ARTICLES

THE PRIVACY IMPLICATIONS OF DIGITAL PRESERVATION: SOCIAL MEDIA ARCHIVES AND THE SOCIAL NETWORKS THEORY OF PRIVACY

JASMINE MCNEALY*

Our cultural heritage isn't just the books, magazines and newspapers we read, nor the movies and TV we watch or the radio we listen to. More and more of our culture takes the form of digital media—and more and more of that is what we create, not just what we consume.[1]

This assertion by Dan Gillmor, director of the Knight Center for Digital Media Entrepreneurship at Arizona State University, identifies the state of culture in this age. Advances in Internet communication have created what some call "digital culture,"[2] or digital heritage,[3] as expressed in blogs, virtual worlds, social network sites and other online media. Martin Deuze goes further to call digital culture an "emerging value system and set of expectations."[4] This culture, according to some, is "so deeply embedded in everyday life that [it] disappear[s]" so

* Assistant Professor, S.I. Newhouse School of Public Communications, Syracuse University, J.D., Ph.D University of Florida.

[1] Dan Gillmor, *Archiving Ourselves,* SALON.COM, Nov. 5, 2010, http://www.salon.com/2010/11/05/archiving_ourselves.

[2] Marcelo Dascal, *Digital Culture: Pragmatic and Philosophical Challenges*, 53 DIOGENES 23 (2006).

[3] Yola de Lusenet, *Tending the Garden or Harvesting the Fields: Digital Preservation and the UNESCO Charter on the Preservation of the Digital Heritage,* 56 LIBR. TRENDS 164, 169 (2007) ("[I]n order to be universally applicable the definition of digital heritage refers both to information products and cultural works, which makes for quite a mixed bag of materials that originate in very different worlds.").

[4] Mark Deuze, *Participation, Remediation, Bricolage: Considering Principal Components of a Digital Culture*, 22 THE INFO. SOC'Y 63 (2006).

as not to be noticeable.[5] Because of this "our constant engagement and disengagement in a wide variety of social networks and the lived experience in a global network society should be seen as the discernible artifacts, activities, and arrangements characterizing 'new media.' "[6] Like the artifacts and activities of offline cultures, which are studied and theorized, digital culture, too, serves as a fertile field for study and exploration. Like offline cultures, also, the artifacts and activities of digital culture must be preserved. "The emergence of the e-culture of blogs, podcasts, digital photography, webcams, gaming, mobile phones, Flickr, and MySpace, calls for radically new directions in preservation."[7]

Enter: the memory institutions. Memory institutions are those that preserve, collect, store and display cultural and historic artifacts; "memory institutions are for a large part engaged in collecting cultural products of our own time as part of their preservation responsibilities."[8] These organizations include libraries, archives, museums and other repositories of history.[9] Such institutions are the leaders in preserving digital culture. Since before 1996, when a working group was created to study digital preservation, there has been a movement advocating the preservation of information that is "born digital."[10] "The purpose of preservation is to protect information of enduring value for access to present and future generations."[11] If digital preservation can be defined, then, as the protection of information for future generations, those institutions that have taken on the task of preservation can be said to have "responsible custody" of the information.[12] This re-

---

[5] *Id.* at 64 (citing Byron Reeves & Clifford Nass, The Media Equation: How People Treat Computers, Televisions, and New Media Like Real People and Places (1996)); *see also* Robert Pappar, Micheal Holmes, & Mark Popovich, *Middletown Media Studies*, 1 The Int'l Digital Media & Arts Ass'n J. 1, 5 (2004).

[6] Deuze, *supra* note 4, at 65.

[7] de Lusenet, *supra* note 3, at 168.

[8] *Id.* at 170.

[9] *See* Amy Friedlander, *The National Digital Information Infrastructure Preservation Program: Expectations, Realities, Choices and Progress to Date,* D-Lib Mag., Apr. 2002, http://www.dlib.org/dlib/april02/friedlander/04friedlander.html.

[10] *Id.; see also* John R. Garrett, *Task Force on Archiving Digital Information*, D-Lib. Mag., Sept. 1995, http://www.dlib.org/dlib/september95/09garrett.html.

[11] Margaret Hedstrom, *Digital Preservation: A Time Bomb for Digital Libraries*, 31 Computers & the Human. 189 (1997) (citing Paul Conway, *Archival Preservation Practice in a Nationwide Context,* 53 Am. Archivist 204, 206 (1990)).

[12] Paul Conway, *Preservation in the Age of Google: Digitization, Digital Preservation, and Dilemmas*, 80 Libr. Q. 61, 64 (2010) (citing Pelham Barr, *Book Conservation and University Library Administration*, 7 C. & Res. Libr. 214, 218 (1946)).

quires that organizations acquire, maintain and provide access to these records.[13]

The global importance of preserving digital information is demonstrated by UNESCO's adoption of the Charter on the Preservation of Digital Heritage in 2003.[14] The Charter was created in response to concern that "digital materials (primarily those digitally born) will become inaccessible in the near future" without proactive steps taken to preserve them.[15] The Charter also emphasizes the necessity for changes in the way archival institutions go about their preservation activities, calling for attitudinal changes related to digital preservation that correspond with advances in preservation technology.[16] The Charter also recognizes the need for legislation and for the "coordination and sharing of tasks and responsibilities" in order for digital preservation to be successful.[17]

One such initiative aimed at preserving digital information for future generations is the National Digital Information Infrastructure Preservation Program (NDIIPP), established by Congress through the Library of Congress (LOC) in December 2000.[18] By law, the LOC is to collaborate with other organizations to create a plan for preserving digital information.[19] Congress allocated $100 million in funding for the program to be released in stages.[20] The LOC began work on the plan by asking for feedback from those with whom digital preservation is concerned—federal agencies, research institutions, businesses, libraries, and educational institutions[21]—and produced a report in

---

[13] *See id.* at 65 (emphasizing that digital preservation requires "the acquisition, ongoing maintenance, periodic transformation, and persistent delivery of digital assets").

[14] United Nations Educational, Scientific and Cultural Organization, Charter on the Preservation of the Digital Heritage (Oct. 17, 2003), http://portal.unesco.org/en/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html; *see also* de Lusenet, *supra* note 3, at 164.

[15] de Lusenet, *supra* note 3, at 164-65.

[16] *Id.* at 165.

[17] *Id.* at 166.

[18] Library of Congress, *NDIIPP Program Background*, http://www.digitalpreservation.gov/about/background.html (last visited Feb.13, 2011).

[19] de Lusenet, *supra* note 3, at 166; *see also* Friedlander, *supra* note 9.

[20] Friedlander, *supra* note 9.

[21] *Id.* (noting that "a broad-based Advisory Board, consisting of representatives from other federal agencies, research libraries, private foundations, and industry, was organized").

