PRIVACY FOR SOCIAL NETWORKING

*Connie Davis Powell**

I. INTRODUCTION

Social networks[1] have changed the manner in which members of society interact with one another. Users of the technology are able to provide up-to-date commentary about the details of their daily activity from their smartphones. While social networks provide access to unprecedented amounts of information and a new medium of communication, the technology has challenged the application of privacy laws, creating a major conflict in the law and society's views of privacy. In 1890, Warren and Brandeis penned one of the most influential law journal articles, *The Right to Privacy*,[2] out of mere frustration with new technology and journalists' increasing ability to intrude upon the private lives of individuals.[3] Warren and Brandeis wrote:

> THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[4]

This Article builds upon the article *"You Already Have Zero Privacy. Get Over It!"*[5] *Would Warren and Brandeis Argue for Privacy for Social Networking?*,[6] which was written out of exasperation with the ever-changing

---

* Connie Davis Powell is an Associate Professor of Law at Baylor University School of Law. She earned a BA in Biology from the University of North Carolina at Chapel Hill and a JD from Indiana University School of Law-Bloomington.

1. Social networks are most adequately defined by Tal Z. Zarsky in *Law and Online Social Networks: Mapping the Challenges and Promises of User-Generated Information Flows*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 741, 746–57 (2008).

2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. *See id.* at 206–07.

4. *Id.* at 193.

5. Scott McNealy, CEO of Sun Microsystems, has been attributed to this quote. Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's in It for You?*, BLOOMBERG BUSINESSWEEK, Apr. 5, 1999, at 84, *available at* http://www.businessweek.com/1999/99_14/b3623028.htm.

6. Connie Davis Powell, *"You Already Have Zero Privacy. Get Over It!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146 (2011).

privacy policies of social network sites.[7] In that article, Warren and Brandeis' arguments in *The Right to Privacy*[8] were applied to advocate for a privacy tort for social networks.[9] This Article seeks to clearly establish this privacy tort and evaluates its pros and cons and the policy considerations with creating tort liability for social networks. Part II discusses the emergence of social networks as a major communication medium. Part III explores the changing attitudes toward privacy, the transformed expectation of privacy of users of social network sites and how such expectations have been derived. Part IV provides a synopsis of the current call for regulations of social media and why current proposals are inadequate to protect user privacy. Finally, Part V provides the basis for expanding three of the four privacy torts to encompass the changing attitudes towards privacy.

II. THE RISE OF SOCIAL NETWORKS

Over the last decade, technology has exploded to create new modes of communication. Notably, the use of social network sites for communication has grown in popularity.[10] Social networks have been generally defined by social network researchers Nicole Ellison and danah m. boyd, 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.[11]

Social networks include web-based sites such as Facebook, Google Buzz, MySpace, LinkedIn, and Twitter, which allow users to register with the service, create a profile, view and post content on other users' pages, send messages, establish and join social groups, invite members to events, and search for other members using the same network and connect with those members.[12] The success of social networks can be attributed to the users' willingness to share their information.[13] The statistics are staggering.

---

7. *Id.* at 147.
8. *See generally* Warren & Brandeis, *supra* note 2.
9. *Id.* at 178.
10. A Pew Institute research poll shows that two thirds of adults online are members of a social network site and have favorable opinions regarding its utility. Mary Madden & Kathryn Zickuhr, *65% of Online Adults Use Social Networking Sites*, PEW INTERNET & AMERICAN LIFE PROJECT, 2 (Aug. 26, 2011), http://pewinternet.org/~/media//Files/Reports/2011/PIP-SNS-Update-2011.pdf.
11. danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 11 (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.
12. *See id.*
13. *Id.*

Thirty billion pieces of content are shared on Facebook each month.[14] Flickr hosts over five billion images with uploads of three thousand images every minute.[15] It is estimated that users of Twitter compose an average of 190 million Tweets per day.[16]

The advent of this new media has transformed the privacy expectations. According to Mark Zuckerberg, "[p]eople want access to all the information around them, but they also want complete control over their own information."[17] Social network sites have embraced this notion by providing privacy options to their users.[18] While social network sites have provided these options, many users are either unaware of the privacy option or do not understand how to maneuver through the complex settings.[19] As a result, much of the information posted is subject to default settings. Indeed, the use and privacy of the information posted is governed solely by the settings of the users and the overall privacy policy of the social network site.[20] Notwithstanding, users continue to post salacious photos, blog about intimate details of daily activities, forge new relationships online, and vent about bosses and colleagues online, with an expectation that the information posted will remain private and will only be viewed by those who are members of their respective social network. Users continue to maintain that privacy is a top priority, which influences their decision to join a particular social network.[21] One must ask if this belief by users of social networks is grounded in reality. The answer to this question is dependent upon how users of social network sites define their expectations of privacy online.

---

14. Jenise Uehara Henrikson, *The Growth of Social Media: An Infographic*, SEARCH ENGINE JOURNAL (Aug. 30, 2011), http://www.searchenginejournal.com/the-growth-of-social-media-an-infographic/32788/.

15. *Id.*

16. *Id.*

17. John Cassidy, *Me Media: How hanging out on the Internet became big business*, THE NEW YORKER, May 15, 2006, at 50–59, (internal quotation marks omitted), *available at* http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy.

18. *See, e.g.*, Guilbert Gates, *Facebook Privacy: A Bewildering Tangle of Options*, N.Y. TIMES, May 12, 2010, http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html (discussing the multitude of privacy option available for users of Facebook).

19. *Id.*

20. *Id.*

21. *2011 Social Networking Security and Privacy Study*, BARRACUDALABS 6 (October 12, 2011), http://www.barracudalabs.com/SNSreport.

