi was thereby able to view these Facebook members' personal information.[14] Sophos' "research shows that 41% of Facebook users will divulge personal information—such as e-mail, address, date of birth and phone number—to a complete stranger."[15] Additionally, strangers were, in most cases, given access to family photos, intimate details about one's likes and dislikes, hobbies, employer details,

6 *Id.* at 50–52.

7 *Id.* at 52.

8 Michael Arrington, Facebook Just Launched Open Registrations, TechCrunch (Sept. 26, 2006), http://www.techcrunch.com/2006/09/26/facebook-just-launched-open-registrations/.

9 Cassidy, *supra* note 5, at 52.

10 *Id.*

11 Carly Brandenburg, Note, *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*, 60 FED. COMM. L.J. 597, 602 (2008).

12 Annie Schleicher, NewsHour Extra: Facebook, MySpace Launch New Targeted Ads, PBS Online NewsHour (Nov. 7, 2007), http://www.pbs.org/newshour/extra/features/july-dec07/social_11-07.pdf.

13 Mint.Com, HOWTO: Protect your Privacy on Facebook, MySpace, and LinkedIn (Sept. 6, 2007), http://blog.mint.com/blog/moneyhack/howto-protect-your-privacy-on-facebook-myspace-and-linkedin/.

14 *Id.*

15 Sophos, Facebook: The Privacy and Productivity Challenge, http://www.sophos.com/security/topic/facebook.html (last visited Oct. 6, 2008).

and other personal information.[16] The Sophos experiment illustrates the precarious nature of first–person problem: the desire to share information with one's friends may also expose users to unknown third parties who may misuse their information.

The fundamental problem with online social networks is the dichotomous demands of users: "People want access to all the information around them, but they also want complete control over their own information."[17] People's expectations of privacy are transforming, and as social networks like Facebook scramble to react to these changes, privacy law in the United States has been at a relative standstill. As the Internet and social networking sites continue to expand and become more integral to modern life, state legislatures have recognized the problem and have begun to take action.[18] These efforts are important progress in the right direction; however, given the global nature of the problem, it is important that the federal government take action.

This Note will address the changing conception of privacy on the Internet through an analysis of the online social networking site, Facebook. The purpose of this Note is to advocate a more modern conception of privacy and to argue for more thorough federal and state action to protect privacy online. Part I of this Note will discuss how online social networks function and the various risks associated with their use. Part II will analyze what privacy means within the context of the first–person problem and will discuss exactly what is sought to be protected. It will also introduce a modern conception of privacy: information privacy. Part III will consider current legislation regulating online social networks, including the Communications Decency Act, and will discuss the accesibilty of traditional forms of common law protection against the misuse of personal information. This section will discuss how U.S. laws and regulations may help to deter harmful activity and encourage more responsibilty on the part of online social network administrators. Part IV will consider the European Union's model of Internet privacy and compare it to the relative hands–off, self–regulatory approach taken by the U. S. government. Part V will discuss new legal constructs to protect against misuse of private information and will analyze the efficacy of current self–regulatory state action to protect social networks' users online. Finally, this Note will advocate for more protective, federal action, similar to the European Data–Protection Supervisor.

16 *Id.*

17 Cassidy, *supra* note 5, at 54 (quoting Mark Zuckerberg).

18 *See infra* notes 145–56 and accompanying text.

I. How Online Social Networks Work and the Risks They Present

As of August 26, 2008, 100 million users have registered on Facebook.[19] Creating an account is easy: go to www.facebook.com, enter your full name, birth date, e-mail, and register your password. Facebook will send a confirmation link to your registered e-mail, which you click on to complete registration. Once you have registered, Facebook presents you with what is essentially a template into which you may enter any information you choose. There is a place to upload an identifying picture and other personal or identifying information. Users may enter their relationship status; high schools, universities, and graduate schools attended; favorite music, movies, and books; hometown, current town, e-mail addresses, and home addresses.

Members may then start adding "friends" on the network, usually people one knows from the non-digital world, who must confirm your friendship before being granted corresponding access to the other person's profile. Members may control who views their personal information: they may make it available system-wide without discretion, or they may limit access to just their friends. Members may create photo albums, much like Web sites such as flickr.com or kodakgallery.com, and "tag," or identify by name, friends in their pictures: "[w]ith just a few clicks, a user can post a picture of a group of friends at a party, say, and 'tag' the image with their names for others to see."[20] By "tagging" a photo, Facebook creates a link the individual's profile from the photograph, making users easily identifiable, even when the viewer of the photograph is not "friends" with the photograph's subjects. "If a Facebook member in the picture objects, he can remove the link to his profile, but he can't get the picture taken down."[21]

Though most harm to users is generated by their own actions (communication with strangers, posting too much personal information, or allowing indiscriminate access to one's profile), there are serious problems caused by the actions of second and third parties. In a recent e-mail to Mark Zuckerberg's roommate, one user explains a common problem:

> By launching the photo feature and creating the system of easy linkages and tagging, you guys have dramatically changed social interactions . . . . Some people envision an upcoming era of "no camera" policies at parties and a growing sense of paranoia among college students worried that all their actions on Friday night appear online just hours later, accessible to hundreds or thousands of users (e.g., I can see Betty getting wasted at the

19 Posting of Mark Zuckerberg to The Facebook Blog, http://blog.facebook.com/blog.php?blog_id=company&m=8&y=2008 (Aug. 26, 2008, 3:21 EST).

20 Cassidy, *supra* note 5, at 58.

21 *Id.*

> [bar] even if I can't access Betty's profile). A single user with low privacy restrictions "overcomes/ruins" all the protective and restrictive steps taken by peers.[22]

The problem doesn't end here, though. Facebook is well known to employers, and the network is commonly used to conduct "background checks" on potential new hires.[23] This type of screening only exacerbates privacy concerns. Though users may have control over who may view their personal profiles, second and third parties are free to post information or images at their discretion.