2002.[22] In 2010, the NDIIPP celebrated ten years of preservation and research work.[23]

Although the ability to preserve digital information expressed in new media may be beneficial for future generations to research, issues separate from how and what to preserve have arisen. For example, the privacy implications of allowing strangers, be they researchers or not, to view aggregated communications by the many users of an online social network deserve some scrutiny. Under traditional privacy law, one could argue, for instance, that Internet users have no expectation that the information that they disclose while using a social networking site (SNS) would remain private. But new media and methods of communication may require rethinking what information is protected as private. Although not specifically analyzing online social media, in his article, *A Social Networks Theory of Privacy*, Lior Jacob Strahilevitz argued that in deciding privacy cases related to intrusion or public disclosure of private facts, "the law should focus on . . . what extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others."[24] The question of whether social media users that allow their communications to be viewed by the public are aware or realize that their communications are being preserved, and are now aggregated and available for viewing at the LOC, may provide an illustration of Strahilevitz's theory with respect to online social networks.

This paper seeks to analyze whether SNS users can claim a right to privacy with respect to their online communications. To do so, this paper will examine the privacy implications of the LOC Twitter archive in light of Strahilevitz's social network theory of privacy. First, this article briefly discusses the LOC Twitter archive. Next, this article explores the online networking phenomenon and the privacy implications associated with social media. Third, this article examines privacy, in particular Strahilevitz's social networks theory of privacy. Part four analyzes whether a challenge to the LOC Twitter archive based on a theory of invasion of privacy by public disclosure of private facts or intrusion would succeed under the social network theory of

---

[22] *See* Library of Congress, Preserving Our Heritage: Plan for the National Digital Information Infrastructure and Preservation Program (Oct. 2002), *available at* http://www.digitalpreservation.gov/documents/ndiipp_plan.pdf.

[23] Laura E. Campbell & Beth Bulabahn, Digital Preservation: The Twitter Archives and NDIIPP 4 (2010), http://www.ifs.tuwien.ac.at/dp/ipres2010/papers/campbell-27.pdf.

[24] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919 (2005).

privacy. This article concludes with considerations for digital archives in relation to protecting personal privacy.

I. The Twitter Archive

In April 2010, the LOC announced that Twitter, the social networking website that allows users to send and receive short messages of up to 140 characters, was donating its digital archive of tweets. This archive, composed of billions of messages, includes the first ever tweet from Twitter co-founder Jack Dorsey, and President Barack Obama's tweet after winning the 2008 presidential election.[25] The Twitter archive will be a part of the LOC's leadership effort in regard to the congressionally mandated NDIIPP, which seeks to preserve digital content for use in the future.[26]

In announcing the new archive, both the LOC and Twitter made sure to emphasize that only "public tweets" would be a part of the collection. According to Twitter, only a small percentage of the upwards of 55 million tweets sent per day are designated protected. Those tweets that are protected will not be a part of the archive.[27] Further, archived tweets will be subject to a six-month release delay, after which the messages will be available for internal library use, research, preservation or public display.[28] In spite of restricting the archive to public tweets and delaying the release of the tweets to the LOC, a question arises as to whether the privacy of Twitter users is being adequately protected. Do Twitter users expect that their messages will be preserved, possibly into perpetuity? Do they expect that people who do not follow them will be able to read and copy their messages?

The creation of the Twitter archive, complete with its interesting and historic communications, perhaps represents the focus of digital preservation: conserving information for future generations. The necessity of this kind of information conservation has been touted by all manner of social science scholars. Noted legal scholar Professor Diane Zimmerman, for instance, laments that current law actually stifles the

---

[25] *See* Twitter Blog, Tweet Preservation, Apr. 14, 2010, http://blog.twitter.com/2010/04/tweet-preservation.html; *see also* The Library of Congress, Twitter Donates Entire Tweet Archive to Library of Congress, http://www.loc.gov/today/pr/2010/10-081.html.

[26] *See NDIIPP Background*, *supra* note 18.

[27] *See* Twitter Blog, *supra* note 25 (noting that only a tiny percentage of accounts are protected).

[28] *Id.*

ability to "save culture," which she concludes is the aim of digital preservation measures.[29] Certainly the advances in online communication and the network referred to as social media are cultural phenomena to be studied by social scientists, historians, and those interested in popular culture.

The very existence of a tweet archive is interesting but not unusual. In fact, Twitter may not be the only social network that permanently archives or "memorializes" the communications of its users. At least, it is not the only site that fails to specifically state in its privacy policy that it will not preserve user information.[30] The Twitter privacy policy makes explicit that information published using its services will be made public, unless the user takes advantage of the site's privacy settings. Although the policy does state that the Twitter servers will record certain information including "IP address, browser type, the referring domain, pages visited, and search terms," as well as possibly user interactions with advertisements, and user coordinates, nowhere does the policy make clear that user tweets will be saved into perpetuity.[31] Nor does Facebook, in its privacy policy, state that user information will be recorded forever.[32] Facebook does, however, disclose that account deactivation and account deletion are two different things.[33] The site further discloses what other kind of history a profile owner can view.[34] The photo-sharing site Flickr, now owned by Yahoo!, discloses that certain information is recorded even when a user deletes his or her account, although after a specified time identifying information is removed.[35] Perhaps the most well-known Web preservation project is the Internet Archive's "Wayback Machine," available at http://www.archive.org, which records and catalogues websites, including blogs, without seeking permission from the creators.[36] All of these ex-

---

[29] Diane L. Zimmerman, *Can Our Culture Be Saved?: The Future of Digital Archiving*, 91 MINN. L. REV. 989, 990 (2006).

[30] *See* Twitter, *Twitter Privacy Policy*, http://twitter.com/privacy (last visited Oct. 23, 2010).

[31] *Id.*

[32] Facebook, *Facebook Privacy Policy,* http://www.facebook.com/policy.php (last visited Oct. 23, 2010).

[33] *Id.*

[34] Facebook, *Facebook Help Center,* http://www.facebook.com/help/?search=hist (last visited Oct. 23, 2010).

[35] Yahoo! Privacy Policy, http://info.yahoo.com/privacy/us/yahoo/datastorage/ (last visited Oct. 23, 2010).

[36] Internet Archive, *About the Internet Archive*, http://www.archive.org/about/about.php (last visited Feb. 12, 2011). Website owners may, however, opt to have their sites excluded from the Internet Archive using the same method that allows them to opt out

amples demonstrate a possibility of social networks creating digital records of profiles, communications, and other media created by their users. For its part, "[the] Twitter [archive] forms part of the historical record of communication in the twenty-first century, capturing news reports, events and social trends."[37] That the LOC is now in possession of an archive of such communications only adds to the interest that social media users may have as to the policies related to the privacy of their communications while using these websites.

II. The Social Media Explosion

Research on Internet use documents the increasing number of people accessing social media sites. According to a report by the Pew Internet & American Life Project, the number of adult Internet users that use social networking sites increased by almost 600% in four years, going from just 8% to 47% between February 2005 and September 2009.[38] Teen use of online social media has also increased, going from 55% of teen Internet users in November 2006 to 73% in September 2009.[39] These statistics demonstrate the explosion of social media usage in the United States. Perhaps the greatest indication of the growth in social media usage is demonstrated by the attraction of marketers and advertisers to the networks. In fact, social media is often touted as a way to retain and attract clients and customers.[40]

With data demonstrating an increase in social media usage, the question remains as to what, exactly, constitutes social media. According to Professor Teresa Correa, social media are digital and Internet tools that have little to do with traditional media. Instead, "it provides a mechanism for the audience to connect, communicate, and interact with each other and their mutual friends."[41] Others define social me-

---

of search engine indexing. *See* Internet Archive, Frequently Asked Questions, http://www.archive.org/about/faqs.php#2 (last visited Feb. 12, 2011).

