Social Media: No 'Friend' of Personal Privacy

Christopher F. Spinelli

Corporate Communications
Elon University

Abstract

This comment examines the lack of regulation of social media websites, such as Facebook and MySpace, and the effects this lack of regulations has had on the liberties guaranteed by the Fourth Amendment to the United States Constitution. This comment argues that by establishing privacy settings on social networking websites, users construct a reasonable expectation of privacy. Examples are provided to illustrate the detrimental nature and ineffectiveness of industry self-regulation. A relevant case study is explored to highlight the societal concerns that are being brought forth within the legal system at an ever-increasing rate. Scholarly opinion is then analyzed in order to reinterpret privacy law so that it properly adapts to rapidly evolving social media networks within cyberspace.

I. Introduction

Industry leaders Facebook and MySpace have largely defined the advent of popular social networking websites. According to Hitwise, a distinguished tracking service, Facebook alone comprises approximately 7.07 percent of all Internet visits.[1] Furthermore, Facebook and MySpace account for an estimated 249 million unique visitors monthly and, on average, Facebook users spend about 6 hours and 30 minutes on the site every month.[2] These statistics are nothing short of remarkable considering that, to a large extent, these websites did not exist prior to 2006.

Social networking websites such as Facebook and MySpace often divulge personal information through the inclusion of personal profiles, pictures, video, and the ability to send messages to friends, family, co-workers, and acquaintances. These key features have raised significant privacy concerns for individual users of these websites. Current policy dictates that the social networking industry should practice self-regulation. However, there has been frequent public objection to self-regulation. Social networking websites have based their arguments on the fact that higher rates of disclosure produce increased revenues. Therefore, social networking sites are less likely to have their users best interests in mind when the disclosure of personal information is at stake. As Brooklyn Law School professor Paul M. Schwartz argues, "Legal protection

****Keywords***: Facebook, MySpace, Fourth Amendment, Social Media Regulation, Privacy Law, Expectations of Privacy in Cyberspace

Email: cspinelli33@gmail.com

1 Reinan, John. "Facebook Overtakes Google -- and the Marketing World Salivates." *MinnPost.com (blog)*. 12 Apr. 2010. Web.

2 ComScore. Marketing Communications. *Social Networking Explodes Worldwide as Sites Increase Their Focus on Cultural Relevance*. ComScore, 12 Aug. 2008. Web.

of personal information on the Internet is generally limited and often incoherent."[3] Additionally, law and policy has been slow in keeping up with the ever-evolving social networking applications that have developed over the course of the past decade. More specifically, "Despite the centrality of these issues the American courts lack a coherent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons. Indeed, jurisdictions cannot agree on a framework for resolving these kinds of cases."[4] The following document will provide an overview of the court decisions and policy initiatives that relate to this discussion. In addition, it will provide a brief summary of the legal opinions held by several attorneys and law professors.

The main focus of this article is to demonstrate how privacy law should evolve to account for the technological advancement of the Internet with a particular emphasis on the social media networks Facebook and MySpace. Although the Supreme Court has been hesitant to definitively rule on this issue, lower court opinions, legal ethics opinions, and relevant policy are included in this comment. These sources are examined in order to understand how the law is approaching the privacy issues surrounding social media including "cyberbullying," employment practices, and law enforcement monitoring of the internet. Through careful analysis, it can be determined how policymakers and the courts can aid in resolving these issues and progressively establish a more clear definition of the legal obligations placed on Facebook and MySpace. After doing so, this article argues that that by recognizing privacy abuse on social networking websites, Congress can pass and enforce new laws that protect Americans from these harms and provide greater protection to individual privacy.

II. Current policy

To a large extent, social networking websites receive government protection from policy written in the 1990s. Section 230 of the Communications Decency Act ("CDA") protects Facebook and MySpace. This policy states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[5] In other words, if person A posts a defamatory comment about person B on a social networking website such as Facebook, person B cannot sue Facebook for allowing the post because social networks cannot be found liable for these criminal damages. The Act establishes the notion of "cyberspace exceptionalism," a concept that endorses the belief that, "the Internet is unique/special/different and therefore should be regulated differently. Section 230 of the CDA is a flagship example of such exceptionalism. It creates rules that really differ between the online and offline worlds, such that publishing content online may not create liability where publishing the identical content offline would. The medium matters."[6]

III. Fourth amendment background & applicable Supreme Court decisions

The Fourth Amendment protects "the people" from "unreasonable searches and seizures."[7] In 1967 the Supreme Court handed down its decision in *Katz v. United States*.[8] Prior to this date, the Court had adopted a literal interpretation of the Fourth Amendment. It had ruled that a violation of privacy could only occur

3 Schwartz, Paul M. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52.1607 (1999), 1632. *LexisNexis*. Web.

4 Strahilevitz, Lior J. "A Social Networks Theory of Privacy." *The University of Chicago Law Review* 72.3, 921. *JSTOR*. Web. Summer 2005.