III. USER DEFINITION OF PRIVACY

Determining the expectation of privacy for users of social networks and whether such expectation is reasonable is by no means a simple task.[22] Defining the concept of privacy has proven to be an insurmountable task. Philosophers and legal scholars alike have grappled with the concept of privacy and have struggled in their attempts to conceptualize privacy.[23] In *The Right to Privacy*, Samuel Warren and Louis Brandeis authored the first scholarly article attempting to conceptualize privacy and defined personal privacy as the "right to be let alone."[24] Concepts of privacy have continually evolved to include notions such as "(1) solitude; (2) intimacy; (3) anonymity; and (4) reserve," which is "the creation of a psychological barrier against unwanted intrusion."[25] Privacy has been defined as "the *control* we have over information about ourselves,"[26] and has been stated to be "a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."[27] While no one unified definition of privacy exists, the concept of privacy is most often defined by societal norms,[28] and such norms have viewed privacy as the right to control access to one's personal information.[29] As discussed above, users of social network sites are eager to share information on such sites but maintain a strong sense of the importance privacy plays in the information that is disclosed.[30] Users of social network sites want to maintain control over the information that is shared while using such technology.[31]

Facebook states that "[p]eople should have the freedom to decide with whom they will share their information, and to set privacy controls to protect those choices."[32] Twitter states that its "[s]ervices are primarily de-

22. Avner Levin and Patricia Sánchez Abril reported their empirical findings related to this question in *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1045 (2009).

23. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002).

24. Warren & Brandeis, *supra* note 2, at 193, 205–07.

25. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Antheneum 1967) (listing four "basic states of individual privacy").

26. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (emphasis in original).

27. ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 15 (Rowman & Littlefield 1988).

28. Levin & Sánchez Abril, *supra* note 22, at 1007–08.

29. *See, e.g.*, WESTIN, *supra* note 25; Richard Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 280 (1974).

30. *See infra* Part IV and *supra* note 21.

31. Cassidy**,** *supra* note 17, at 50–59.

32. *Facebook Principles*, FACEBOOK, http://www.facebook.com/principles.php (last visited Jan. 19, 2012).

signed to help you share information with the world[,]"[33] while cautioning its users to "[k]eep in mind that although you may consider certain information to be private, not all postings of such information may be a violation of this policy."[34] So how are the expectations of privacy set for users of social networks? They are set by privacy policies.[35]

Prior to the enactment of California's Online Privacy Protection Act of 2003,[36] websites provided little information or expectation with regard to the collection and disclosure of personal information collected online. Indeed, the preamble to the California Online Privacy Protection Act provides:

> Existing law does not regulate the security and confidentiality of consumer personal and identifying information obtained by persons and entities engaged in online . . . transactions.[37]

The preamble to the California Online Privacy Protection Act is still accurate to date, as no federal or state law regulates how information is collected or used by any online site operator.[38] Indeed, California's legislation, and substantial state legislation enacted since, only regulates the disclosure of information practices.[39] As such, the privacy of users of social network

---

33. *Twitter Privacy Policy*, TWITTER, http://twitter.com/privacy (last visited Jan. 19, 2012).

34. *Safety: Private Information*, TWITTER HELP CENTER, http://support.twitter.com/entries/18368 (last visited Jan. 19, 2012).

35. Privacy policies are policies adopted by a website owner to govern the website's collection, use, and disclosure of private information about the site's users. The idea that privacy policies set users' expectations is somewhat tongue-in-cheek. As James Grimmelmann so aptly pointed out in his article *Saving Facebook*, 94 IOWA L. REV. 1137, 1141 (2009), "privacy policies are irrelevant; users don't pay attention to them when making decisions. . . ."

36. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2009). The Online Privacy Protection Act requires operators of commercial websites or online services that collect personal information from California residents through such websites or services to conspicuously post a privacy policy on the site and to comply with its policy. *Id.* § 22575(2). In addition, the Online Privacy Protection Act requires, among other things, that site operators identify the information categories collected and shared with third parties. *Id.* § 22575(b)(1).

37. Online Privacy and Disclosure Act of 2002, A.B. 2297, 2001–02 Leg., Reg. Sess. (Cal. 2002), *available at* http://www.leginfo.ca.gov/pub/01-02/bill/asm/ab_2251-2300/ab_2297_bill_20020830_enrolled.html.

38. In contrast, the European Union has taken a more hands-on approach in the regulation of privacy online. In 1995, the European Union adopted a directive regarding the protection of individuals' data online. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. The EU requires website operators to obtain express consent to collect a user's personal data. *See id.* at 41.

39. CAL. BUS. & PROF. CODE §§ 22575–22579.

sites is governed by the self-regulatory regime of contracts between the social network site and the user via the site's privacy policy. This self-regulatory regime has proven to be insufficient to protect the expectation of privacy for the users.[40] The premise that users of the social network sites "should have the freedom to decide with whom they will share their information, and to set privacy controls to protect those choices[,]"[41] is a farce at best. Users have no control other than that which the social network site grants through its privacy policies and terms of use.[42] Because the social network site is free to define what information is public,[43] it is imperative to point out a very important, yet rarely read, type of clause that is usually posted somewhere in the legal terms that govern use of the network:

> Social Network Site reserves the right to modify or change this policy and adopt new policies by providing notice (all such notices and changes shall be posted yet buried somewhere on the network and if you really try to find it, you may, but the odds of finding these changes are slim to none. LOL).[44]

While the above-emphasized clause is meant to spur laughter, the reality is that it took me roughly ten minutes to actually locate this clause on Facebook's website.[45] The aforementioned clause has been the impetus for the many changes to privacy policies of social networks such as Facebook.[46]

The Electronic Frontier Foundation's[47] terms of use project, which tracks changes to the terms and condition timeline of Facebook policy changes is illustrative:[48]

---

40. *See infra* Part IV.

41. *Facebook Principles*, *supra* note 32.

42. *See supra* note 35.

43. A social network site's designation of information as "public" is not a coincidence. Under current tort standards, one does not have any privacy rights in information that is made public. *See generally* Restatement (Second) of Torts § 652 (1977).