[37] Campbell & Bulabahn, *supra* note 23, at 1.

[38] Amanda Lenhart et al., Pew Internet & American Life Project: Social Media & Mobile Internet Use Among Teens and Young Adults 17-18 (2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf.

[39] *Id.*

[40] *See, e.g.*, David Meerman Scott, The New Rules of Marketing and PR: How to Use News Releases, Blogs, Podcasting, Viral Marketing and Online Media to Reach Buyers Directly (2007).

[41] Teresa Correa, Amber W. Hinsley & Homero G. de Zúniga, *Who Interacts on the Web?: The Intersection of Users' Personality and Social Media Use*, 26 Computers in Hum. Behav. 247, 247-48 (2010).

dia more broadly than just networking sites, to include blogs, wikis, user-generated media, and forums.[42] Researchers boyd and Durbin provide a more complex three-prong definition of social media:

> We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.[43]

However broadly or narrowly defined, social media is about interaction or the ability of users to form networks and otherwise mingle with others that they know or have just met. Boyd and Ellison assert, "What makes social network sites unique is not that they allow individuals to meet strangers, but rather they enable users to articulate and make visible their social networks."[44] The majority of SNS users are not actually actively looking to meet people with whom they have not had previous contact, but instead are searching for friends or acquaintances with whom to connect.[45] The connection of users with those already in their social network is one of the norms of SNS.

A. *Social Media Norms*

Social networking websites like Facebook, Twitter, and LinkedIn require users to create profiles and input identifying information. This information may be as benign as a name or user name, or more specific information like geographic coordinates.[46] For the most part, users are able to choose what information, and the accuracy of the information, they provide. Individuals are then able to connect with "friends," both real and imagined, or "follow" others whose status updates or tweets they find interesting. Users may then send messages, chat, view user-generated media, and otherwise interact using the web-

---

[42] Andrew Schrock, *Examining Social Media Usage: Technology Clusters and Social Network Site Membership*, 14 First Monday (Jan. 5, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2242/2066.

[43] danah boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. of Computer-Mediated Comm. 210, 211 (2008).

[44] *Id.*

[45] *Id.*

[46] *See* Twitter, *Twitter Privacy Policy*, *supra* note 30.

site as a medium. Overall, users are allowed to share and consume information.[47]

Those using social networking sites also may share certain personality traits.[48] Correa, for example, found a correlation between extraversion, openness to new experiences, and emotional stability and the use of SNS.[49] Further, SNS users have been categorized by some researchers into passive users, inviters and "linkers who fully participate in the social evolution of the network."[50] Whatever the category of SNS user, individuals participating on these sites use them to strengthen already existing relationships. Professors Ellison, Steinfeld, and Lampe found that Facebook users most often search for people that they already know.[51] Lenhardt also found that teens continued to use social network sites to connect to friends.[52] Adults also primarily use social network sites to connect with friends.[53] In this way, social media are thought to build social capital through the facilitation of networking, communication, and the creation of trust between users.[54]

Like other SNS, Twitter allows users to communicate with others by posting status updates. After the creation of a profile, Twitter asks its users to answer a simple question, "What are you doing?"[55] Individuals "tweet" by answering this question in 140 characters or less. But it is not only the family, friends, and coworkers of Twitter users that may

---

[47] Lee Humphreys, Phillipa Gill & Balachander Krishnamurthy, *How Much is Too Much? Privacy issues on Twitter*, 2010 Proc. of the Int'l Comm. Ass'n Conf. 9, *available at* http://www.cs.utoronto.ca/~phillipa/papers/ica10.pdf.

[48] Correa et al., *supra* note 41, at 250; Schrock, *supra* note 42.

[49] Correa et al., *supra* note 41, at 251.

[50] Ravi Kumar, Jasmine Novak, & Andrew Tomkins, *Structure and Evolution of Online Social Networks*, 2006 Proc. of Int'l Conf. on Knowledge Discovery in Data Mining 611 (2006), *available at* http://portal.acm.org/citation.cfm?id=1150476.

[51] Nicole B. Ellison, Charles Steinfield & Cliff Lampe, *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. Computer-Mediated Comm. 1143 (2007).

[52] Lenhart et al., *supra* note 38.

[53] Amanda Lenhart, Pew Internet & Am. Life Project: Adults and Social Network Websites 2 (2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.

[54] Jon Garon, *Wiki Authorship, Social Media, and the Curatorial Audience*, 1 Harv. J. Sports & Ent. L. 95, 96-99 (2010) (defining social capital as features of social organization such as network, norms, and social trust that facilitate coordination and cooperation for mutual benefit (quoting Anita Blanchard & Tom Horan, *Virtual Communities and Social Capital*, *in* Social Dimensions of Information Technology: Issues for the New Millenium 7 (G. David Garson ed., 2000))).

[55] Twitter, http://www.twitter.com (last accessed Dec. 1, 2010).

view the tweets. Anyone may search and view published tweets, and Twitter has allowed search engines like Google and Bing to show tweets related to whatever topics for which individuals using the search engines search.[56] Although a significant proportion of tweets share information unrelated to the author, the majority of tweets include information about what the author is doing at that moment.[57]

B. *SNS Users and Information Disclosure*

The ability of the public to view unprotected tweets would usually mute any claims of invasion of privacy with respect to Twitter users. At the same time, Twitter users (and other SNS users) may have a different conception of what is private, as well as ignorance in regard to the security of the information that they post. The social science literature on SNS and privacy related topics continues to grow. Many of the studies relating to privacy and SNS have used Facebook as a platform for study. This information is relevant for an evaluation of Twitter because the ability of a Facebook user to provide status updates is similar to a tweet on Twitter. Further, Facebook and Twitter allow cross platform posting of status updates/tweets, so that posting a tweet on Twitter appears as a status update on Facebook.

Professors Gross and Acquisti investigated the Facebook-related information disclosure behavior of more than 4,000 students at Carnegie Melon University. More specifically they studied the extent to which those Facebook users disclosed personal information, finding that many users did in fact disclose personal information.[58] More than 87 percent disclosed their birthdate, 39.9 percent posted their phone number, and 50.8 percent listed their address.[59] Further, 89 percent of the profile names were thought to be likely accurate, and 80 percent of the profile images were thought to contain information useful for identifying the user.[60] The researchers concluded that the student users of Facebook appeared unconcerned about how the amount and

---

[56] *See* Michael Learmonth, *Google, Microsoft's Bing to Include Twitter in Search*, Advertising Age, Oct. 22, 2009, *available at* http://adage.com/digital/article?article_id=139838.

[57] *See* Mor Naaman, Jeffrey Boase & Chih-Hui Lai, *Is it Really About Me?: Message Content in Social Awareness Streams, in* Proc. of the 2010 ACM Conf. on Computer Supported Cooperative Work 189, 191 (2010).