5 Congressional Research Service, Library of Congress (1996) (enacted). Print.

6 Goldman, Eric. "Re: Roommates.com Denied 230 Immunity by Ninth Circuit En Banc (With My Comments)." Web log comment. *Technology & Marketing Law Blog*. 3 Apr. 2008. Web. <http://blog.ericgoldman.org/archives/2008/04/roommatescom_de_1.htm>.

7 U.S. Const. amend IV.

8 Katz v. United States, 389 U.S. 347 (1967).

in a physical or tangible sense. In other words, "the Fourth Amendment was not violated as long as there was no official search of a person, or his tangible, material effects."[9] Thus, establishing the trespass doctrine, which held that the Fourth Amendment is not implicated unless there is a physical intrusion, or trespass, into a private area such as an individual's residence. In the landmark privacy case of *Olmstead v. United States* this doctrine was upheld in light of the advent of wiretapping technology. Recognizing the dangers this ruling posed to the Fourth Amendment in light of technological advances, Justice Brandeis authored a famous dissent, hinting at a new Fourth Amendment standard:

> Time works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available… Discovery and invention have made it possible… by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. Can it be that the Constitution affords no protection against such invasions of individual security?[10]

Justice Brandeis' words emphasize the dangers that the advancement of technology poses to individual privacy. His view was ultimately vindicated nearly 40 years later in *Katz*.

Fearful of the limited protection that a trespass standard provided, *Katz* adopted a two-step approach to determine the legality of Fourth Amendment searches and seizures. Justice Harlan explained in his concurring opinion: "there is a twofold requirement, first, that a person have exhibited an actual expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[11] Thus, Harlan established the modern Fourth Amendment standard for a search: an invasion of a zone of which a person has a reasonable expectation of privacy

In regards to this discussion, the question then becomes, "how is this construction of the Fourth Amendment then applied to an intangible medium such as a social networking website?" To date, the Supreme Court has yet to consider this question. Therefore, the lower courts are forced to draw analogies to Supreme Court rulings dealing with situations outside of cyberspace.

Some courts have expressed their discontent with this approach. For instance, in *United States v. Walser* the Tenth Circuit Judge Stephanie Seymour stated, "[t]he advent of the electronic age and . . . the development of desktop computers . . . go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law."[12] Yet, the fact remains that lower courts are forced to connect expectations of privacy on the Internet with the provisions outlined in *Katz*. In doing so, they have relied largely on *Smith v. Maryland* and *United States v. Miller*. In *Smith*, the Court ruled that the installation of a pen register did not constitute a search that would breach the defendant's reasonable expectation of privacy.[13] For clarification, "A pen register is a device installed by the telephone company which can track the phone numbers of all calls outgoing from a person's house."[14] Therefore, since the numbers are automatically shared with a third party, the telephone company, an individual cannot reasonably expect this information to be private.

In *Miller*, the Court ruled that a person does not have a reasonable expectation of privacy over his bank records. In delivering the majority opinion Justice Powell stated, "documents subpoenaed are not [Miller's] 'private papers', but instead, part of the bank's business records." Therefore, "Miller's rights were not violated when a third party - his bank - transmitted information that he had entrusted them with to the government."[15]

In most respects, the decisions handed down in both *Smith* and *Miller* permit the government to, with-

9 See Olmstead v. United States, 277 U.S. 438, 466 (1928).

10 Id. at 472-73 ("Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.") Id at 472 (Brandeis, J., dissenting).

11 Katz, 389 U.S. at 361.

12 United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

13 Smith v. Maryland, 442 U.S. 735 (1979).

14 Hodge, Matthew J. "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com." *Southern Illinois University Law Journal* 31.95 (2006), 102. *LexisNexis*. Web.

15 United States v. Miller, 425 U.S. 435 (1976).

out any suspicion at all, seize and search the records of third party entities, such as Facebook and MySpace.