44. Of course, this is not an actual statement on any social network site, but as a former drafter of privacy policies, my general practice was to include reservations to modify the agreement in the terms of use of the online service provider in a section that discussed and incorporated the privacy policy.

45. The task of locating the reservation of rights clause in the policies posted on Facebook was somewhat troubling. In fact, I actually had to conduct a search on Google to locate its whereabouts.

46. The latest change on Facebook is an attempt to make the privacy and user policies more user friendly. While Facebook should be commended for this attempt, the current changes seemingly over simplify the policies and leave one searching for a complete policy to compare what appears to be a top-level summary. *Data Use Policy*, FACEBOOK, http://www.facebook.com/about/privacy (last visited Apr. 4, 2012).

47. The Electronic Frontier Foundation (EFF) has started the archival project, which tracks changes of the terms of use and privacy policies of many social network sites on TOSBack.org.

Facebook Privacy Policy circa 2005

> No personal information that you submit to Thefacebook [sic] will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.[49]

Facebook Privacy Policy circa 2006

> We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about.[50]

Facebook Privacy Policy circa 2007:

> Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.[51]

Facebook Privacy Policy circa November 2009:

> Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences. You should also consider your settings whenever you share information....
>
> Information set to "everyone" is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the

48. Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELEC. FRONTIER FOUND. (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline. Facebook is used herein most often, as it has been the social network site that has garnered the most users and subsequently has promoted the most privacy changes.

49. *Id.* (internal quotation marks omitted).

50. *Id.* (internal quotation marks omitted).

51. *Id.* (internal quotation marks omitted).

> internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings.[52]

Facebook Privacy Policy circa December 2009:

> Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings.

Facebook Privacy Policy circa April 2010:

> When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to "everyone."... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.[53]

Facebook Privacy Policy current, dated September 2011:

> When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available. . . Choosing to make your information public is exactly what it sounds like: anyone, including people off of Facebook, will be able to see it. Choosing to make your information public also means that this information:
>
> - can be associated with you (i.e., your name, profile picture, Facebook profile, User ID, etc.) even off Facebook
>
> - can show up when someone does a search on Facebook or on a public search engine

52. *Id.* (internal quotation marks omitted).
53. *Id.* (internal quotation marks omitted).

> • will be accessible to the games, applications, and websites you and your friends use
>
> • will be accessible to anyone who uses our APIs such as our APIs Graph API.
>
> Sometimes you will not be able to select an audience when you post something (like when you write on a Page's wall or comment on a news article that uses our comments plugin). This is because some types of posts are always public posts. As a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available. . . .
>
> The types of information listed below are always publicly available, and are treated just like information you decided to make public.
>
> • **Name[:]** This helps your friends and family find you. If you are uncomfortable sharing your real name, you can always deactivate or delete your account.
>
> • **Profile Pictures[:]** This helps your friends and family recognize you. If you are uncomfortable making your profile picture public, you can always delete it by hovering over your photo and clicking "Change Picture."
>
> • **Network[:]** This helps you see whom you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you are uncomfortable making your network public, you can leave the network.
>
> • **Username and User ID[:]** These allow you to give out a custom link to your profile or Page, receive email at your Facebook email address, and help make Facebook Platform possible.[54]

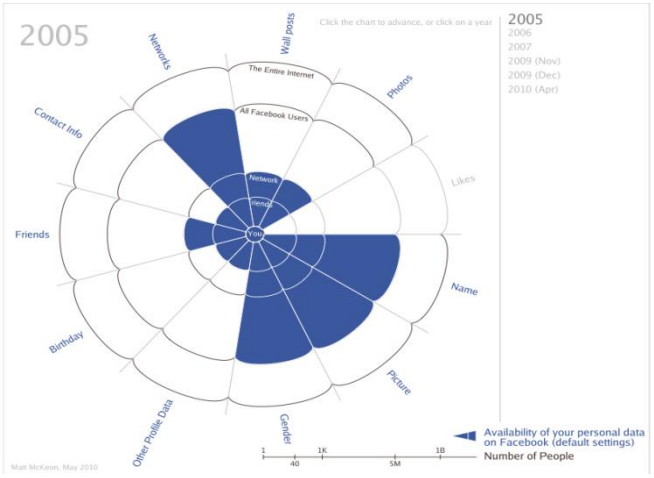
What is readily apparent with the successive changes made to Facebook's privacy policy is with each change, the policy regarding privacy became longer.[55] But what is most disconcerting is that Facebook whittled away user control with each policy change. Kurt Opsahl of the Electronic

---

54. *Information We Receive and How it is Used*, FACEBOOK, http://www.facebook.com/about/privacy/your-info#everyoneinfo (last visited on Jan. 25, 2012).

55. One of the major complaints about online policies is that they are dense and not user-friendly. Indeed, Facebook and Twitter have introduced what have been themed user-friendly policies. While these policies are appeasing to the eye of the user, they are disjunctive and misleading.

Frontier Foundation suggests that Facebook gained its core group of users by allowing meaningful control of the information posted on its network.[56] While changes made by social network sites are within the networks' authority, the above-illustrated timeline of changes made by Facebook appears to be a privacy bait-and-switch.[57] User privacy expectations upon enrolling in the network are vastly different from those that currently govern information on the network. The diagrams below, by IBM researcher Matt McKeon, create a visual that shows the whittling away of user control.[58] The graphic account by McKeon supports the position that "Facebook has steadily—and quite deliberately—carved away at the privacy protections its service was originally founded upon. It has essentially created a bait-and-switch scam: promising one thing but delivering something entirely different."[59]



[60]

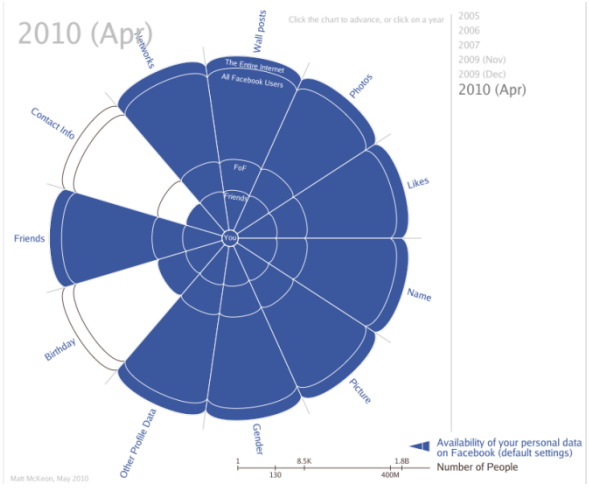
56. Opsahl, *supra* note 48.