[58] Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook Case)* § 3.3, *in* Proc. of the ACM Workshop on Priv. in the Electronic Soc'y (WPES) (2005).

[59] *Id.*

[60] *Id.*

type of information they posted online could affect their privacy. Young and Quan-Haase took the next step to study how students protect their privacy while using Facebook.[61] The majority of respondents in the study, 64 percent, changed their profile setting to "only friends," which allows only those people that the user has designated as a friend to view his or her profile information.[62] The researchers also found that the main reason that students would use their full and real name on their profile was to help their friends find them on the site.[63]

Lewis, Kaufman and Christakis studied the phenomena of changing user profile privacy settings.[64] In their study, only 33.2 percent of Facebook users had profiles set to private.[65] More important are the researchers' findings with respect to predictors of private behavior. Overall, Lewis et al. found that users with more friends with profiles set to private were more likely to have a private profile themselves.[66] Also, the more frequently a user changes his or her profile, the more likely he or she is to set it to private.[67] Those with private profiles also had "tastes," or designated things as their favorites, that were significantly different from those with public profiles; users with private profiles had more mainstream tastes.[68]

That an SNS user changes or fails to change his or her privacy settings may result from the user's understanding of the threats to his or her privacy. In their study of Facebook users, Debatin et al. found an association between a user's familiarity with the site's privacy settings and the use of the settings.[69] Ninety-one percent of the SNS users in Debatin's study knew about Facebook settings, and 77 percent had made their profile privacy settings more restrictive.[70] Conversely, those users unfamiliar with the settings were less likely to protect their

---

[61] *See* Alyson L. Young & Anabel Quan-Haase, *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, *in* Proc. of the Fourth Int'l Conf. on Communities & Tech. 265 (2009).

[62] *Id.* at 268.

[63] *Id.* at 269.

[64] Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. Computer-Mediated Comm. 79 (2008).

[65] *Id.* at 86.

[66] *Id.* at 87.

[67] *Id.*

[68] *Id.* at 89.

[69] Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. Computer-Mediated Comm. 83, 93 (2009).

[70] *Id.* at 93.

profiles.[71] A similar 2009 study by Tuunainen, Pitkanen and Hovi supports these findings.[72]

The disclosure of information on SNS profiles is also related to the users' risk-related attitudes and their trust in the specific SNS site. In a comparison study of whether risk-taking attitudes are related to SNS use, as well as trust and privacy measures, Fogel and Nehmad found that study participants with SNS profiles displayed higher risk-taking attitudes than those without.[73] Debatin et al. similarly found that the majority of SNS users saw the benefits of using SNS as outweighing the risks to their privacy.[74] Further, users were more likely to perceive a risk to the privacy of others than to themselves.[75]

Studies of Twitter users have found information disclosure behavior similar to those in the Facebook studies above. Krishnamurthy and Wills, for example, found that 99 percent of Twitter users kept the default privacy settings, which allowed their name, followers, location, URL and biographical information to be public.[76] Although a high proportion of Twitter users maintained the default privacy settings, in a content analysis study, Humphreys et al. found that the majority of public tweets did not contain personal information.[77] Similarly, very few of the public tweets studied included information identifying the author (.6 percent) or included the author's location as well as their proper name (.01 percent).[78] The researchers noted, however, that although the information-specific tweets may not identify the author directly, aggregation, or the collection and reading of tweets about the same person over time, could expose that person's habits.[79]

Even when Twitter users attempt to "protect" their tweets by setting their profiles to private, their communications may still be disclosed.[80] Meeder et al. investigated the leaked tweets of over five

---

[71] *Id.*

[72] *See* Virpi Kistiina Tuunainen, Olli Pitkanen & Marjaana Hovi, *Users' Awareness of Privacy on Online Social Networking Sites–Case Facebook*, *in* Bled 2009 Proc. 1 (2009).

[73] Joshua Fogel & Elham Nehmad, *Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns*, 25 Computers in Hum. Behav. 153, 159 (2009).

[74] Debatin et al., *supra* note 69, at 94.

[75] *Id.*

[76] Balachander Krishnamurthy & Craig E. Wills, *Characterizing Privacy in Online Social Networks*, *in* Proc. of the First Workshop on Online Soc. Networks 37, 39 (2008).

[77] Humphreys et al., *supra* note 47, at 15.

[78] *Id.* at 16.

[79] *Id.* at 17.

[80] See Brendan Meeder et al., *RT @IWantPrivacy: Widespread Violation of Privacy Settings in the Twitter Social Network*, IEEE Symp. on Security & Priv. 1 (2010).

million Twitter users with their profiles set to private. Their study found that 4.68 percent of users with protected accounts had at least one tweet that was "retweeted," and thereby exposed to others outside of the users' control.[81] These users may have been unaware that their tweets were retweeted because, instead of using the retweet function on Twitter, many retweeters would simply cut and paste the tweet.[82] Ninety percent of these retweets reached less than 730 users; only .4 percent reached more than 10,000.[83] However, these tweets may have contained embarrassing information about family members and friends, or information harmful to the employment or reputation of the authors.[84]

The studies detailed above demonstrate that SNS users, in particular those on Facebook and Twitter, may not be doing all that they could to protect their privacy while using SNS. This is attributable to a lack of knowledge about privacy settings as well as the perceived benefits of risk-taking behavior. This may also be attributable to the nature of SNS culture in general. Social media is based on surveillance and consumption of other people's information.[85] While allowing SNS users to connect with friends and acquaintances, this surveillance may lead to privacy disclosures that could have embarrassing and otherwise harmful results for those involved.

III. Conceptions of Privacy

The legal protection of privacy in the United States is both young and evolving. Although not specifically mentioned in the Constitution, privacy is a right thought to be protected under constitutional "penumbras" in the First, Third, Fourth, and Ninth Amendments.[86] The Fourth Amendment is most closely associated with privacy, as the U.S. Supreme Court found in its opinion in *Schmerber v. California*, which stated that the "overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[87] Fourth Amendment jurisprudence has created zones of privacy that protect from unwarranted government intrusion

---

[81] *Id.* at 6.
[82] *Id.* at 7.
[83] *Id.* at 6.
[84] *Id.* at 7-9.
[85] Humphreys et al., *supra* note 47, at 9.
[86] Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965).
[87] 384 U.S. 757, 767 (1966).

those things that an individual wants to keep private, "even in an area accessible to the public."[88]

While the Fourth Amendment is concerned with government intrusion, individuals have recourse against other private individuals for invasion of privacy in tort law. The bedrock of tort invasion of privacy in the United States is an 1890 Harvard Law Review article by future U.S. Supreme Court Justice Louis Brandeis and Samuel Warren.[89] *The Right to Privacy*, as the article was entitled, called for the recognition of a "right to be let alone."[90] Of particular interest to Warren and Brandeis was the ability of a person to be free from harassment by the press who had "overstepp[ed] in every direction the obvious bounds of propriety and of decency," filling their pages with "idle gossip."[91] Legislatures and courts began recognizing privacy torts soon after the article's publication.[92]

Professor William Prosser further delineated Warren and Brandeis' "new" tort in his 1964 *California Law Review* article.[93] In evaluating the privacy cases that had arisen after Warren and Brandeis published their article, Prosser found that "[t]he law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff."[94] These four privacy invasions he called intrusion, public disclosure of private facts, false light, and appropriation.[95] The first two invasions, intrusion and public disclosure of private facts, are most related to the discussion here.