However, as Matthew Hodge states in his comment, state and appellate courts have not strictly adhered to these rulings when interpreting an expectation of privacy based their own *state* constitutions.[16] Furthermore, Congress itself has passed legislation that has largely supplanted these rulings.[17]

IV. Consequences of pure market self-regulation

In most cases, the policies previously described have been used to protect the social media industry and have not protected an Internet user's privacy. Essentially, social media outlets have been permitted to regulate themselves. Paul Schwartz advances two critical assertions why this self-regulation has been largely ineffective in protecting one's privacy on the Internet. "(1) the 'knowledge gap,' which refers to the widespread ignorance regarding terms that regulate disclosure or nondisclosure of personal information and (2) the 'consent fallacy,' which points to weaknesses in the nature of agreement to data use. Both support a conclusion that reliance on a privacy market will not generate appropriate rules regarding personal data use in cyberspace."[18] Further research has shown that Schwartz is quite correct in this assessment, especially when applied to social networking websites. According to a research survey conducted by students at M.I.T. in 2005, over 90% of users of Facebook said that they had not read the site's terms and conditions.[19] Additionally, in December 2009 Facebook overhauled the privacy settings of every user's profile and reset them to the default. In conducting its own survey, Facebook revealed that 35% of users had read the documentation outlining this change and modified their privacy settings appropriately. Therefore, 65% remained largely unaware of whom their information was being shared with.[20] In investigating this development, Danah Boyd, a Social Media Researcher at Microsoft Research New England, has noted that in her interviews with Facebook users she has yet to find an individual who could correctly describe their current privacy settings. In a recent speech, Boyd narrated a story involving a woman who had moved away from her abusive father. "The young woman talked with her mother (who had moved with her) about possibly joining Facebook. They sat down to make the content as private as possible, which worked well. But in December, the young woman clicked through Facebook's privacy dialog (as most people did) and had no idea her content was public. She only found out when someone who should not have seen the content told her."[21]

In conjunction with Boyd's analysis, in March 2009 Cambridge University's Computing Laboratory published a report criticizing Facebook for its excessive use of pithy legal language within its terms of service document. These criticisms stem from the fact that Facebook has publicly claimed to be a democratic service, when in fact, if read carefully, its terms of service prove otherwise. As Professor Ross Anderson of Cambridge University stated following the release of the aforementioned study, "We should not be surprised that corporations do not want to give power to their users, but pretending that the site is democratic when it is not is offensive - it is reminiscent of the old German Democratic Republic, which was actually a Russian colony and not democratic at all."[22] The report itself identifies several terms that are particularly vague and can produce multiple interpretations.

Facebook has failed by its own standards by not providing a Statement that is clear and free

16 Hodge, "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com" 103.

17 Hodge, "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com" 104.

18 Schwartz, Paul M. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52.1607 (1999), 1683 *LexisNexis*. Web.

19 The Global Covenant Network. *The Shocking Truth of Facebook*. I-Newswire, 2 Aug. 2008. Web.

20 Kincaid, Jason. "Danah Boyd: How Technology Makes A Mess Of Privacy and Publicity." *TechCrunch*. WordPress.com, 13 Mar. 2010. Web.

21 Kincaid, "Danah Boyd: How Technology Makes A Mess Of Privacy and Publicity."

22 Saran, Cliff. "Cambridge Researchers Slam Facebook Democracy." *ComputerWeekly.com*. Reed Business Information Ltd, 17 Apr. 2009. Web. <http://www.computerweekly.com/Articles/2009/04/17/235687/cambridge-researchers-slam-facebook-democracy.htm>.

> from "legalese." §14 "Disputes" is a particularly bad example, as the Statement contains many loaded legal terms such as "indemnify and hold harmless," which most users will not be able to properly interpret. §14.3 then provides a long disclaimer of responsibility, which is typed in all capital letters, limiting readability, and contains technical phrases such as "NON-INFRINGEMENT," "DAMAGES, KNOWN AND UNKNOWN," and "MATERIALLY AFFECTED." Finally, §16, "Other," adds several more critical disclaimers of responsibility in a set of seven disorganized sentences… the Statement reverts to increasingly arcane legal formalisms after most users will have stopped reading."[23]

Yet, the most troubling revelation that the Cambridge report discloses is the way in which Facebook has concealed the details of its privacy policy.