57. *Id*.

58. Matt McKeon, *The Evolution of Privacy on Facebook*, MATTMCKEON.COM, http://mattmckeon.com/facebook-privacy/ (last visited on Jan. 25, 2012) (providing graphic illustrations of the changes in privacy).

59. Dan Tynan, *How Facebook Pulled a Privacy Bait and Switch*, PC WORLD (May 11, 2010, 7:58 AM), http://www.pcworld.com/article/196023/how_facebook_pulled_a_privacy_bait_and_switch.html.

60. McKeon, *supra* note 54. This chart by Matt McKeon shows the original privacy promises made by Facebook.



61

Notwithstanding changes made by Facebook to its network's privacy policies, Facebook still maintains that the policies and applications that it has developed make the users' control of their personal information attainable.[62] So the question remains, what are the users' expectations of privacy on social networks? Daniel Solove makes a very interesting argument that privacy for users of social networks is not grounded in secrecy or disclosures, but rather the ideas of "dissemination" and "accessibility."[63] The expectation of privacy of social network site users is to maintain control of dissemination and accessibility by having the privacy settings and policies of the social network honored. The Supreme Court has recognized that:

> [B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to

61. *Id.* This chart illustrates the existing default settings of public information.

62. This outlook by Facebook is a contradiction to Zuckerberg's statement at the Crunchie conference in San Francisco in 2010, suggesting that privacy is no longer a societal norm. *See* Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN (Jan. 10, 2010, 8:58 PM), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

63. Solove, *supra* note 23, at 1152–53.

> the use of a particular person or group or class of persons: not freely available to the public."[64]

Having determined the expectation of privacy of users of social network sites, the remaining question to be answered in this section of the Article is whether this expectation is reasonable. Phrased differently, is there an expectation of privacy (or control by users of information freely disclosed) on social network sites that society is willing to recognize as reasonable?[65] The above-quoted text from the Supreme Court's decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press* validates the subjective expectation of privacy held by the users of social network sites.[66] The second prong requires determining whether disclosure on a social network renders the subjective expectation of privacy by users unreasonable.[67] To make this determination, it is instructive to review tort law's distinction between private and public disclosures.[68] Under the public disclosure of private facts tort, in order for a cause of action to exist, the fact disclosed must be private.[69] Like the definition of privacy itself, no one definition of "private" in privacy torts exists. What we are left with are examples of what is public and what is not private. Many courts have found that matters are no longer private when they occur in public.[70] With respect to

---

64. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763–64 (1989) (citations omitted).

65. Fourth Amendment privacy jurisprudence requires for standing that there be a subjective expectation of privacy. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

66. *Reporters Comm.*, 489 U.S. at 763–64.

67. In this section, I purposefully mix tort theory of privacy and Fourth Amendment privacy expectations. It is my opinion that use of the concepts of publicity and reasonable expectation of privacy is necessary when attempting to understand why users of social network sites are outraged with the changing of privacy settings and why the laws need to adapt to reflect the current societal view on privacy.

68. Most jurisdictions have adopted invasion of privacy torts which protect the subjective expectation of privacy that Warren and Brandeis argued for in *The Right to Privacy* by providing a remedy to those whose private information is disclosed or rendered public by a third party. This section focuses solely on the public disclosure tort that creates a cause of action for one who publicly discloses a private matter that is "highly offensive to a reasonable person" and "is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (1977). "Publicity" requires widespread disclosure in most jurisdictions. *Id.* cmt. a. The last element, "not of legitimate concern to the public," is known as the "newsworthiness test" and is designed to protect free speech interests. *Id.* cmt. g.

69. *Id.* cmt. b.

70. *See, e.g.*, Gill v. Hearst Publ'g Co., 253 P.2d 441, 443–44 (Cal. 1953); Melvin v. Reid, 297 P. 91, 93 (Cal. Dist. Ct. App. 1931) (stating there can be no privacy in that which is already public); Cefalu v. Globe Newspaper Co., 391 N.E.2d 935, 939 (Mass. App. Ct. 1979); Penwell v. Taft Broadcasting, 469 N.E.2d 1025, 1028 (Ohio Ct. App. 1984).

disclosure of information to third parties, the two leading cases are *Y.G. v. Jewish Hospital of St. Louis*[71] and *Multimedia WMAZ, Inc. v. Kubach*.[72]

In *Y.G. v. Jewish Hospital of St. Louis*, a couple unable to conceive a child underwent *in vitro* fertilization at the defendant hospital.[73] The procedure was successful and only the hospital and one mother-in-law knew of the couple's participation in the *in vitro* program.[74] The couple did not disclose their involvement because their church condemned the practice.[75] Several months into their pregnancy, the couple was invited to a party at the hospital to celebrate the *in vitro* fertilization program's five-year anniversary.[76] A camera crew and reporter from a local television station were at the party, and while the plaintiffs refused to be interviewed and "made every reasonable effort" to avoid being filmed, their image was used on the nightly news, with a voiceover stating that the (unnamed) couple were expecting triplets as a result of their participation in the program.[77] After the broadcast, the couple was chastised by their church and the husband was ridiculed at his workplace.[78] The hospital argued that the plaintiffs had waived any reasonable expectation of privacy as to their involvement in the *in vitro* clinic by attending a party that forty other people also attended.[79] The court rejected this argument, holding that by attending the party the plaintiffs "clearly chose to disclose their participation to only the other *in vitro* couples. By so attending this limited gathering, they did not waive their right to keep their condition and the process of *in vitro* private, in respect to the general public."[80]