One of the latest networks to spark controversy is JuicyCampus.com, which epitomizes the third–party problem posed by online social networks. As of October 6, 2008, the site offers services to 500 campuses with the plans to expand further.[24] Students may anonymously post comments about any topic, and the Web site assures its visitors that posts are 100% anonymous. The Web site also provides a search engine, so visitors may search for specific names without the hassle of perusing the entire site. The site explains on its FAQ page that the operators will not remove posts unless a court finds the post criminal, and claims immunity for everything posted on the site pursuant to section 230 of the Communications Decency Act.[25]

Posts on JuicyCampus.com range from innocuous to devastating. Students report anything from others' sexual exploits and other embarrassing information to simply discussing their favorite teachers or favorite bars on campus. Common discussion topics may include "the sluttiest girls" on campus or the "biggest cocaine users" on campus.[26] Though students' reactions to the site are mixed, there is a general consensus among college administrations and student leaders that the site needs to be banned or terminated.[27] For the time being, individuals remain free to anonymously spread rumors or reveal personal information about others.

Unauthorized exposure to third parties takes a different form on Facebook, where users may believe that they have control over personal information posted strictly on their personal profile, but this is not the case.

---

22 *Id.*

23 Brandenburg, *supra* note 11, at 598.

24 Posting of JuicyCampus to Official JuicyCampus Blog, http://juicycampus.blogspot.com/2008/10/500–campuses.html (Oct. 6, 2008, 11:12EST). As of February 5, 2009, JuicyCampus.com has closed. The author chose to keep this discussion to emphasize the recurring issues present on blogs and social networks.

25 JuicyCampus.com, Frequently Asked Questions, http://www.juicycampus.com/posts/faq (last visited Nov. 2, 2008); *see infra* Part III A and B.

26 David L.Hudson, Jr., *Taming the Gossipmongers: Websites That Dish Dirt May Soon Get Their Publishers' Hands Muddy*, ABA J., July 2008, at 19, 19.

27 MSNBC.com, Backlash Targets JuicyCampus.com: Students Protest Anonymous, Salacious Posts (Feb. 17, 2008), http://www.msnbc.msn.com/id/23211511/.

One of the more controversial examples of this lack of control is Facebook's targeted advertising based on users' listed interests and activities on the Internet (both on and off Facebook).[28] This type of "behavior advertising" is part of a larger advertising scheme utilized by the private sector that tracks Internet searches through cookies and collecting other relevant personal data used in determining what ads will pop–up while a specific user browses the Internet. Facebook utilizes a similar program and offers advertisers access to users' personal information listed on their Facebook profiles, much to the ignorance of Facebook users who post that content for social purposes. Users have consented to this data mining, however, usually by offhandedly clicking "I accept" to a release as a condition to adding certain third party programs to their profiles.[29]

In 2007, several mergers and acquisitions between online media advertisers sparked controversy in the United States and Europe and amplified the behavioral advertising issue. The Google–DoubleClick merger may be the most significant, and it was investigated by the Federal Trade Commission and the European Commission.[30] Of primary concern was the potential for the merged companies to amass and control a large amount of personal data.[31] Google collects "users' search history and Internet preferences, while DoubleClick is a leader in aggregating information on Internet preferences."[32] The main fear is that "Google's extensive library of user information coupled with DoubleClick's business model of consumer profiling could enable them to build extremely intimate portraits of individuals and unfairly exploit such information."[33] There is no current legislation regarding online advertising, and self–regulatory measures have proved ineffective according to the Electronic Privacy Information Group, a non–profit privacy activist group.[34]

In May 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with the Privacy Commissioner of Canada against Facebook, alleging that the site failed to inform members "how their personal information is disclosed to third parties for advertising and other profit–making activities and its failure to obtain permission from Facebook members to such uses and disclosures of their personal information."[35]

---

28 Schleicher, *supra* note 12.

29 *Id.*

30 Jacqueline Klosek et al., *International Legal Developments in Review: 2007 Industries*, 42 INT'L LAW. 621, 622 (2008).

31 *Id.*

32 *Id.*

33 *Id.* at 622–23.

34 *Id.* at 623.

35 News Release, Canadian International Public Interest Clinic, CIPPIC Files Privacy Complaint Against Facebook (May 30, 2008), http://www.cippic.ca/uploads/NewsRelease_30May08.pdf.

The complainant alleged that Facebook users are in the dark about the extent to which their personal data is being shared with advertisers and are being deceived about the level of privacy that exists on the site.[36] Specifically, users are confronted with form agreements to release all personal information to third parties, and users consent in order to have full access to utilities on the site.[37] Further, users are unaware of the extent to which their "friends'" privacy settings affect their personal privacy on the site.[38] The complaint alleged that such behavior is deceptive and in strict violation of the Canadian Personal Information Protection and Electronic Documents Act, of which the United States has no equivalent.[39]

The first–person problem of privacy on online social networks is clear. Users are not well informed concerning the risks posed when an individual posts information on the site. In fact, the site has successfully encouraged users to believe their personal data is private and under their individual control. Conversely, the ability of second parties to post personal information under lower privacy settings and for third parties to "mine" and misuse this personal information (originating from both the first person and second person) has the potential to seriously affect the lives of those involved, as well as any sense of security on the Internet. Yet, most users are ignorant of the extent to which their personal information is being used and disseminated throughout the Internet. In this digital world, questions remain as to exactly what is private on online social networks, what is worth protecting, and how personal information can be effectively protected.