> The Privacy Policy and several other documents are referenced by the Statement but not included in it, and must be accessed separately despite §16.1, which says, 'This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.' The privacy policy is glossed over with the platitude 'Your privacy is very important to us,' which might re-assure users who will then skip over reading it, despite it carrying the same legal weight as the Statement. [24]

Boyd's story and the analysis conducted by Cambridge University's Computing Laboratory illustrates that self-regulation has prompted social networking websites to take advantage of both the "knowledge gap" and "consent fallacy" for purely financial gains. The greater number of profiles that are open to the public increases the likelihood that advertisers will utilize the website. Default privacy settings allow companies to view a person's interests, hobbies, etc. and advertise certain products to a specific individual. To generate considerable profit, social networking websites need to appeal to these advertisers. Therefore, ensuring that a large number of profiles remain public, to a large extent, conforms to the website's financial interests.

V. Determining expectations of privacy on Facebook or MySpace

Law professor James Grimmelmann analyzes a pertinent case study in his lecture on Internet privacy and its application to Facebook,

> "In 2006, two students at the University of Illinois were urinating on the front of a bar. When a police officer approached, Marc Chiles escaped while Adam Gartner was detained. Gartner denied knowing Chiles. Later, the officer accessed Facebook and scoured student profiles. When he realized Chiles and Gartner were Friends on Facebook the officer charged the latter with obstruction of justice."[25]

Grimmelmann goes on to explain that, "when users make privacy choices using Facebook's technical controls, they're expressing expectations about who will and won't see their information, and society should treat those expectations as reasonable for Fourth Amendment purposes."[26] However, to date, Facebook has not been held legally responsible for policing its own network. Although it explicitly states to its users that it has no control over the actions of other individuals using the website, there should at least be some measures taken to deter hackers or law enforcement officials from using the network in a criminal manner, legally or otherwise. The same M.I.T. students who reported that over 90% of users of Facebook stated that they had not read the site's terms and conditions, were also able to download over 70,000 profiles using an applica-

---

23 Bonneau, Joseph, Soren Preibusch, Jonathan Anderson, Richard Clayton, and Ross Anderson. *Democracy Theatre: Comments on Facebooks Proposed Governance Scheme*. Rep. University of Cambridge Computer Laboratory, 2009. 4-5. Web. <http://preibusch.de/publications/Bonneau_Preibusch_Anderson_Clayton_Anderson__Facebook_Governance_Comments.pdf>.

24 Bonneau, Preibusch, J. Anderson, Clayton, and R. Anderson, *Democracy Theatre: Comments on Facebooks Proposed Governance Scheme* 5.

25 Grimmelmann, James. *Internet Law: Spring 2010*. *Reading Packet 3: Privacy, 50*. New York Law School. Web. <http://james.grimmelmann.net/courses/internet/Internet2010SReader3.pdf>.

26 Grimmelmann, James. "Saving Facebook." *Iowa Law Review* 94 (2009), 1197. *JSTOR*. Web.

tion they had created.[27] What's more troubling is that Grimmelmann reports, "Facebook has trouble controlling its own employees, who treat access to profile and user-activity information as a 'job perk."[28] This kind of unwanted disclosure has recently led to a number of state and appellate cases, which will be discussed in greater detail below. As indicated earlier, the courts have received little guidance from the federal government in ruling on this issue.

VI. "Cyberbullying:" a product of unwanted disclosure

"Cyberbullying" has emerged as a prominent Internet safety concern over the course of the past several years. A United States research center dedicated to the study and prevention of cyberbullying has defined it as, "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices."[29] Therefore, cyberbullying clearly constitutes as a violation of the privacy rights that protect against the disclosure of private facts that would be considered highly offensive to a reasonable person, and the placing of someone in a false light. Facebook and MySpace are two mediums where cyberbullying has occurred quite frequently. The lack of website surveillance, and an effective legal response, has aided in facilitating this type of behavior. This has resulted in the filing of a number of recent lawsuits. The most current being, *Finkel v. Facebook*.[30]

There, teenager Denise Finkel sued four high school students, their parents, and Facebook arguing that they were liable for the production of defamatory statements made about her. The suit began after Finkel discovered that the four students had created a Facebook group entitled, "90 Cents Short of a Dollar." Statements made within the group declared and implied that Finkel "was a woman of dubious morals, dubious sexual character, having engaged in bestiality, an 'IV drug user' as well as having contracted the H.I.V. virus and AIDS."[31] Finkel asserted in her complaint that Facebook should be held accountable for allowing the defamatory material to be published on its website claiming, "[Facebook] should have known that such statements were false and/or have taken steps to verify the genuineness of the statements."[32] Predictably, the court granted Facebook's motion to dismiss the charges as a result of the protection supplied under Section 230 of the CDA. However, Finkel's attorney's response raised an interesting argument. They chose to highlight that in its terms of service Facebook claims ownership of the material posted on their website. As a result, "Facebook wants to use the CDA as a shield to immunize itself form being sued for defamation due to any postings of its users while also claiming ownership of the content posted on its site."[33] To a large extent, these assertions are meritless and the court rejected this response due to the fact that "Ownership of content plays no role in the Act's statutory scheme."[34] Ultimately, there is no precedent to support Finkle's claim that ownership should establish liability under Section 230 of the CDA. However, this argument shows that Facebook has been permitted to, as the cliché goes, have its cake and eat it too. Policies should be enacted to prevent Facebook from claiming ownerships over its materials and at the same time being absolved of responsibility over the very material it owns.