Intrusion is the intentional and highly offensive invasion of a zone of privacy created by another individual.[96] This invasion can be physi-

---

[88] Katz v. United States, 389 U.S. 347 (1967).

[89] *See* ALPHEEUS MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946); *see also* Harry Kalven Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?,* 31 LAW & CONTEMP. PROBS. 326 (1966).

[90] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890). Warren and Brandeis were not the first to ponder the right to be let alone. The authors recognize Judge Thomas Cooley as having written about it previously. *Id.* at 195 (citing THOMAS C. COOLEY, LAW OF TORTS, 29 (2d ed. 1888)).

[91] *Id.* at 196.

[92] *See, e.g.*, 1903 N.Y. Sess. Laws 308, ch. 132, §§ 1-2 (codified as amended at N.Y. Civ. Rights Act §§ 51-52 (2009)); Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

[93] William Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

[94] *Id.* at 389.

[95] *Id.*

[96] The Restatement defines "intrusion upon seclusion" as: "One who intentionally intrudes, physically or otherwise, upon the solitude or the seclusion of another or his

cal or electronic so long as a person enters an otherwise private place or affairs that another has taken the effort to keep private.[97] The intrusion claim is often used against members of the press as a result of their newsgathering techniques. In *Dietemann v. Time, Inc.*, for example, the Ninth Circuit ruled that, in pretending to seek medical assistance in the private home of a plumber practicing faith healing, two journalists had invaded the man's privacy by intrusion by entering his home and surreptitiously taking pictures.[98]

Although one's home is a major sphere of privacy, information found in public records or observed in areas open to the public are not the subject of intrusion liability.[99] Concomitantly, the courts have recognized that certain information observable in public may provide a cause of action for intrusion. Perhaps one of the best illustrations of this is *Shulman v. Group W Productions*.[100] *Shulman* arose when a documentary film crew rode along with a medical helicopter team to a car accident where two members of the Shulman family were injured. The camera crew filmed both the rescue and the medical care on scene and within the helicopter. In addition, the flight nurse wore a microphone that recorded conversations with the injured Shulman at the scene.[101] The footage and sound were later broadcast as part of a documentary.[102] Although ruling that the plaintiff had to prove that the camera crew intruded into a private place in a manner highly offensive to a reasonable person, the California Supreme Court found that there were triable issues of fact with regard to whether the reporters invaded Shulman's privacy.[103]

Although the court concluded that the cameraman's presence at the accident scene was not intrusive, it ruled that a jury could find that Shulman had a reasonable expectation of privacy within the helicop-

---

private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[97] *See id.* cmt. b.

[98] 449 F.2d 245, 248-49 (9th Cir. 1971).

[99] *See, e.g.*, Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. Ct. App. 1970) (finding no invasion of privacy in the observation of an individual in public); Desnick v. Am. Broad. Cos., 44 F.3d 1345 (7th Cir. 1995) (finding no invasion of privacy in the hidden recording of an eye clinic by patients).

[100] 955 P.2d 469 (Cal. 1998); *see also* Rafferty v. Hartford Courant Co., 416 A.2d 1215 (Conn. Super. Ct. 1980) (holding that the plaintiff maintained a reasonable expectation of privacy even at an event held in a public park).

[101] *Shulman,* 955 P.2d at 474-75.

[102] *Id.* at 475.

[103] *Id.*

ter.[104] Shulman was also entitled to privacy in her conversations with the flight nurse at the scene, and in the information being relayed about her injuries.[105] The court ruled that a reporter's pursuit of a story did not justify an intrusion, but that offensiveness depended on the method of investigation.[106] A reasonable jury could have found that the recording of Shulman's conversations with the flight nurse and the filming of Shulman in the helicopter were offensive.[107]

The reasonable expectation of privacy idea, as alluded to by the *Shulman* court, is an objective standard to be decided by a jury.[108] This standard is evaluated based on what society would consider reasonable. The justification for this standard is "address[ing] the problem of idiosyncratic individual preferences" in relation to privacy.[109] "Some individuals may have an unusually strong desire for privacy and may make impossible demands for privacy at great variance with social practice."[110] In place of a variable standard of privacy, the courts have settled on a standard that best comports with public policy. As such, for the most part, individuals have no expectation of privacy in what they say or do in public. A rationale for finding a reasonable expectation of privacy in Shulman's conversation with the first responders while in a public place can be found in the context of the situation. Surely society would understand the need of a person in medical crisis to be able to speak openly to a health professional without fear a stranger will record what he or she discloses.[111]

Public disclosure of private facts also makes use of a similar reasonableness expectation. This category of invasion of privacy asks whether the defendant has publicized private information about the plaintiff.[112] The focus is not so much on whether or not the information is private, but whether the *publication* of the information is highly offensive to a reasonable person.[113] This highly-offensive requirement, like the reasonable-expectation requirement, takes into account socie-

---

[104] *Id.* at 490.
[105] *Id.* at 491.
[106] *Id.* at 494.
[107] *Id.*
[108] *See id.*
[109] Daniel J. Solove, Understanding Privacy 71 (2008).
[110] *Id.*
[111] The *Shulman* court makes note of this. *See Shulman*, 955 P.2d at 491-92; *see also* Doe v. New York, 15 F.3d 264 (2d Cir. 1994).
[112] Restatement (Second) of Torts § 652D.
[113] *Id.* cmt. c.

tal views of offensiveness. It is, for example, highly offensive to a reasonable person to publish a photograph of a woman whose skirt has blown up above her head in public[114] or to report that someone suffered from a rare disease.[115] At the same time, it is not highly offensive to publish a picture of a young couple kissing at a restaurant[116] or of a young woman exposing her breasts at a rock concert.[117]

In addition, the law of public disclosure of private facts requires that the private information published not be of a "legitimate public concern." The courts have broadly recognized a newsworthiness defense for the most part, basing newsworthiness upon a community standard.[118] Overwhelmingly the courts have held that information taken from public records meets the standard of a public concern, and therefore there is no invasion of privacy by publishing it.[119] Further, the public interest in certain information does not necessarily degrade over time. The classic case for this is *Sidis v. F-R Publishing Corp.*, in which the court ruled that a man who had received great media attention for his intellect as a child was still considered newsworthy over 20 years later.[120] Similarly, newsworthiness was found even after a lapse of time with respect to an allegedly abusive ex-husband who had since reformed,[121] but not with respect to a former prostitute who was tried for murder.[122]

A. Strahilevitz and A Social Networks Theory of Privacy

The general principle in both intrusion and public disclosure is that those things done in public do not receive protection against invasions of privacy. Courts in both kinds of cases have recognized, however, limited privacy—that in certain situations, individuals may still have a reasonable expectation of privacy in information that they have

---

[114] *See* Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964).

[115] *See* Barber v. Time, Inc., 159 S.W.2d 291 (Mo. 1942).

[116] *See* Gill v. Hearst Publishing Co., 253 P.2d 441 (Cal. 1953).