II. WHAT IS PRIVATE?

A. Definition of Privacy on the Internet

Duncan Watts, a sociologist at Columbia University, has offered an explanation for the exponential popularity of Facebook among its eighteen to twenty–four year old, relatively better educated, and higher income demographic.[40] Watts claims "the growth of sites like Facebook and MySpace reflects a dramatic shift in how young people view the Internet."[41] After nearly a decade of study, Watts believes that the popularity of Web sites like Facebook "doesn't have anything to do with networking at all. It's voyeurism and exhibitionism. People like to express themselves, and they are curious about other people."[42] But proponents of the site paint a

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.*

40 Cassidy, *supra* note 5, at 55; *see* Schleicher, *supra* note 12.

41 Cassidy, *supra* note 5 at 55.

42 *Id.*

different picture. They claim that the positive aspects of free speech, self expression, networking, and business opportunities are immense on these sites, and these positive aspects outweigh the dangers, particularly for smart users.[43] In order for all users to benefit from these sites, it is important that they are protected from unseen dangers and privacy violations.

There are infinite articulations of what "privacy" means. Scholars differ on what attributes of privacy deserve focus. Scholarly definitions range in emphasis on personal autonomy, control over private information, or simple data protection.[44] Despite their differing definitions of privacy, scholars' "proffered justifications for protecting privacy include allowing individuals to define themselves and the information they want to share with others in the formation of relationships . . . that privacy provides for emotional release, invites self–evaluation, facilitates decision–making, and promotes physical and psychological autonomy."[45] One persuasive articulation of privacy is "information privacy," which offers insight into what should be protected online and why.

B. Information Privacy

Upon the advent of privacy law theory, wide–scale public communication was limited to print sources, such as newspapers and books.[46] With the emergence of radio and television in the early and mid–1900's, public communication became more direct and invasive to the family home. However, these methods of communication were regulated by the government, and private individuals rarely had access to such communication.[47] In distinct contrast to these earlier forms of communication, the Internet offers instantaneous access to hundreds of millions of users from inside their homes. The content and available information on the Internet is largely unregulated, and though an individual user may not necessarily have a powerful voice on the Internet, the potential

43 Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges and Promises of User–Generated Information Flows*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 741, 742–43, 748–52 (2008); Amy Dvorak, *LinkedIn? No, But I'll Try*, LEGAL MGMT., July/Aug. 2008, at 88.

44 Scott Rempell, *Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas*, 18 FLA. J. INT'L L. 807, 811–812 (2006). An in–depth analysis of the meaning of privacy is beyond the scope of this Note; however, the author advocates that control over information is the most relevant articulation of privacy when discussing the "first–party problem" of online social networks. For an in depth discussion of privacy, *see* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE. L. J. 421 (1980).

45 Rempell, *supra* note 44, at 812.

46 Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 889 (2006).

47 *Id.* at 889.

to reach millions is still there. This power presents unprecedented vulnerabilities to the privacy and safety of individuals.

Information privacy is "usually defined as the right of individuals to control information about themselves."[48] The concept of information privacy finds its basis primarily in "tort law of privacy, state and federal privacy legislation and the constitutional protections guaranteed by the First and Fourth Amendments."[49] Information privacy scholars, despite their many doctrinal disagreements, hold two common arguments and assumptions. First, there is a "binary distinction between 'decisional privacy' and 'information privacy.'"[50] Second, these scholars tend "to approach the problems of privacy from a technological or intellectual property background, and have been interested in the technical aspects of information regulation in addition to its jurisprudential implications."[51] Finding examples of both decisional and informational privacy in the holdings of seminal Supreme Court privacy cases, *Griswold v. Connecticut*,[52] *Roe v. Wade*,[53] and *Lawrence v. Texas*,[54] for example, scholars seem to lack coherency as to the definition of informational privacy.[55] It appears these scholars have extrapolated informational privacy from the guarantees of the First Amendment as interpreted in the Supreme Court's recent privacy holdings that identified a "zone of privacy."[56]

A preeminent information privacy scholar, Daniel Solove, has contributed extensively to the study and the development of privacy in the context of the Internet and social networking sites. Solove's academic focus is on the inadequacy of privacy law to address current problems presented by the Internet and advocates the "abandon[ment] of the binary view of privacy, which is based on the archaic notion that if you're public, you have no claim to privacy."[57] Solove advocates that privacy law should recognize an individual's social expectations of confidentiality and enforce duties upon others to that effect.[58] Solove has also opined that the modern explosion of Internet use and the consequential lack of control over personal information has in effect turned the Google search into "a digital scarlet letter."[59] Solove

48 Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006).

49 *Id.*

50 *Id.*

51 *Id.*

52 Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

53 Roe v. Wade, 410 U.S. 113, 152–53 (1973).

54 Lawrence v. Texas, 539 U.S. 558, 578 (2003).

55 Richards, *supra* note 48, at 1106–11.

56 *Id.* at 1111; *Griswold* 381 U.S. at 485.

57 DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 190 (2007).

58 *Id.* at 191.

59 Benjamin F. Heidlage, *Limiting the Scarlet A: Daniel Solove's the Future of Reputation*, 83

has proposed several solutions to the problem, including an expansion of privacy torts and expansion of "defamation liability to bloggers who fail to remove defamatory third-party comments"[60] as well as alternative dispute resolution for users to resolve privacy violations.[61] As discussed *infra*, these suggested solutions are certainly options, but recent case law interpreting existing federal law may be a better option.[62] In any case, the United States has yet to recognize information privacy in a manner that might allow for the expansion of privacy torts, but recent case law suggests the Supreme Court might be ready to make such a logical leap.