Current federal policy has also ineffectively punished individual users who have abused their use of

27 I-Newswire, *The Shocking Truth of Facebook*.

28 Grimmelmann, "Saving Facebook" 1183.

29 *Cyberbullying Research Center*. Web. <http://www.cyberbullying.us/index.php>.

30 "Finkel v. Facebook." *Citizen Media Law Project*. Berkman Center for Internet & Society, 3 Mar. 2009. Web.

31 "Finkel v. Facebook." Cmplt. ¶ 23.

32 "Finkel v. Facebook." Id. ¶ 28.

33 Altschul, Mark M. "Finkel Opposition to Facebook Motion to Dismiss." Letter to Supreme Court of the State of New York. 16 Feb. 2009. *Citizen Media Law Project*. *Citizen Media Law Project*. Web.

<http://www.citmedialaw.org/sites/citmedialaw.org/files/2009-03-26-Finkel%20Opposition%20to%20Facebook%20Motion%20to%20Dismiss.pdf>.

34 Alonso, Morris D. "Notice of Motion to Dismiss." Letter to Altschul & Altschul & Orrick Herrington & Sutcliffe. 23 Apr. 2009. *Citizen Media Law Project*. Web. <http://www.citmedialaw.org/sites/citmedialaw.org/files/2009-04-23%20Finkle-%20Schwartz%20notice%20of%20motion%20to%20dismiss.pdf>.

Facebook and MySpace. For instance, in *United States v. Drew*[35] a 47-year-old mother, Lori Drew, was partly responsible for the suicide of 13-year-old Megan Meier. Drew created a fake MySpace account and contacted Meier posing as a 16-year-old boy. Using the account, Drew harassed Meier and inflicted significant emotional distress. A month after the fake account was created, Meier hung herself in her bedroom closet. Drew was later indicted and accused of violating the Computer Fraud and Abuse Act on several counts. One of the charges brought against Drew accused her of violating MySpace's terms of service as a result of her accessing MySpace servers in order to gather more information on Meier. The creation of a false account violated MySpace's terms and conditions as well. The indictment was legally questionable because the Computer Fraud and Abuse Act, as currently written, only encompasses federal, state, and designated financial computer systems. As a result, on August 28, 2009, Drew was acquitted of these charges.

This case has incited a significant call to change state and federal policy. Most notable is a bill introduced to Congress on August 2, 2009, titled the Megan Meier Cyberbullying Prevention Act. If it were to be passed, the bill would establish a federal definition of cyberbullying and criminalize online communication that is done "with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person."[36]

Further highlighting the ineffectiveness of social networking website self-regulation, in February 2007 a case titled *Doe v. MySpace* attempted to reframe the responsibility of social networking websites in the context of protection from sexual predators. The plaintiff accused MySpace of negligence that stemmed from the belief that MySpace should have "implemented basic safety measures to prevent sexual predators from communicating with minors."[37] The District Court again denied these claims on the basis of the Communications Decency Act. The Appeal's Court affirmed this decision, relying on precedent established in *Green v. AOL* and finding that MySpace was not liable for user-generated content on its website.[38] The Supreme Court denied certiorari to hear the case in November 2008.

All three of these cases provide a clear example of how Facebook's and MySpace's practice of self-regulation have been ineffective and unreliable. The question then becomes whether the government should abandon this policy of self-regulation and begin to hold Facebook and MySpace liable due to their claimed ownership of defamatory content, and the necessity to protect children. Without enforcing it personally, or specifically mandating guidelines for Facebook and MySpace, the government essentially permits the existence of a medium that has the potential to become a safe-haven for sexual predators and the circulation of defamatory comments.