[117] *See* Mayhall v. Dennis Stuff, Inc., 31 Media L. Rptr. 1567 (2002).

[118] *See* Virgil v. Time, Inc., 527 F.2d 1122 (9th Cir. 1975); Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665 (Cal. Ct. App. 1984).

[119] *See, e.g*, Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975); Florida Star v. B.J.F., 491 U.S. 524 (1989).

[120] 113 F.2d 806 (2d Cir. 1940).

[121] *See* Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222 (7th Cir. 1993).

[122] *See* Melvin v. Reid, 297 P. 91 (Cal. Dist. Ct. App. 1931).

disclosed to another person or a group of people.[123] In *Sanders v. ABC, Inc.*,[124] for example, a reporter wore a hidden camera and microphone to record her daily interactions while working undercover as a telephone psychic.[125] The reporter recorded her coworker's conversations, once when he was in the aisle speaking with another coworker and a second time when he spoke directly to the reporter.[126] A *Prime-Time Live* broadcast contained excerpts from the second conversation.[127]

The California Supreme Court noted that although in California there was no intrusion unless the plaintiff proved that he or she had a reasonable expectation of privacy, this did not mean that the privacy had to be "absolute or complete."[128] "[M]ass media videotaping may constitute an intrusion even when the events and communications recorded were visible and audible to some limited set of observers at the time they occurred."[129] The court found that the idea of seclusion was relative; so even though an individual did not have an expectation of confidentiality in a conversation, the individual might have a reasonable expectation of privacy with regard to that conversation not being recorded.[130] "There are degrees and nuances to societal recognition of our expectations of privacy; the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law."[131]

The court also found that privacy, with respect to intrusion, requires an evaluation into the identity of the intruder.[132] This is so because employees might still have an expectation of privacy with respect to a "stranger" entering their workplace "despite the possibility that the conversations and interactions at issue could be witnessed by coworkers or the employer."[133] The ABC reporter was not considered an em-

---

[123] *See* K. J Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 Rutgers L. Rev. 1235 (2004); Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 Harv. J. L. & Tech. 1 (2007).

[124] 978 P.2d 67 (Cal. 1999).

[125] *Id.* at 70.

[126] *Id.*

[127] *Id.* at n.1.

[128] *Id.* at 71.

[129] *Id.* at 72. The court based this finding on its decision in *Shulman v. Group W Productions*, 955 P.2d 469 (Cal. 1998). See text accompanying notes 100-08, 111.

[130] *Sanders,* 978 P.2d at 72.

[131] *Id.*

[132] *Id.* at 73.

[133] *Id.* at 73-74.

ployee of the psychic company when she recorded the conversations of her coworkers.[134] The employee whose conversations were recorded was therefore able to prevail on his intrusion claim based on the idea of limited privacy.

Using the *Sanders* opinion as one of his examples, in his 2005 *Chicago Law Review* article, Professor Lior Strahilevitz argues that, in deciding limited privacy cases, the courts should seek assistance from social science literature, which can help explain how information flows through human social networks.[135] In privacy cases related to intrusion or public disclosure of private facts, this would mean "the law should focus on . . . what extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others."[136] According to Strahilevitz, insights from social science would provide a more objective evaluation of privacy instead of the traditional methods of evaluating what is considered private, which he deems "abstract, circular, and highly indeterminate."[137]

Strahilevitz bases his theory on the literature surrounding human social networks, in particular the literature on "network theory." Human social networks are described as "scale-free" networks, meaning they are made up of both supernodes and peripherals.[138] Peripherals have a small number of connections, whereas supernodes are able to transmit a large amount of information to a large number of others because they have a large number of connections.[139] This scale-free network is efficient in information dissemination.[140]

As a further illustration of how a scale-free network works, Strahilevitz uses the game "Six Degrees of Kevin Bacon," in which it is theorized that the actor Kevin Bacon can be connected with all of the actors who have appeared in U.S. films since 1898.[141] Bacon would be

---

[134] *Id.* at 76. When she answered the phones and gave readings, she was functioning as an employee of the telepsychic company.

[135] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 921 (2005).

[136] *Id.* at 921.

[137] *Id.*

[138] *Id.* at 948 (citing DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE 107 (2003)).

[139] *Id.*

[140] *Id.* This is assuming that the network does not become congested and the links between nodes do not disintegrate.

[141] *Id.* at 949; *see also* ALBERT-LÁSZLÒ BARABÀSI, LINKED: THE NEW SCIENCE OF NETWORKS 58-62 (2002).

considered a supernode because he has many connections to others. Those actors with few connections would be considered peripherals.[142] This is a simplistic explanation of a scale-free network; human networks and connections continue to grow and change. And even though two individuals may be separated by only a few connections, the individuals may never meet or hear about each other.[143] This is perhaps the uniqueness of scale-free networks—that although information could be disclosed to many individuals, for the most part, it is not. According to Strahilevitz, whether and how far information is disclosed depends on that information reaching a supernode; at the same time, that information reaches a supernode does not render that information public.[144]

Strahilevitz bases his assertion on the work of Mark Granovetter, a sociologist who found that human social networks are clustered.[145] The clusters are based on the strong ties created as a result of the similarities between the people in them, whether it be shared interests, jobs, or ancestors.[146] The connectedness of the people in these network clusters makes the information within the network cluster redundant, meaning that because everyone in that cluster is so strongly connected, once one person learns something, the others in the network will already know it, or will know it soon after.[147] Information gained from weak ties, or those ties that are not within the main cluster, will be new,[148] which is an advantage of weak ties.[149] But weak ties also assist in the spread of gossip.[150]

Supernodes with many weak ties to other network clusters play a significant role in the dissemination of information.[151] At the same

---

[142] Strahilevitz, *supra* note 135, at 951.

[143] *Id.* at 951-52 (citing Jeffrey Travers & Stanley Migram, *An Experimental Study of the Small World Problem*, 32 Sociometry 425, 431-33 (1969)).

[144] Strahilevitz, *supra* note 135, at 953.

[145] *Id.* at 954 (citing Mark Granovetter, *The Strength of Weak Ties: A Network Theory Revisited*, 1 Soc. Theory 201, 201-02 (1983)).

[146] Granovetter, *supra* note 145, at 204.

[147] Strahilevitz, *supra* note 135, at 955.

[148] *Id.*

[149] *Id.* According to Granovetter, weak ties lead to information about new opportunities that an individual would not have had by just relying on his strong ties. Granovetter, *supra* note 145, at 205.

[150] Strahilevitz, *supra* note 135, at 956 (citing Gabriel Weimann, *The Strength of Weak Conversational Ties in the Flow of Information and Influence*, 5 Soc. Networks 245, 254-55 (1983)).