In *Lawrence v. Texas*, the Supreme Court invigorated the right to privacy.[63] When officers responded to a complaint and encountered two men engaged in homosexual sodomy, the men were arrested for violating a Texas state law that made homosexual sodomy illegal.[64] In striking down the Texas law as violative of the Due Process Clause, the Court based its holding on privacy grounds.[65] The Court identified two aspects of the constitutionally protected liberty interests: "spatial" and "transcendent" dimensions that guarantee freedom of one's person as well as freedom of thought, belief, expression, and intimate conduct.[66] The Supreme Court also based its holding on the realm of privacy found in precedent, history, and, most importantly, an "emerging awareness" in our culture.[67]

This *Lawrence* holding suggests an emboldened view of privacy by the Supreme Court, one that may be relevant for Internet privacy jurisprudence. The holding may leave open the possibility of judicial recognition of a constitutionally protected right of information privacy on online social networks based on the transcendent dimensions of privacy. If the government is held to a standard whereby they may not intrude upon a person's right to privacy in the bedroom or right to expression and belief, then why should private actors be held to a different standard? The threat is the same, the privacy interest violated is the same, and the risk of violation is even higher by virtue of the expansive exposure of personal information on the Internet.

N.Y.U. L. REV. 982, 983 (2008) (citing SOLOVE, *supra* note 57, at 94).

60 *Id.* at 986.

61 SOLOVE, *supra* note 57, at 191–92.

62 *See infra* Part III.

63 Lawrence v. Texas, 539 U.S. 558, 578 (2003).

64 *Id.* at 563.

65 *Id.* at 578.

66 *Id.* at 562.

67 *Id.* at 572.

C. The Unauthorized Viewer and Malicious Third Parties

There is little case law in the area of Internet privacy and the issues encountered on online social networks. As many of the safety and obscenity issues caused by these sites are beyond the scope of this Note, the remainder of the discussion will focus on the first–person problem of posted information that is misused or disseminated to unintended viewers and legal recourse for users whose privacy is compromised. Though case law suggests that individuals have a right to privacy where their expectations of privacy are reasonable, the status of legal remedies does not comport with the problem of the unauthorized viewer or a malicious second party.

As a general matter, courts have traditionally found that by placing information about oneself on a public forum like the Internet, the claim to a reasonable expectation of privacy is lost. Take, for example, *United States v. Gines–Perez*, where the court specifically addressed the issue of privacy and the Internet.[68] In *Gines–Perez*, the defendant was arrested on drug charges when his vehicle was stopped and searched by police, at which time drugs and drug paraphernalia were discovered.[69] The defendant was recognized by officers as a result of a photograph the officers had viewed previously on the Internet, allegedly downloaded from a private Internet site.[70] The defendant claimed he had an expectation of privacy in the site, and that access to the photograph constituted an illegal search and seizure.[71]

The court directly addressed the issue of constitutional privacy on the Internet, though they recognized there was "no clear guidance . . . available in case law."[72] Nonetheless, in the context of state action and the heightened privacy protection associated therewith, the court acknowledged that the applicable test is one of constitutional privacy.[73] Thus, the relevant inquiry is first "whether a person has exhibited an actual (subjective) expectation of privacy; and second, whether the expectation of privacy is one that society is prepared to recognize as 'reasonable.'"[74] The court stated that it was convinced that "placing information on the information superhighway necessarily makes said matter accessible to the public, no matter how many protectionist measures may be taken."[75] The court continued that it is "obvious that a claim to privacy is unavailable to

68 United States v. Gines–Perez, 214 F. Supp. 2d 205, 224–26 (D.P.R 2002).

69 *Id.*

70 *Id.* at 212–13

71 *Id.* at 213.

72 *Id.* at 225.

73 *Id.*

74 *Id.* (citing Katz v. United States, 389 U.S. 347, 361 (1967)).

75 *Id.*

someone who places information on an indisputably, public medium, such as the Internet, without taking any measure to protect the information."[76]

Within the context of privacy invasion conducted by private parties, the test for whether a privacy interest exists is largely the same. One recent case applies this test and may offer a useful analogy to the unauthorized third-party viewer problem on online social networks. In *Sanders v. American Broadcasting Companies*, Sanders brought an action for the tortious invasion of privacy by intrusion against a fellow employee who secretly taped conversations between the two for media production.[77] The court held that the tort may lie where a "'defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff . . . if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.'"[78] The court held that even though the conversation in question could have been overheard by other employees (but not the general public) making the plaintiff's expectation of privacy incomplete, the plaintiff may still have a cause of action for invasion of privacy.[79]

The *Sanders* holding was partially based on the common law concept of workplace privacy and that the recording was intended for media production. However, this result may be extrapolated to the first-person problem of online social networks. The court stated that "the reasonableness of a person's expectation of visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion."[80] Thus, in situations where a person may not have a reasonable expectation in, perhaps, intimate or lewd behavior at a party, they most likely do not expect a picture of the party to be posted on the Internet or the details of an intimate encounter described on JuicyCampus.com. Within the confines of that party, one expects that their behavior may be observed and repeated within their social circle, similar to the workplace environment. One may not, however, reasonably expect their behavior to be widely reported and recounted on an online social network so that the information is accessible to a large number of unknown users.

---

76 *Id.*

77 Sanders v. American Broadcasting Company, 978 P.2d 67, 70 (Cal. 1999). California adopted the tort of intrusion in *Shulman v. Group W. Productions, Inc.*, 955 P.2d 469, 490 (Cal. 1998). The RESTATEMENT (SECOND) OF TORTS § 652B (1977), as articulated in *Shulman*, describes the tort as follows: "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Id.*

78 *Sanders*, 978 P.2d at 71 (citing Shulman v. Group W. Productions, Inc., 955 P.2d 469, 490 (Cal. 1998)).

79 *Id.* at 77.