VII. Facebook's & MySpace's connection to discriminating employment practices

The limited amount of regulation on websites such as MySpace and Facebook has also led to a disturbing trend in the workplace. Both have displayed an inability to keep information that is thought to be private, out of the hands of current or potential employers. The damaging effects this can have on one's career was made clearly evident in *Barrow County School District v. Payne*.[39] There, Ashley Payne was a Barrow County schoolteacher who, in August 2009, was forced to resign from her job. Ms. Payne alleges that she was asked to resign after photos from a recent vacation in Europe surfaced on Facebook. These photos reportedly show Ms. Payne holding wine and beer. Below the photo is a posting that states she was "headed out to play Crazy Bitch Bingo." The school contends that it was forced to ask for Ms. Payne's resignation after a parent called the school complaining about the content. However, Ms. Payne asserts that she was not "Facebook friends" with any of her students and had enabled all proper privacy settings on her profile. Contending such, Ms. Payne has filed a lawsuit against the school district. As of this writing, the trial is forthcoming.

35 United States v. Lori Drew, No. CR 08-0582-GW, http://www.scribd.com/doc/23406419.

36 Congress, 1st Session, H.R. 1966, (April 2, 2009), http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1966.

37 *Doe v. MySpace*, 528 F. 3d 413 (5th Cir. 2008).

38 Green v. America Online (AOL), 318 F. 3d 465 – 2003.

39 "Barrow County School District v. Payne." *Citizen Media Law Project*. Berkman Center for Internet & Society, 4 Mar. 2010. Web.

The Payne case highlights a frequent trend that has become quite common in today's job markets. Employers have become especially adept at using Facebook and MySpace to screen job applicants and current employees. A 2006 survey conducted by researchers at the University of Dayton concluded, "Out of a pool of 5,000 employers nationwide, 40% would consider using the Facebook profile of a potential employee in making the hiring decision. Several employers even reported rescinding offers after checking out profiles on Facebook."[40] In many cases, these employers violate Facebook and MySpace's terms of service in retrieving information from a current or prospective employee's profile. For instance, "a method employers have been known to use involves the use of their current employees' Facebook accounts to search applicant's profiles in which they are in the same network, such as the same college. The employee may have reservations about probing the profiles of their younger college mates, but do so anyway for fear of repercussions from their employer due to noncompliance."[41]

To a limited extent, a recent court case, *Pietrylo v. Hillstone Restaurant*[42] challenged this common, unethical practice in a court of law. Two employees at Hillstone Restaurant decided to create a MySpace page where other fellow employees could join and express their grievances with the management. The page was protected by the password and none of the managers were invited to join. However, one manager eventually learned of the MySpace page and, after repeated attempts, convinced an employee to reveal the page's password. Shortly thereafter, the creators of the MySpace page were fired for "damaging employee morale and violating the restaurant's 'core values. '"[43] The two employees, Pietrylo and Marino filed a lawsuit against the restaurant alleging that its actions violated the Federal Stored Communications Act. In addition, both plaintiffs argued that the restaurant's actions also violated their right to privacy. The jury found that the restaurant did violate the federal Stored Communications Act, due to the fact that the restaurant compelled the employee to allow them unauthorized access to stored electronic communications. However, they also found that the plaintiffs had no reasonable expectation of privacy within the MySpace group. The jury reached this conclusion by following the third party doctrine, which states, "Knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information."[44] This case illustrates how the unethical practice of coercing an employee to reveal communication on a social networking working website is punishable in a court of law. Yet, this can only occur if the website is protected by a password and stored communication is being sought. Unfortunately, Facebook and MySpace profiles do not fall under the category of stored communication. Thus, limiting the employer's responsibility in coercing a fellow employee to allow him or her to view a current or potential employee's profile and bypass privacy settings.

In addition, "a [second] means of accessing Facebook profiles and by far the most invasive is to hack into the Facebook database. This may not be such a hard task for many tech-savvy IT employees at most companies. By this means the company would have access to any profile they wish."[45] The ease with which IT employees can hack into information stored on Facebook is further highlighted by the actions of the two M.I.T. students previously described in this comment. If two undergraduate students were able to access over 70,000 profiles using a program they designed, it is not unreasonable to suggest that it is not difficult for a company's IT professionals to easily find ways to bypass Facebook and MySpace's privacy controls.

VIII. Application of tort law

In his comment, *A Social Networks Theory of Privacy*[46]*,* law professor Jacob Strahilevit contends

40 C. Wiley, "Facing the Consequences of Facebook." University of Dayton. 22 Nov. 2006. 4 Mar. 2007, http://www.udnews.org/2006/11/facing_the_cons.html.