Similarly, in *Kubach*, an HIV-positive man disclosed his condition to relatives, "friends, medical personnel and members of his AIDS support group," approximately sixty people in all.[81] Kubach agreed to appear on a local television broadcast to discuss AIDS, conditioned upon his identity being digitally masked to the viewing audience.[82] The station employee responsible for the digitization was unable to properly digitally mask Kubach because of low settings, and Kubach was recognized by members of his

71. 795 S.W.2d 488 (Mo. Ct. App. 1990).
72. 443 S.E.2d 491 (Ga. Ct. App. 1994).
73. 795 S.W.2d at 492.
74. *Id.* at 492–93.
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Y.G.*, 795 S.W.2d at 502.
80. *Id.*
81. *Kubach*, 443 S.E.2d at 494 n.1 (stating that Kubach disclosed his HIV status to "a relatively small number of people he thought had reason to know of his disease").
82. *Id.* at 493 (noting that Kubach would not have participated without assurances that his identity would be concealed from the viewing public).

local community when the broadcast aired.[83] The station argued that Kubach had waived his expectation of privacy in his HIV status by disclosing it to his friends, relatives, acquaintances, and medical service providers.[84] The court disagreed, commenting that Kubach had made these disclosures to people who "cared about him . . . or because they also had AIDS."[85]

These cases suggest that even if an individual discloses information about himself to dozens of people without legal or contractual constraints on those people's ability to disseminate the information further, the information can remain "private" for the purposes of privacy tort law.[86] This type of privacy has been termed "limited privacy" and is seen not only in the public disclosure tort but also in the intrusion tort.[87] For example, in *Sanders v. American Broadcasting Companies, Inc.*,[88] an ABC investigative journalist obtained employment as a telephone psychic and used hidden cameras to expose fraud in the telephone psychic industry.[89] One of the coworkers, Mark Sanders, sued after part of his conversation with the journalist was broadcast on ABC's PrimeTime Live program.[90] The defendant argued that because Sanders' coworkers could overhear the parties' conversations, there was no reasonable expectation of privacy in the communication.[91] The court disagreed:

> This case squarely raises the question of an expectation of limited privacy. . . . [P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. 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. . . . "The mere fact that a person

83. *Id.*

84. *Id.* at 493–94 (noting the argument made by the station in further support of its position that Kubach had appeared on a national television show where he allowed his back to be viewed undigitized and his voice to be heard undisguised).

85. *Id.* at 494.

86. It is imperative to point out at this juncture that not all courts have recognized this limited right of privacy. *See, e.g.*, Med. Lab. Mgmt. Consultants v. Am. Broad. Co., 306 F.3d 806, 815–16 (9th Cir. 2002); Myrick v. Barron, 820 So. 2d 81, 85 (Ala. 2001); Johnston v. Fuller, 706 So. 2d 700, 702–03 (Ala. 1997); Duran v. Detroit News, Inc., 504 N.W.2d 715, 720 (Mich. Ct. App. 1993); Fisher v. Ohio Dep't of Rehab. & Corr., 61 Ohio Misc. 2d 303, 306 (Ohio Cl. Ct. 1988).

87. Sanders v. Am. Broad. Cos., 978 P.2d 67, 72 (Cal. 1999).

88. *Id.* at 69.

89. *Id.* at 70.

90. *Id.* at 70 n.1.

91. *Id.* at 75.

> can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."[92]

The disclosures on social network sites by their users dovetail greatly with these cases. Yet in the relatively few cases involving disclosures and access of information on social network sites, courts and juries alike have been unwilling to recognize this limited right of privacy.[93] For instance, in *Pietrylo v. Hillstone Restaurant Group*,[94] a group of employees were terminated based upon posts to a MySpace group, the Spec-Tator.[95] The jury in this case rejected their claims for invasion of privacy.[96] Explaining that while the Spec-Tator was "a place of solitude and seclusion which was designed to protect the Plaintiffs' private affairs and concerns[,]" the jury found that the plaintiffs did not have a reasonable expectation of privacy in the MySpace group.[97]

Similarly, in *Moreno v. Hanford Sentinel, Inc.*,[98] the court refused to recognize the limited privacy expectation, maintaining that once information is posted on a social network, it is public information.[99] The court ruled that there were no private facts at issue with the publication of a post by Cynthia Moreno bashing her hometown because "[a] matter that is already public or that has previously become part of the public domain is not private."[100] The court commented that there could be no reasonable expectation that the information would remain private and found that "the fact that Cynthia expected a limited audience does not change the above analysis. By posting the article on MySpace, Cynthia opened the article to the public at large. Her potential audience was vast."[101]

The apparent discrepancy in these MySpace cases can be attributed to a lack of understanding of how social network sites operate. As discussed above, users are able to designate the information that they wish to keep private—that is, shared only with those in their network—and, thusly, have an expectation of limited privacy. The use of privacy controls works nicely

---

92. *Id.* at 72 (quoting 1 MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.10[A][2](1998)).

93. *See infra* notes 90–96 and accompanying text.

94. No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 24, 2008).

95. *Id.* at *1–4.

96. *Id.*.

97. Jury Verdict Sheet, Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 24, 2008), ECF No. 61.

98. 91 Cal. Rptr. 3d 858 (Cal. Ct. App. 2009).

99. *Id.* at 861.

100. *Id.* at 862.