80 *Id.*

Though this type of privacy invasion is not on the same scale as a media production, there is still harm caused to the individual's privacy interest. It may be that the harm caused by dissemination to one's campus or circle of friends is equally devastating to the individual, and dissemination to the general public has only a slight incremental effect on the overall harm caused. In these situations, one should be able to claim a right to privacy in that information and bring a corresponding action in tort for the violation. The case may be, however, that the party disseminating the harmful information cannot be found.[81] In such cases it is paramount that the individual have an alternative course of action: either in the form of a cause of action against the service provider, or some sort of *ex post* remedy.

III. CURRENT LAW

A. The Communications Decency Act: An Act of Unintended Consequences

The Communications Decency Act (CDA), enacted in 1996, provides that "[n]o provider or user of an interactive computer device shall be treated as the publisher or speaker of any information provided by another information content provider."[82] The Act preempts civil liability for "'Good Samaritan' blocking and screening of offensive material" by the service provider.[83] Additionally, the Act states that "[n]othing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section [and] no liability may be imposed under any State or local law that is inconsistent with this section."[84] The scope of immunity provided by the Act has consistently been interpreted broadly: courts have not imposed any affirmative screening duties on network providers, and have consistently protected providers from liability where third party system users publish defamatory or other harmful information.

In the seminal case *Zeran v. America Online, Inc.*, the Fourth Circuit interpreted the scope of immunity provided by the CDA, an interpretation courts have followed for many years.[85] In this case, Zeran was presumably the object of a prank whereby an anonymous person posted Zeran's home telephone number on an Internet bulletin as the number to call in order to purchase offensive t–shirts regarding the Oklahoma City bombing.[86] Zeran received harassing telephone calls and complained to AOL to remove the post and issue a retraction; AOL removed the first post, but would not issue

81 *See* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (describing where an anonymous distributor of clandestine locker room videos could not be found).

82 Communications Decency Act, 47 U.S.C. § 230(c)(1) (2000).

83 47 U.S.C. § 230(c).

84 47 U.S.C. § 230(e)(3).

85 Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

86 *Id.* at 329.

a retraction.[87] Subsequently, the anonymous person posted multiple new bulletins for offensive t–shirts and other memorabilia with Zeran's number attached.[88] Zeran then brought an action against AOL alleging that the service "unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter."[89]

The *Zeran* court held that section 230 of the CDA, by its plain language, "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."[90] The court explained that "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred."[91] The court reasoned that section 230 was enacted in order to remove the "specter of liability" involved when a provider filters information posted by users, presumably qualifying providers as publishers of defamatory information that is not caught by filtering activities.[92] The court affirmed summary judgment in favor of AOL, citing the impracticality of requiring service providers to screen all posts, the "chilling effect" screening would have on users' First Amendment rights, and AOL's role as a provider entitled to immunity under section 230.[93]

Despite the policy objectives advocated by the *Zeran* court, the CDA also states that the policy promulgated under the Act is "to promote the continued development of the Internet and other interactive computer services."[94] Additionally, the Act is intended to "preserve the vibrant and competitive free market that presently exists for the Internet," and also to "encourage the development of the technologies which maximize user control over what information is received by individuals . . . who use the Internet."[95] Paradoxically, the CDA has been consistently used as a shield from liability for service and network providers rather than an impetus to increase individuals' control over their personal information that is disseminated over the Internet, and it offers little protection to users, either in the form of deterrence or *ex post* remedies.

87 *Id.*

88 *Id.*

89 *Id.* at 328.

90 *Id.* at 330.

91 *Id.*

92 *Id.* at 331.

93 *Id.* at 333.

94 Communications Decency Act, 47 U.S.C. § 230 (b)(1) (2000).

95 47 U.S.C. § 230 (b)(2)–(3).

B. Reinterpretation of the Communications Decency Act

Two recent federal court of appeals opinions suggest that the *Zeran* Court and its progeny have misinterpreted the CDA, which was actually intended to provide more protection to Internet users.[96] In *Chicago Lawyers' Committee v. Craigslist*, the Seventh Circuit affirmed the district court's holding denying liability under section 230 of the CDA.[97] In rendering its opinion, however, both courts declined to follow the expansive *Zeran* approach to section 230 interpretation. Instead, the Seventh Circuit explained that the *Zeran* holding "makes [Internet service providers] indifferent to the content of information they host or transmit."[98] The court noted that the word immunity is absent from the Act itself and nothing in the legislative history suggests the Act was meant to provide such broad immunity.[99] The court held that section 230 has a more narrow scope and only bars actions in which an Internet service provider would be treated as the publisher of third party content.[100] This means that actions like traditional defamation cannot lie under section 230, but the Act does not preclude other actions that do not treat the provider as a publisher.

More recently, in *Fair Housing Council v. Roommates.com*, the Ninth Circuit declined to apply section 230 immunity to a Web site that provided a roommate–matching service.[101] The Web site required users to register and create profiles by answering a series of questions regarding personal attributes and roommate preferences.[102] The Fair Housing Council brought an action against Roommates.com alleging that the Web site's actions allowed discriminatory postings in violation of the Fair Housing Act.[103]

The court held that the Web site had effectively become a "content provider" because "every... page is a collaborative effort between Roommate and the subscriber."[104] Thus, section 230 immunity was not available to the Web site. Though the court confirmed the ruling in *Craigslist* because that Web site in no way contributed to the development of illegal content, the court also stated that "[r]equiring website owners to refrain from taking affirmative acts that are unlawful [is not] an undue burden."[105] The court noted that where a "plaintiff would bring a claim under state or federal law based on a website operator's passive acquiescence in the misconduct of

96 Hudson, *supra* note 26, at 19–20.

97 Chicago Lawyers' Comm. v. Craigslist, 519 F.3d 666, 671 (7th Cir. 2008).

98 *Id.* at 670.