41 Engler, Peter, and Peter Tanoury. *Employers Use of Facebook in Recruiting*. Publication. Ethica Publishing. Web.

42 Pietrylo v. Hillstone Restaurant. LexisNexis. United States District Court District of New Jersey. 24 July 2008. Web.

43 Pietrylo v. Hillstone Restaurant, United States District Court District of New Jersey.

44 Pietrylo v. Hillstone Restaurant, United States District Court District of New Jersey.

45 Engler and Tanoury, *Employers Use of Facebook in Recruiting.*

46 Strahilevitz, Lior J. "A Social Networks Theory of Privacy." *The University of Chicago Law Review* 72.3: 919-88. *JSTOR*. Web. Summer 2005.

that understanding social networks will aid the courts in applying a more balanced standard of a reasonable expectation of privacy. Strahilevit agrees that state and appellate courts have been inconsistent in making this determination. "Jurisdictions cannot agree on a framework for resolving these kinds of cases. Hence, Georgia law holds that disclosing sensitive information to dozens of people, and perhaps even tens of thousands of strangers, does not necessarily render information 'public' for the purposes of the public disclosure of private facts tort, but Ohio law governing the same tort holds that a plaintiff's decision to share sensitive information with four coworkers eviscerates her expectation of privacy in that information."[47]

The key to resolving this type of discrepancy is to accept "the fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[48] According to Strahilevit, "tort law can thus function as a form of social insurance: protecting those people who engaged in socially desirable sharing of personal information, but who had the misfortune to see those personal details disseminated to the general public without their consent."[49] In his analysis, Strahilevit proposes that a reasonable expectation of privacy can be determined based on "the possibility that the information will be disseminated to a number of people that exceeds the size of his social network."[50] On Facebook and MySpace, privacy features are often used to restrict access to a specific group of people. Therefore, they are an appropriate indication of with whom the individual would like his information to be shared, and the extent to which he would prefer it to be spread. In accordance with this assertion, any unauthorized access by an outside party to bypass a person's privacy settings would constitute a violation of their reasonable expectation of privacy. Strahilevit's proposal conforms to the research conducted by Boyd and Cambridge University's Computing Laboratory concluding that many users incorrectly believe that only select friends and family can access their information. Therefore, Strahilevit's solution can go a long way in resolving instances of cyberbullying, defamation, child predation, and employee discrimination on Facebook and MySpace. Although Strahilevit offers an effective resolution to many of the problems plaguing social networking websites such as Facebook and MySpace, it is unreasonable to expect a reinterpretation of privacy law to come from the Judicial Branch. Rather, it is the legislature that must become the innovator of new laws that govern privacy through this newborn medium. In doing so, they should heed the advice of scholars such as Strahilevit, and establish a system that clearly outlines how social networks are used to determine a person's reasonable expectation of privacy.

IX. Proposed resolution

The argument furthered in this comment places emphasis on the need to correct privacy concerns facing the users of social networking websites such as MySpace and Facebook. It is evident that free market self-regulation of social networking websites denies individuals the privacy protection they deserve. As shown earlier, it is counter-intuitive for social networking websites to protect one's privacy because it adversely affects financial gain provided by the business of advertisers. Additionally, protecting social networking websites from any sort of regulatory responsibility through the application of Section 230 of the CDA, has produced multiple negative consequences including the emergence of "cyberbullying" and concerns over the potential for child molestation and employee discrimination.

Congress should take decisive action to combat these growing problems. One such solution may involve the passing of legislation that redefines a "reasonable expectation of privacy" on social networking websites. A more appropriate way to view privacy on social networking websites is advanced by J.D. candidate Matthew Hodge. In his comment, Hodge provides an analogy that accurately depicts how social networking websites should be regarded in light of privacy controls. By relating an individual's Facebook or MySpace account to a safety deposit box Hodge asserts:

> In each case, a person rents a small area in a public facility to store effects or information. The vendors of these areas hold them out to be private, by giving the purchaser a tangible key, or in the case of cyberspace, through a password. In both the case of the safety deposit

47 Strahilevitz, "A Social Networks Theory of Privacy" 921.

48 Strahilevitz, "A Social Networks Theory of Privacy" 923.

49 Strahilevitz, "A Social Networks Theory of Privacy" 927.

50 Strahilevitz, "A Social Networks Theory of Privacy" 974.

> box and storage area, the vendor/owner may have a legitimate business purpose to have access to the area, but it would not be one which a person would reasonably expect to occur. In both situations, this information, much like the profile with the protection of the extra settings, could be considered to be not in open view, and therefore, be the equivalent of a 'closed, opaque container.[51]