101. *Id.* at 863.

within the prescribed definition of limited privacy.[102] Indeed, an adoption and use of Lior Strahilevitz's network theory principles advanced in *A Network Theory of Privacy* would prove beneficial in determining whether a limited privacy interest exists in information that has been previously disclosed.[103] Strahilevitz proposed that the appropriate legal analysis to determine whether a privacy interest exists in information after a disclosure should be "what the parties should have expected to follow the initial disclosure of information by someone other than the defendant."[104] In other words, information should be deemed private if the information stays confined to the initial group to which it was disclosed, even if such a group is rather large.[105] As such, use of controls provided by social network sites sets a reasonable expectation of privacy, albeit limited, for their users.

IV. LOSS OF CONTROL

> Wanting privacy is not about needing something to hide. It's about wanting to maintain control. Often, privacy isn't about hiding; it's about creating space to open up. If you remember that privacy is about maintaining a sense of control, you can understand why Privacy is Not Dead. There are good reasons to engage in public; there always have been. But wanting to be in public doesn't mean wanting to lose control.[106]

The first outcry regarding the disclosure of information in contradiction to users' expectations of privacy occurred in September 2006 when Facebook introduced its "News Feed" feature.[107] The feature allowed the display of Facebook users' activities to friends within the network.[108] Specifically, the application monitored the activity on its members' pages, such as "a change in one's relationship status, the addition of a new person to one's friends list, the listing of a new favorite song or interest," and sends that

---

102. As the court stated in *Sanders*, there are degrees and nuances in privacy. Sanders v. Am. Broad. Cos., 978 P.2d 67, 72 (Cal. 1999).

103. *See* Lior Jacob Strahilevits, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

104. *Id.* at 988.

105. As discussed herein, the requirement of complete secrecy of information has been generally rejected in contemporary privacy cases. *See id.*

106. danah boyd, *Making Sense of Privacy and Publicity*, SXSW (Mar. 13, 2010), http://www.danah.org/papers/talks/2010/SXSW2010.html.

107. This section focuses on Facebook for two reasons: (1) Facebook is the largest social network site with more than 800 million active users; and (2) to date, Facebook has had the most policy changes with regard to user controls of dissemination and accessibility of information. *See Facebook Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Jan. 25, 2012).

108. Warren St. John, *When Information Becomes T.M.I.*, N.Y. TIMES, Sept. 10, 2006, http://www.nytimes.com/2006/09/10/fashion/10FACE.html.

information to members of the user's network.[109] While the information disseminated was ordinarily deemed public, the idea that friends no longer had to visit a user's page to glean the information was disconcerting to users.[110] As a result, a number of protest pages developed and Facebook instituted privacy controls that allowed users to dictate to whom their information would be broadcast.[111] Interestingly enough, Zuckerberg admitted, "'We really messed this one up. . . . In general the more control you can give people the better. . . . If you give people control over everything they do, you'll never put them in a situation that's uncomfortable.'"[112]

Notwithstanding the above quoted understanding of the importance of user control (privacy), the most egregious loss of control occurred in December of 2009 when Facebook made one of the most controversial changes to its privacy policy.[113] The change created a scenario in which users' profiles were publicly searchable with most of the information opened up for all to see by default.[114] The "control" was given to users in a pop-up, which asked the users to reset their user preferences.[115] Specifically, the pop-up asked users to make information available to "Everyone" or to keep the old settings.[116] Not surprisingly, users by-passed the pop-up and unwittingly set their preferences to "Everybody" by default.[117] As a result of this common, yet unfortunate, behavior, the acceptance of the policy as revised rendered the following information "publicly available information": "users' names, profile photos, lists of friends, pages of which they are fans, gender, geographic regions, and networks to which they belong."[118] Prior to the change, information that was publicly available by default was users' names and networks.[119]

---

109. *Id*.
110. *Id*.
111. *Id*.
112. *Id*. (quoting from Mark Zuckerberg, *An Open Letter from Mark Zuckerberg*, FACEBOOK (Sept. 8, 2006, 2:48 AM), http://blog.facebook.com/blog.php?post=2208562130).
113. *See* boyd, *supra* note 102. The change in the policy no longer allowed users to have an invisible account, allowing only those you wanted in by default. According to the changes, certain aspects of the profile would be accessible to the public from a general search.
114. *Id*. Privacy policy available at *Data Use Policy*, FACEBOOK, http://www.facebook.com/about/privacy/ (last visited Jan. 25, 2012).
115. *See* boyd, *supra* note 102.
116. *Id*.
117. *Id*.
118. *Information We Receive and How it is Used*, *supra* note 50.
119. *Id*.

IV. SETTLEMENTS/PRIVACY BILL OF RIGHTS/PRIVACY BILLS

As social network sites continue to become a primary mode of communication, privacy advocates and Congress alike have recognized the problem and have begun to take action. The Electronic Privacy Information Center (EPIC) and other privacy advocates filed a complaint with the Federal Trade Commission (FTC) as a result of the changes in policy by Facebook in 2009.[120] The complaint alleged, among other things, that the manner in which the changes were presented and ultimately made to individuals' privacy settings were deceptive and in violation of the FTC Act.[121] This prompting by EPIC launched the FTC's investigation of Facebook, which concluded on November 29, 2011 and ended with a settlement.[122] The settlement required that Facebook provide consumers with clear and prominent notice and obtain express consent before their information is shared beyond the privacy settings that are currently established.[123] The most meaningful of the conditions of settlement as it relates to privacy is the requirement that "affirmative express consent" must be obtained prior to utilizing any information that "exceeds the restriction imposed by the privacy setting(s) in effect for the user."[124] EPIC has filed another complaint in response to a new feature, Timeline, with the FTC questioning whether this change is in compliance with the settlement agreement.[125]

The Electronic Frontier Foundation advocacy includes the formation of a Social Network Bill of Rights.[126] The Bill of Rights has three main rights: (1) The right to informed decision-making—providing users with meaningful choices about policies regarding access and use of user data; (2) The right to control—requiring social network sites to ensure the retention of control over the use and disclosure of user data with the network taking a limited license; (3) The right to leave—enabling users to delete their data and account if the user no longer wishes to be a part of the social network. The EFF advocates that the above-listed principles, if demanded and adhered to by social network sites, will provide an environment where innova-

120. *Complaint, Request for Investigation, Injunction, and Other Relief*, EPIC.ORG (Dec. 17, 2009), http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

121. See 15 U.S.C. §§ 41–58.

122. *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm.