99 *Id.* at 671 (citing Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003)).

100 *Id.*

101 Fair Hous. Council v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008).

102 *Id.* at 1161–62.

103 *Id.* at 1162.

104 *Id.* at 1165, 1167.

105 *Id.* at 1169 n.24.

users, the website operator would likely be entitled to CDA immunity."[106] In response to the dissent's First Amendment concerns, the court stated that "[t]he [I]nternet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations."[107]

The *Roommates.com* decision is important because it clearly redefines and limits the scope of immunity provided by section 230 of the CDA. The court opens the door to the possibility that immunity might be denied in situations where the Web site operator is found to be partly responsible for the posted content.[108] The nature of Roommates.com is integral to the holding, however, because the Web site "'was structured in a way that sought out information that would lead to violations of the law.'"[109]

This fact is not fatal to the holding's applicability to online social networks. It may be that sites like JuicyCampus.com and Facebook encourage unlawful or tortious statements by their design. When one visits a site like JuicyCampus.com, they are bombarded with requests to post information about people at their school, proclaiming it is "the place to spill the juice about all the crazy stuff going on at your campus."[110] JuicyCampus.com assures visitors that their posts will be "100% anonymous" and even ranks posts as "most viewed," "most discussed," and "most agreed."[111] And on sites like Facebook, users are presented with a template in which to enter personal information or any other type of information they like, defamatory or otherwise.[112] Not only does the template provided ask for specific types of information, the social climate on the site serves to promote detailed disclosure between and among users.

By providing these fields and commands in an environment where users feel social pressures to participate, these social networking sites may in fact persuade one to post illegal or tortious content. This argument may certainly be made, and in that case, the rule articulated in *Roommates.com* should apply. Thus, reinterpretation of the CDA might provide a means by which individuals could enforce their right to privacy, in turn encouraging online social networks to engage in more active screening or censoring of tortious or otherwise harmful content.

106 *Id.*

107 *Id.* at 1164 n.15.

108 Hudson, *supra* note 26, at 20.

109 *Id.* (citing SOLOVE, *supra* note 57, at 94).

110 JuicyCampus.com, http://www.juicycampus.com (last visited Oct 13, 2008).

111 JuicyCampus.com, http://www.juicycampus.com/posts/gossips/all-campuses/ (last visited Oct. 13, 2008).

112 *See supra* notes 19–23 and accompanying text.

C. Tort Law

Traditionally, tort law has been the means by which one enforces his right to privacy against private actors.[113] Though tort actions have proven difficult to apply in the Internet context, causes of action such as false light, public disclosure, and defamation may translate well into the online social network context and offer some protection for users as well as a deterrent effect for misuse of personal information. For example, the *Restatement (Second) of Torts* defines the tort for public disclosure as "[o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[114] An additional requirement for tort liability is that the information must be "communicated to the general public or to enough people so that it is 'substantially certain to become public knowledge.'"[115] Similarly, false light and defamation require the information to be false, and published to a third party.[116] In the context of social networks like Facebook, however, vast public dissemination and false statements are rarely the problem. The problem typically comes from dissemination of truthful information or pictures within one's social circle, to data mining advertising agencies, or to unknown third parties, like employers, who may view the information. Thus, applicability of false light and defamation torts in the Internet context is seldom recognized.

Nevertheless, tort law may offer potential remedies for the purposes of online social network privacy. It might be possible to prove "public knowledge" in a more limited sense to include the "public" present on the particular online social network. This is suspect, however, because access is limited for the most part to those users who are "friends" with one another.[117] It may be argued that most of the damage created by disclosure of personal information is the damage caused within one's existing social circle, thus a re–definition of public dissemination may be appropriate. Alternatively, defamation and false light may prove to be applicable in situations where a third party has posted false information about another. This type of *ex post* protection may have a deterrent effect upon individuals using sites like JuicyCampus.com and Facebook from disseminating false

113 *See* Scott Jon Shagin, *The Prosser Privacy Torts in a Digital Age*, N.J. LAW., Apr. 2008, at 9.

114 RESTATEMENT (SECOND) OF TORTS § 652D (1977).

115 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, 1331 (2007) (quoting RESTATEMENT (SECOND) OF TORTS §652D, cmt. a (1977)).

116 RESTATEMENT (SECOND) OF TORTS § 558 (1977); Shagin, *supra* note 113, at 11–12.

117 Users must approve and verify that a person is a "friend" before they have corresponding access to each other's profiles. *See supra* notes 19–21 and accompanying text.

information. The question still remains what can be done about the harmful dissemination of accurate personal information.

IV. The European Model

The European Union (EU) has made a collective attempt to resolve these issues with the 1995 passage of the Data Protection Directive[118] in an effort to provide broad protection to individuals against "nonconsensual uses of personal data."[119] The Directive is based on the idea that "privacy is a fundamental human right,"[120] and has eight basic principles that limit the scope of personal data collection and dissemination.[121] The Directive provides that personal data may only be collected for "explicit and legitimate purposes, . . . [and] collections of data [may] be maintained only to the degree that they are relevant to the purpose for which they were collected, and that data be maintained in an accurate and . . . up–to–date form."[122] The Directive provides further protection by reflecting "an 'opt–in' system, under which each individual must provide unambiguous consent to the collection and use of personal information."[123] A data controller must inform individuals of the purposes for which their personal data may be used, and individuals must be given "a reasonable opportunity to access the data and to force the correction or deletion of inaccurate or inappropriately collected information."[124] In all, the Directive aims to give individuals extensive control over the use and dissemination of personal data, and imposes affirmative duties upon those entities that collect and manage such personal information.[125]

Although there has been a great deal of criticism concerning the adoption and implementation of the Directive's policy goals in individual European Union Member States,[126] many countries have successfully implemented such policies, serving as a useful example for the United States. A prime

118 Ronald J. Mann & Jane L. Winn, Electronic Commerce 210 (2d ed. 2005) ("[A] directive is a legislative template that, literally, directed member states to assess their existing laws on the topic . . . [imposing a duty on the member state] to enact legislation to bring its national law into conformity with the substance of the directive.").