Congress should take Mr. Hodge's assertion into consideration when passing several new Acts that would protect the privacy of personal information on social networking websites. After placing these Acts in effect, in order to ensure that this new perception of social networking privacy is respected, a regulatory agency should be installed to police the misuse of these websites. This agency would behave similarly to the FCC, which was similarly created in large part to keep up with the regulation of emerging technology. The United States can follow the lead of nations such as Australia[52] and Canada[53], which have already established an Office of the Privacy Commissioner. This independent regulatory agency is obligated to "Determine how public bodies may collect, use and disclose personal information" and "set out how private organizations (including businesses, charities, associations and labour organizations) may collect, use and disclose personal information."[54] In fact, the Canadian office has already filed a case against Facebook that outlines its various privacy infractions.[55]

This comment has examined privacy on social networking websites largely from a legal perspective because it draws attention to important privacy concerns that require further clarification and interpretation. Historically, it typically takes an extended period of time for the law to catch up with new technology. Yet, the extraordinarily rapid growth of social networking websites such as Facebook and MySpace emphasize the perception that time is of the essence. Commonly, important legal issues are discussed in the lower courts extensively before the Supreme Court deems it necessary to provide further legal clarification. In this particular instance, however, an effective solution must swiftly come from the legislature. It is not hard to conceive that the current Supreme Court will have difficulty understanding the innovative technological capabilities of social networking on the Internet. The average age of the current Supreme Court is 68 years of age and on several occasions Justices have showcased their inability to stay up-to-date with current technology. This became especially apparent during oral arguments conducted on April 19th, 2010 for a case concerning text messaging.[56] At one point Chief Justice Roberts asked what the difference was "between email and a pager?"[57] Shortly thereafter, Justice Anthony Kennedy inquired as to what occurs when an incoming text arrives at a cell phone just as another is being sent. "Does it say: 'Your call is important to us, and we will get back to you?"[58] At one point, Justice Scalia even asked whether texts are printed out in "hard copy."[59] The struggles the Supreme Court had in understanding the technological functions of cell phones highlights that it is unlikely the Court will understand the significance of addressing privacy on social networking websites in a prompt manner.

The Internet is evolving at a breathtaking pace. Its advancement has opened up new doorways through which the exchange of information can now flow. In deciding to create a profile on a social networking website such as Facebook or MySpace, an individual makes a conscious decision to share their personal information with others. However, this same individual does not expect this information to be guaranteed virtually no protection. It is improper to assert that privacy is rendered impotent the instant one establishes an account. Despite the difference in medium, citizens still deserve a right to certain protections. It is the duty of

51 Hodge, "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com" 119.

52 "Privacy Law." *Australian Government - Office of the Privacy Minister*. Web. <http://www.privacy.gov.au/>.

53 "About Us." *Office of the Privacy Commissioner of Canada*. Web. <http://www.priv.gc.ca/index_e.cfm>.

54 *Office of the Privacy Commissioner of Canada*.

55 McNish, Jacquie. "Jennifer Stoddart Blazes a Global Trail for Privacy Protection." *Globe and Mail*. 27 Apr. 2010. Web. <http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/jennifer-stoddart-blazes-a-global-trail-for-privacy-protection/article1548740/>.

56 Frauenfelder, Mark. "Supreme Court Justices Ask Important Questions About Text Messaging and Email." *Boing Boing*. Happy Mutants LLC, 21 Apr. 2010. Web. <http://www.boingboing.net/2010/04/21/supreme-court-justic.html>.

57 Frauenfelder, "Supreme Court Justices Ask Important Questions About Text Messaging and Email."

58 Frauenfelder, "Supreme Court Justices Ask Important Questions About Text Messaging and Email."

59 Frauenfelder, "Supreme Court Justices Ask Important Questions About Text Messaging and Email."

the U.S. government to ensure that these rights and liberties are protected even in the advent of technological development. Action must be taken to resolve the problems facing millions. If not, privacy in cyberspace runs the risk of becoming virtually extinct.

Acknowledgments

This author is thankful to Dr. Naeemah Clark at Elon University for her supervision and advice, without which the article could not be published. The author also appreciates the numerous reviewers who have helped revise this article, particularly Matthew Bova, a J.D. candidate at George Washington Law School, whose revisions and advice are greatly valued.