123. Agreement Containing Consent Order, *In re* Facebook, Inc., No. 92-3184 (F.I.C. 2011), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

124. *Id.*

125. *Id.*

126. Kurt Opsahl, *A Bill of Privacy Rights for Social Network Users*, ELEC. FRONTIER FOUND. (May 19, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users.

tion in social network services can develop while maintaining user privacy and control.[127]

In addition to privacy advocate groups developing an interest in the policies of social network sites and privacy, Congress has begun to review the practices.[128] Recognizing the potential impact on privacy and communications generally, Congress held hearings on July 28, 2010.[129] The hearings focused on determining whether there was sufficient governmental interest in regulating social network sites, or whether to maintain the status quo.[130] Senators John Kerry and John McCain have introduced Internet privacy bills that would, in effect, maintain the status quo of a self-regulatory regime, but have also introduced a Commercial Privacy Bill of Rights similar to that proposed by privacy advocates.[131] Representative Cliff Stearns introduced a similar bill in the House.[132] In addition, Representative Ed Markey is currently introducing a mobile device privacy bill that again seeks to provide users with the ability control access and tracking of data.[133]

---

127. *Id.*

128. *See generally Online Privacy, Social Networking and Crime Victimization: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 111th Cong. (2010).

129. *See generally id.*

130. *See generally id.*

131. *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011). *See also* Paul Eng, *Kerry and McCain Introduce Online Privacy Bill in U.S. Senate*, CONSUMERREPORTS.ORG (Apr. 13, 2011, 10:23 AM), http://news.consumerreports.org/electronics/2011/04/online-privacy-bills-mccain-kerry-bills-web-tracking-ads-yahoo-goolge.html.

132. *See* Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011).

133. Ed Markey, *Discussion Draft, Mobile Device Privacy Act*, (Jan. 25, 2012, 5:13 PM), http://markey.house.gov/sites/markey.house.gov/files/documents/Mobile%20Device%20Privacy%20Act%20--%20Rep.%20Markey%201-30-12_0.pdf.

The Bill requires:

> A. Monitoring software must be disclosed when a person buys a mobile phone, and also after the sale if any party decides to install monitoring software after the fact.
>
> B. App makers that include monitoring software must also disclose it.
>
> C. All disclosures must say whether the monitoring software has been installed, and detail the type of information collected, where it's going, and how it will be used.
>
> D. Consumers must give their consent before monitoring or data transfer takes place.
>
> E. Those who receive data must be able to secure it.
>
> F. Data sharing agreements have to be filed with the FTC and FCC.

See generally id. See also John Eggerton, *Markey Drafts Mobile Privacy Legislation*, MULTICHANNEL.COM (Jan. 30, 2012), http://www.multichannel.com/article/479874-Markey_Drafts_Mobile_Privacy_Legislation.php.

What is clear from the settlement, the proposed bill of rights, and bills introduced in Congress, is that there is this grave concern that privacy (as defined herein as control of use of information) is being lost as technology advances. There is an awareness of the balance that must be struck between the technology and legislation to ensure growth and innovation, and yet preserve the privacy expectation of users of social media. All of these measures fall short, however, of creating a disincentive for social media services to continue down the path already taken.

V. SOCIAL NETWORK PRIVACY TORT

"Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[134]

The problem as presented by advocates and sought to be addressed by privacy bills is the regulation of social networks. While the efforts are commendable, the proposed regulations as well as current settlement agreements[135] still provide loopholes. As discussed earlier, the major "win" for users is the requirement that they are informed of, and have consented to, any changes. We must, however, face the fact that a growing number of users simply do not read user policies![136] Knowing this propensity of its users, can informing them of the user policy when no one reads it, or surreptitiously placing a notice at a point where users will by-pass it to get to the site, satisfy these requirements?[137] Did the social network site comply with the spirit and the letter of the settlement? Or is it the users' own fault for failing to read? Asking these questions exposes the loopholes that currently exist with respect to regulating behavior of social network sites, while at the

134. Warren & Brandeis, *supra* note 2, at 193.

135. The FTC provides copies of settlements with Google, Twitter and Facebook on its website. *See Case Names Only*, FED. TRADE COMM'N (Aug. 25, 2011), http://www.ftc.gov/os/caselist/index.shtm.

136. *See* Cheryl Hall, *Social Media Users Lose Privacy Rights*, YAHOO! BUS. & HUMAN RIGHTS PROGRAM (Sept. 7, 2011), http://www.yhumanrightsblog.com/blog/2011/09/08/social-media-users-lose-privacy-rights/. Peter Vogel, professor of Internet law at SMC states, "'social media users almost never read the terms of service and privacy policies. . . ." *Id.* Indeed, a 2006 U.C. Berkeley Study indicated that only 1.4 % of users read the agreements often and thoroughly. *See generally* Victoria C. Plaut & Robert P. Bartlett, *Blind Consent? A Social Psychological Investigation of Non-Readership of Click-Through Agreements*, 31 LAW & HUM. BEHAV. 1 (Feb. 2007), *available at* http://www.law.berkeley.edu/files/bclbe/Blind_Consent(1).pdf (last visited Aug. 31, 2012).

137. It should be noted that users do not ignore these policies because of laziness, but rather because they often are written in such a manner that the user population simply could not understand. *See generally id.*

same time continuing to allow the proliferation of a self-regulatory regime with monitoring by a federal agency.