119 *Id.*

120 *Id.*

121 Ryan Moshell, Comment, . . . *And Then There Was One: The Outlook for a Self–Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 Tex. Tech. L. Rev. 357, 368–69 (2005).

122 Mann & Winn, *supra* note 118, at 211.

123 *Id.*

124 *Id.*

125 The European concept of privacy is very similar to the expanding concept of information privacy.

126 Moshell, *supra* note 121, at 370–373.

example is the United Kingdom's Data Protection Act of 1998.[127] The Act applies broadly to "data processor[s]" and "data controller[s]" who control personal data about "data subjects."[128] A "data controller" is a party that "determines the purposes for which and the manner in which any personal data . . . are processed," and a "data processor" is a third party that "processes the data on behalf of the data controller."[129] The "data subject" is "an individual who is the subject of personal data."[130] The Act broadly defines "data" as any "information relating to individuals that . . . is structured . . . in such a way that specific information relating to a particular individual is readily accessible."[131] The Act operates in conformity with the EU Directive and provides extensive control to the individual regarding the processing and correction of personal data. Further, data may not be transferred to non–EU states, the United States included, that do not provide an adequate level of protection without enforcing safeguards for that information (usually in the form of contractual agreements).[132]

The European concept of data protection is similar to the emerging concept of information privacy, and in that respect, the European model may serve as a useful example for future U.S. action. Of particular importance is the creation in the United Kingdom and the European Union of independent regulatory bodies that enforce the Directive and the DPA, respectively. The idea of an independent enforcement body is compelling. Though the United States has articulated clear policies of self–regulation,[133] an independent body that would serve to enforce self–regulations (in conjunction with tort action and other federal regulations like the CDA) is a persuasive solution to the privacy issues presented by online social networks. Furthermore, the U.S. government has entered the private sector to regulate privacy before,[134] and the need for privacy regulation on online social networks is equally as great, and will continue to grow in importance as the Internet continues to proliferate.

127 Data Protection Act, 1998, c. 29 (Eng.). Similar acts have been adopted in Australia, New Zealand, Hong Kong, Taiwan, and Israel. MANN & WINN, *supra* note 118, at 212.

128 Data Protection Act, 1998, c. 29, § 1(1) (Eng.).; MANN & WINN, *supra* note 118, at 212.

129 Data Protection Act, 1998, c. 29, § 1(1) (Eng.).

130 *Id.*

131 *Id.* This definition includes a hybrid from both the "data" and "relevant filing system" definitions in the Act.

132 Data Protection Act, 1998, c. 29, sched. 1 (Eng.); MANN & WINN, *supra* note 118, at 213–16.

133 Moshell, *supra* note 121, at 373–77.

134 *Id.* at 373–85.

V. Proposed Solutions

A. Contractual Privacy

Scholars offer guidance with regard to how legal regimes should adjust to the increasing concern over privacy invasion on the Internet. One interesting approach to closing the gap in privacy law is proffered by Andrew J. McClurg in his article *Kiss and Tell: Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality.*[135] McClurg notes that we have entered into a new era, and genre really, of information privacy.[136] Information that is traditionally communicated through conversation is now immediately available in mass communication form.[137] In his article, McClurg expands on an argument advanced by Professor Eugene Volokh that "the only constitutionally permissible means for enforcing personal information privacy is contract law."[138] Specifically, McClurg argues that "an implied contract of confidentiality arises in intimate relationships that the parties will not disseminate through an instrument of mass communication private, embarrassing information (including photos or videotapes) about the other acquired during the relationship."[139] A major shortcoming of this theory is that it offers no protection for people whose private information is disseminated by third parties with whom they have little or no prior contact, or simply with whom the relationship does not rise to the level of "intimate." This approach may prove useful, however, when seeking remedies for the second-party problem presented by online social networks.

B. Facial Recognition Software

In situations where information, true or false, is posted by third parties who do not have any obligation that may arise from a close, confidential relationship, a pro-active *ex post* solution might be effective. In a recent note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, the author discusses the privacy implications of the widespread use of facial recognition software.[140] Facial recognition software exacerbates the problem by creating a searchable database of photos of unsuspecting individuals by matching an individual's name and face through comparison to previously

135 McClurg, *supra* note 46.

136 *Id.* at 887.

137 *Id.*

138 *Id.* at 888.

139 *Id.*

140 Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy*, 120 Harv. L. Rev. 1870 (2007).

tagged photos.[141] This type of software sifts through photographs available to the public on Internet sites and matches faces with registered users; Polar Rose is one such server that searches all photographs available on the web.[142] The author recognizes that intimate, spontaneous, and/or impulsive actions that are out of character have the unique ability to be documented and disseminated world–wide on the Internet.[143] The note argues that the databases created by facial recognition software present a precarious violation of privacy and the author advocates an "opt–out" regime by which individuals may prevent their names from appearing on these databases.[144]

While the aforementioned note paints a devastating picture of privacy on the Internet caused by the use of facial recognition software, widespread use of these search engines may offer much needed protection from the dissemination of potentially harmful photographs of private individuals. In situations where compromising photographs of unsuspecting victims were disseminated on the Internet by third parties to the detriment of the photograph's subjects—which may result in loss of employment and social scrutiny—facial recognition software may offer a solution.[145] Instead of utilizing such software to create privacy violations, sites like Facebook could be required to offer this software to users as a means to notify users when pictures (tagged or untagged) of themselves are upoloaded onto the site. Users could thereby be offered an opportunity to protect against the dissemination of unwanted personal photographs.