[151] Strahilevitz, *supra* note 135, at 958.

time, the culture of a network cluster may dictate whether information is disseminated.[152] To illustrate this, Strahilevitz examines social science studies on those who are HIV-positive,[153] the flow of gossip at an all-girls school,[154] and the dissemination of a rumor about the closing of a bakery in Hong Kong.[155] Evaluating these studies, Strahilevitz found that certain groups have created a culture of nondisclosure of information to those outside of the group. So while HIV-positive individuals may disclose their status and challenges to others in their support groups, those in the support group would not, in turn, disclose this information to others.[156] Further, with respect to the school girls, gossip was transmitted most often when it was relevant to the audience or speaker.[157] Also, as information moved through a network, it tended to degrade, or be less likely to be passed on.[158]

From these studies and the previous literature, Strahilevitz identifies structural and cultural factors that courts should consider when evaluating whether an individual should expect any information that he or she has disclosed to a few others to remain private.

> Information will or will not be disseminated through a social network depending on. . .:
>
> The structure of a network
>
> - Prevalence of ties and supernodes
> - Mix of strong and weak ties
> - Proximity of disclosure to a supernode
> - Difficulty of aggregating complex information through weak ties
> - Concealment versus efficiency tradeoff in network structure
> - Extent to which technologies used by members of a social network facilitate or constrain information dissemination
>
> The cultural variables
>
> - Differentials in the willingness to disclose facts to particular groups or types

---

[152] *Id.* at 959.

[153] *See* Gene A. Shelley et al., *Who Knows Your HIV Status? What HIV+ Patients and Their Network Members Know About Each Other*, 17 Soc. Networks 189 (1995).

[154] *See* Stanley Schachter & Harvey Burdick, *A Field Experiment on Rumor Transmission and Distortion*, 50 J. Abnormal & Soc. Psychol. 363 (1955).

[155] Gina Lai & Odalia Wong, *The Tie Effect on Information Dissemination: The Spread of a Commercial Rumor in Hong Kong*, 24 Soc. Networks 49 (2002).

[156] Strahilevitz, *supra* note 135, at 961-62.

[157] *Id.* at 963 (citing Schachter & Burdick, *supra* note 154, at 369).

[158] Strahilevitz, *supra* note 135, at 965.

- Presence of moral or legal constraints on disclosure
- Network participants' ability to know which information other network members are likely to deem relevant
- Propensity of certain information to degrade as it passes through a network
- Whether the information is of the type that is ordinarily transmitted through strong or weak ties[.][159]

To properly evaluate privacy using these factors, the content of the information an individual wishes to keep private also must be evaluated.[160]

B. *Strahilevitz and Online SNS*

In his article, Strahilevitz never applies these factors to online social network sites, although he does mention new technology.[161] Although scholars believe that Strahilevitz's theory provides a good middle ground between traditional privacy theory and normative theories of how privacy should be evaluated with respect to the Internet,[162] others have noted the differences between offline and online social networks.[163] Gross and Acquisti note three differences between the two kinds of networks that may make the application of Strahilevitz's theory to online networks difficult.[164] First, ties in offline networks are more diverse than the taxonomy of strong and weak connote. Online connections are decontextualized into "binary relations."[165] SNS, although allowing users to "articulate and utilize" relationships, provide no real definition of "friend."[166] Two people may both be categorized as "friends" even though the user may not have the same level of intimacy with each of them. The word "friend," therefore, loses the nuance that it has in offline relationships.[167]

Second, Gross and Acquisti assert that the number of weak ties that an individual has will increase while using SNS because the type of

---

[159] *Id.* at 970-71.

[160] *Id.* at 971.

[161] *Id.* at 968-69. Strahilevitz does mention Friendster, which was one of the first social networking sites that allowed individuals to connect with "friends" on the Web.

[162] *See* James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1196 (2009).

[163] *See* danah boyd, *Friendster and Publicly Articulated Social Networking*, *in* Conf. on Hum. Factors & Computing Sys. 1279 (2004); *see also* Gross & Acquisti, *supra* note 58, at 71.

[164] Gross & Acquisti, *supra* note 58, at 73.

[165] *Id.*

[166] boyd, *supra* note 163, at 1279-80.

[167] Gross & Acquisti, *supra* note 58, at 73.

communication popular on these sites corresponds to weak ties.[168] An SNS user's motives for "friending" someone are varied.[169] In their study of Facebook users, for example, Debatin et al. found that only slightly more than half of the people surveyed restricted their friendship to people that they actually knew.[170] Over a third accepted people that they had only heard of from friends, and ten percent were willing to accept anyone as a friend.[171]

Lastly, trust is different in online and offline networks.[172] Although the same amount of information is provided to friends of differing tie strength, trust in online networks may be "assigned differently and have different meaning than in their offline counterparts."[173] Trust is central to the use of technology,[174] but trust may actually decrease in an online social network.[175] With respect to Twitter, this may mean that there are actually two social networks at play at the same time, "a very dense one made up of followers and followees, and a sparser and simpler network of actual friends."[176]

In sum, the decontextualization of relationships that happens on SNS does not provide a complete and accurate picture of the level of intimacy and trust between users. Although users may have many friends online, many of the connections on SNS may actually be meaningless.[177] Further, SNS users may have such high numbers of connections because there is a very small cost to having such a connection online in comparison to offline.[178] But the lack of differentiation between connections neglects the fact that an SNS user may want to dis-

---

[168] *Id.*

[169] boyd, *supra* note 163, at 1280. Boyd notes two rationales often used for "friending" another person: political reasons and wanting to see a larger portion of the whole social network.

[170] Debatin et al., *supra* note 69, at 94.

[171] *Id.*

[172] Gross & Acquisti, *supra* note 58, at 73.

[173] *Id.*

[174] *See* boyd, *supra* note 163, at 1280.

[175] Gross & Acquisti, *supra* note 58, at 73.

[176] Bernardo A. Huberman, Daniel M. Romero & Fang Wu, *Social Networks That Matter: Twitter Under the Microscope*, 14 First Monday 1 (2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2317/2063. Huberman et al. used a broad definition of "friend," which included another user to whom there were two or more posts directed.

[177] *Id.* Huberman et al. found that most of the links between users on Twitter were unnecessary with respect to interaction between the two parties.

[178] *Id.*

close information to some connections and not others; this leads to problems with respect to privacy.[179]

IV. Evaluating the Twitter Archive in Light of the Social Theory of Privacy Networks

Using the social network theory to decide privacy cases related to the use of online social networks will be a highly fact-specific endeavor. As such, it is perhaps instructional to examine how the courts have decided a privacy case concerning social media, and then evaluate how the court's decision may have been different after incorporating the social network theory of privacy. To date there have been no invasion of privacy by intrusion or publication-of-private-facts cases reported in connection with Twitter. However, a recent case involving Myspace, another popular SNS, provides an adequate situation for examination.

Moreno v. Hanford Sentinel, Inc., arose as a result of a local newspaper publishing a post that a college school student made on her Myspace page.[180] Cynthia Moreno wrote and posted "An Ode to Coalinga," a rant about how much she hated her hometown, as well as negative comments about the city and some of the people who live there.[181] Although Moreno removed the post only six days after publishing it, the principal at the high school that her sister attended obtained a copy and passed it along to the local paper, which published it in the "letters to the editor" section along with Moreno's full name.[182] This resulted in death threats against Moreno and her family, forcing the family to move out of town and to close their twenty-year-old business.[183]

The California appellate court affirmed the trial court's ruling that Moreno failed to prove invasion of privacy. The court asserted that in posting the ode on her Myspace profile, Moreno engaged in an "affirmative act [that] made her article available to any person with a computer and thus opened it to the public eye."[184] Moreno's publica-

---

[179] *See* Ronald Leenes, *Context is Everything: Sociality and Privacy in Online Social Network Sites*, *in* Priv. & Identity Mgmt. for Life 48, 57-58 (2010), *available at* http://ssrn.com/abstract=1706295.