As suggested in *You Have Zero Privacy Get Over It!*, conventional laws and regulations do not sufficiently address the privacy challenges of social network sites.[138] Privacy advocates, the FTC, and Congress alike find that there is a need to preserve the user controls of disclosure and use once a choice is made to restrict access.[139] What remains is the courts' recognition that the expectation of privacy can be maintained in a limited form on these networks.[140] There exists in the common law a remedy which does not require legislation.[141] An expansion of the privacy torts, more specifically the torts of public disclosure, invasion, and appropriation, can adequately address the problems that plague social network sites users.[142]

Before addressing the particulars of the expansion, it is instructive to briefly review the theory behind tort law. Prosser and Keeton describe deterrence as one of the factors underlying tort doctrine:[143]

> The "prophylactic" factor of preventing future harm has been quite important in the field of torts. The courts are concerned not only with compensation of the victim, but with admonition of the wrongdoer. When the decisions of the courts become known, and defendants realize that they may be held liable, there is of course a strong incentive to prevent the occurrence of the harm. Not infrequently one reason for imposing liability is the deliberate purpose of providing that incentive.[144]

The factors that underlie tort doctrine seemingly would address the problem that users of social network sites face with the whittling away of privacy online. Currently, there is no incentive for social network sites to discontinue their policy change practices, nor is there any deterrent effect from the settlement agreement, bill of rights, or proposed online privacy bills. As such, tort law is appropriate, as it provides incentives for behavior modification, incremental deterrent effects through liability for behavior, and compensation for the ensuing harm.[145] In the context of social network sites, "[o]nce an individual has established privacy settings and parameters .

---

138. Powell, *supra* note 6, at 147.

139. *See supra* Part IV.

140. See *supra* Part III and its discussion of MySpace cases.

141. *See* Warren & Brandeis, *supra* note 2, at 193.

142. In *You Have Zero Privacy. Get Over It!*, I only argued for the expansion of the disclosure tort. Powell, *supra* note 6, at 147. I now believe that the technology and potential uses of information dictates an expansion of the intrusion and appropriation tort.

143. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 4, at 25 (W. Page Keeton ed., 5th ed. 1984).

144. *Id.*

145. J. Clark Kelso, *Sixty Years of Torts: Lessons for the Future*, 29 TORT & INS. L. J. 1, 5–6 (1993).

. . [t]he failure to obtain permission and subsequent disclosure of this information would constitute a 'legal injuria,'" the harm ultimately being the loss of control of dissemination and use of one's information—invasion of privacy.[146] "If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."[147] As such, it logically follows that the privacy torts could be expanded to encompass the current definition of privacy held by users of social network sites.

The public disclosure of private facts tort is defined by the Restatement (Second) of Torts as:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[148]

Extending this tort to accommodate current views on privacy requires the addition of an "or" and a subsection worded as follows: "(c) discloses information that has previously been restricted from public views on social networks" would provide the necessary remedy.[149] The intrusion upon seclusion tort is defined by the Restatement (Second) of Torts as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[150]

Expanding this tort would require the following revision: One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, *or accesses, or monitors electronically information restricted by privacy settings without notice and consent*. This addition creates liability for failing to disclose how information will be used and acting inconsistently with the disclosures without obtaining consent once privacy settings have been designated.

The tort of appropriation is currently defined as: "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[151] Expanding this tort re-

146. Powell, *supra* note 6, at 178. It is important as we move through this section to recognize that social networks' users' privacy expectations are control, and, as such, loss of that control is a violation or an invasion of privacy.

147. Warren & Brandeis, *supra* note 2, at 213.

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

149. Powell, *supra* note 6, at 179.

150. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

151. *Id.* § 652C.

quires the following revision: "One who appropriates to his own use or benefit the name, likeness, or *restricted data* of another is subject to liability . . . ." As used herein, "restricted" shall include all information collected or disclosed with privacy settings. Again this revision creates liability for knowingly using data that was acquired in a manner inconsistent with the privacy settings established by the user.

These minor revisions to existing tort law provide the incentive for social network sites to comply with their own policies as well as any settlements with the FTC and any online privacy bills that are passed. The changes create liability, which should cause social network sites to pause before making changes that will adversely affect the control of their users. The "imposition of liability substantially affects how categories of actors respond to the risks they create or confront."[152]

VI. CONCLUSION

Facebook founder Mark Zuckerberg declared that "the age of online privacy is dead, and we killed it."[153] Prominent privacy scholar Anita L. Allen suggests that there has been "the rapid erosion of expectations of personal privacy . . . people expect increasingly little physical, informational, and proprietary privacy, and . . . prefer less of these types of privacy relative to other goods."[154] The traditional view of privacy, as equivalent to secrecy, has certainly rested its head. However, a new definition of privacy has evolved—one in which individuals expect to maintain control over the information that they select to disclose. Users of social network sites freely share their private affairs with those in their networks. Some even restrict access to a subset of friends. Users expect, however, that their restrictions will be honored and that their private affairs will remain private within their network—not public for the whole world to see. As the concepts of privacy evolve, so must the laws that assign liability for invasion of privacy. Tort liability has for decades been used to deter invasions of privacy as privacy was previously defined. Technology and new attitudes dictate that such laws evolve as well. The common law is well suited for this purpose. Expanding and revising privacy torts are the way to ensure that social network sites honor their policies and their users' expectations of privacy.

---

152. Howard A. Latin, *Problem-Solving Behavior and Theories of Tort Liability*, 73 CAL. L. REV. 677, 677 (1985).

153. *See* Melissa Smich, *FaceBook's Mark Zuckerberg: The Age Of Online Privacy Is Dead, And We Killed It*, WEB HOSTING BLOG (Jan. 12, 2010), http://myhosting.com/blog/2010/01/facebooks-mark-zuckerberg-the-age-of-online-privacy-is-dead-and-we-killed-it/.

154. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 729–30 (1999).