C. Self–Regulation and Anonymous Removal Systems

The positive uses of facial recognition software and the McClurg formulation have shortcomings. They do not protect the individual from the harm caused by dissemination of private, written information, or from the dissemination of photos that may hypothetically fall through the screening system of facial recognition software because of the angle or blurriness of the photo. In accordance with U.S. policy in favor of self–regulation, on September 3, 2008, New Jersey Attorney General Ann Milgram reported that Facebook would begin testing a program called "Report Abuse," designed to be used as a self–help privacy protection tool on the social networking site.[146] The purpose of the program is to "provide an easy–to–recognize and easy–to–use mechanism to report inappropriate content,

141 *Id.* at 1871–73.

142 *Id.* at 1871–72.

143 *Id.* at 1874–75.

144 *Id.* at 1873, 1887.

145 *Id.*

146 Amy E. Bivins, *Cybersecurity: Facebook Social Networking Service to Test New Jersey 'Report Abuse!' Complaint System*, E–COMMERCE LAW DAILY (BNA), Sept. 4, 2008.

cyber predators, and online bullies to social networking website operators and law enforcement authorities."[147]

The "test-run" for this program will provide a link on randomly selected Facebook Web pages, and clicking on the prominently placed icon will allow users to report many types of online abuse as well as provide users with online safety tips.[148] The link will not appear on all pages until after this temporary trial period, when Facebook and state officials convene to discuss the success of the trial.[149] The "Report Abuse" system imposes affirmative monitoring duties—unlike the CDA—on an Internet service provider that agrees to display the icon and utilize the system.[150] Specifically, "a service must agree to follow certain standards of service, including reviewing and routing complaints to appropriate law enforcement agencies."[151] Interestingly, the "Report Abuse" program is already running on several social networking cites, including "myYearbook.com, BlackPlanet.com, MiGente.com, Glee.com, Faithbase.com, Dweeber.com, and AsianAve.com."[152]

The inauguration of such self-help technology on online social networks is part of a larger push for self-regulation to protect children from online predators.[153] As part of this effort, "Facebook, together with attorneys general from 48 states and the District of Columbia, announced May 8, [2008], that the service joined an Internet safety technical task force formed in January as part of an agreement between the attorneys general and social networking site MySpace."[154] The task force is "led by Harvard Law School's Berkman Center for Internet & Society," and has agreed to issue a "formal report with findings and recommendations for social networking site privacy and child protection self-regulation" by the end of 2008.[155] It has been suggested however, that "if those sites do not comply with the agreement and devise an effective self-regulatory system for protecting children online, it could create an incentive for lawmakers to push additional legislation."[156]

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 *Id.*

152 *Id.*

153 *Id.* This movement has included several legislative efforts, both federal and state, but few have come to fruition. "Included in these efforts are state bills requiring parental access to children's online profiles, but "the bills died in Iowa (H.F. 2202) and Florida (H.B. 1029/S.B. 2232), and proposals in New Jersey (A. 108/S.B. 1132) and Illinois (H.B. 4874/S.B. 1682) have yet to move out of committee." *Id.*

154 *Id.*

155 *Id.*

156 *Id.* Attorneys have suggested that if an agreement on self regulation is not satisfactory, legislatures will take immediate action.

Though much of what this task force is designed to accomplish is beyond the scope of this Note, it offers hope that change in Internet privacy law may be afoot. The "Report Abuse" program has important implications for the future of privacy. A similar program could be implemented whereby users are able to click on a link entitled "Privacy Violation" to report the unauthorized dissemination of personal information or unwanted photos. The link could provide anonymous removal requests be sent to offending users who would then have the opportunity to chose to remove the material. If the offending user does not respond to these requests, then an additional layer of protection could be offered whereby Facebook would have the power to remove objectively offensive material.[157]

CONCLUSION

Privacy as we know it is changing. As the Internet continues to shape our lives and individuals develop digital personas, privacy should be conceptualized as control over one's personal information: both substantive information and behavioral information. In order to better protect an individual's digital persona, a regime of deterrence and accountability must be formed to prevent egregious privacy violations. To accomplish this objective, privacy law should redirect its focus primarily to the online service provider. The CDA should continue to be interpreted to impose liability where the service provider contributes to the creation of user content, as seen in *Roommates.com*[158] and *Craigslist*.[159] The implementation of self-regulatory systems, like "Report Abuse," that impose affirmative reporting and monitoring duties when the provider is notified of unlawful behavior, will create accountability and subsequently decrease online privacy risks.

As for the risks posed by second and third parties, tort liability and contractual privacy should be expanded to apply to Internet privacy violations. Instances of privacy violations should be investigated by an independent body, either a federal agency or a non-profit privacy rights advocate group, in order to create an Internet culture that holds people responsible for tortious behavior. Additionally, *ex post* remedies should be provided to social network users, such as an anonymous removal request systems and the positive use of facial recognition software. Facebook and similar social networking sites should also change their privacy policy from an opt-out structure, to an opt-in structure in order to ensure users understand the import of their privacy settings. But most importantly, users need to become more educated about the use of personal information and

157 Though there are obvious First Amendment concerns with this sort of program, these issues are beyond the scope of this Note.

158 Fair Hous. Council v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008).

159 Chicago Lawyers' Comm. v. Craigslist, 519 F.3d 666 (7th Cir. 2008).

the potential for harm on these networks in order to take individual action to decrease their risks. Though the law of privacy will continue to change through this digital dialectic, one thing remains clear: privacy law in the United States can no longer stand still.