[180] 172 Cal. App. 4th 1125, 1128 (2009).

[181] *Id.*

[182] *Id.*

[183] *Id.* at 1129.

[184] *Id.* at 1130.

tion of her poem on the Internet, therefore, excluded her from having any reasonable expectation of privacy in that posting.[185]

What's interesting about the court's opinion that Moreno had no reasonable expectation of privacy in her Myspace posting is its treatment of *Sanders v. ABC*.[186] Although the *Moreno* court noted that an individual does not automatically relinquish any expectation of privacy by disclosing his or her information to a few people, the court quickly dispensed with any argument that Moreno could have a limited expectation of privacy in her Myspace posting solely based on her use of the Internet.[187] The court dismissed the claim that Moreno expected her audience to be small, and called the fact that she removed the posting after only six days "of no consequence."[188] Further, the court ruled that Moreno had no expectation of privacy in her name because, although she used only her first name in connection to her SNS page, her identity was ascertainable from her page and she posted a photo of herself on her profile.[189]

Perhaps this is where the California appellate court erred. Recall the studies of student information disclosure on Facebook, a Myspace competitor. Studies by both Gross & Acquisti and Young & Quan-Haase demonstrate that the information that Moreno disclosed on her Myspace profile may be in the norm for social media. Consider that Gross & Acquisti found that over three-fourths of the college students in their study posted their profile pictures.[190] Young & Quan-Hasse found that students would often use their full names in connection with their profiles to facilitate connections with friends.[191] This makes what Moreno did, in regards to posting her photo and her identifying information on her Myspace profile, ordinary behavior.

The fact that anyone on the Internet had the potential to access Moreno's profile, and subsequently her posts, does not mean that everyone did in fact access her post. More to the point, although the court opinion makes no mention of how many friends she had on Myspace, this may have proven relevant to its decision. A review of the literature surrounding information disclosure on social media may

---

[185] *Id.*
[186] 978 P.2d at 67 (Cal. 1999).
[187] *Moreno*, 172 Cal. App. 4th at 1130.
[188] *Id.*
[189] *Id.* at 1130-31.
[190] Gross & Acquisti, *supra* note 58, at 76.
[191] Young & Quan-Haase, *supra* note 61, at 269.

have provided the court with context about the environment in which Moreno made her disclosure. Further, the *Moreno* court did not take into consideration that, in expressing her hatred of her hometown on her profile, Moreno was talking to her friends or people with whom she could commiserate. Recall that many scholars have found that people, both young and old, use SNS to connect with people that they already know.[192] And although friendship on SNS is a complex issue, considering the literature, one could infer that Moreno was talking to her friends when she posted the poem.

In addition, using the *Sanders* decision one could infer that an individual does not have to disclose information only to his or her closest friends. The plaintiff in *Sanders* discussed private matters with his co-workers, who may or may not have been his actual friends, and was still thought to have a reasonable expectation that they would not disclose his information. With respect to SNS, this should mean that it does not matter how close an individual is with the people who can view his or her postings; he or she may still have an expectation that they will not disclose that information to others. For Moreno, this may mean that it was reasonable for her not to expect her ode to go any farther than the computer screens of her online friends. She certainly should not have expected it to be printed in the local paper.

The above analysis demonstrates how the *Moreno* decision may have come out if that court would have used the social network theory of privacy to analyze the facts. A similar conclusion could be made with respect to a Twitter user having a reasonable expectation that her tweets would not be aggregated and made available for viewing by a government institution. Consider, again, the literature with respect to information disclosure and Twitter. Although restrictions can be placed as to who can view an individual's profile page, most Twitter users do not change the default privacy settings.[193] Further, and perhaps more ominous, is the fact that although much of the information disclosed on Twitter does not directly identify the author, the aggregation of this information could expose a person's habits.[194]

---

[192] *See* Correa et al., *supra* note 41 at 248; Ellison et al., *supra* note 51; boyd & Ellison, *supra* note 43; LENHART ET AL., *supra* note 38, at 2.

[193] Krishnamurthy & Wills, *supra* note 76, at 39.

[194] Humphreys et al., *supra* note 47, at 17.

The aggregation of information about a person in the offline world has sometimes been considered intrusive.[195] Indeed, scholars have noted the dangers of private information aggregation.[196] Information aggregation can lead to erroneous judgments about the subject of the information because aggregation removes the context from which the information originated.[197] With respect to Twitter, this means that the aggregated tweets that will now appear in the LOC's archive will be divorced from the "conversation" in which they first appeared, and could be interpreted as meaning or conveying a message that the author did not contemplate.

V. Conclusion

So what does this mean for the LOC in creating an archive of born-digital information for the use of future generations? The answer may not be so simple as the *Moreno* court's maxim that if you publish it on the Internet, you have no expectation of privacy. As demonstrated by the literature detailed above, online social networks and the culture surrounding them is complex. Therefore, the information surrounding disclosure and privacy in these networks will, likewise, be complex. Yet the literature on the use of privacy controls and social media is important to understanding privacy on SNS, just as Strahilevitz demonstrated that the sociological data on how individuals disclose information is important to understanding when further revelation of that information should be considered a breach of privacy.

This social network theory of privacy provides a more nuanced way of conceptualizing what should be considered private. Traditional privacy theory generalizes information into two categories: things that are private, and things that are public. Although recognizing that a person may still retain a limited expectation of privacy in some information that is disclosed to a few others, limited privacy has not been applied to online social networks. It would be beneficial for both online and offline privacy situations for courts to have a better understanding of the way information moves through these networks, the kinds of information disclosure that are normal, the kinds of ties that

---

[195] *See, e.g.*, Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. Ct. App. 1970) (Brietel, J., concurring); Summers v. Bailey, 55 F.3d 1564 (11th Cir. 1995).

[196] *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119, 152 (2004); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosures*, 53 Duke L.J. 967 (2003).

[197] *See* Nissenbaum, *supra* note 196; Solove, *supra* note 196.

individuals have, and the categories of individuals—whether supernodes or peripherals.

Before making the Twitter archive accessible, if only to researchers, the LOC, as a supernode, has the ability to decide what information should be disclosed. Of course the LOC could use the traditional measure of what is considered public information—that is, in general, anything that the public is able to view. But the LOC could also consider the literature on privacy and online social networks. This may mean considering the statistics about what kind of information SNS users allow to remain public. Or the solution could be as simple as asking SNS users whether they would like their information included in the archive.[198] By obtaining permission from the user, the LOC would dispense with a lawsuit before it happens.

---

[198] At first glance this may seem prohibitive because of cost. But the LOC could collaborate with Twitter to, for example, place a link to a permission page on the start page of every user's profile or send an email linking to a permission page through the Twitter system as when a user is notified that a new person is following him or her.