5-1-2013

Protecting the User: The Necessity of Governing the Privacy Settings of Social Media Websites

Lauren Estacio

Protecting the User: The Necessity of Governing the Privacy Settings of Social Media Websites

by Lauren Estacio

INTRODUCTION

As society's use of and dependence on the internet increases, social media websites are becoming more prevalent and integral to daily life. The nature of many, if not all, social media sites is to put personal information out into the cloud that is the internet to be viewed and enjoyed by others. This benefit of increased access to information, however, is also accompanied by often unforeseen costs. Many social media users believe that the information they post is visible only to their small circle of close friends or family and may not realize the potential harms that can arise when such information is disseminated more broadly than they anticipated. Tort laws governing privacy are an individual's primary weapon against such harms, but these laws provide inadequate protection for users who unsuspectingly disseminate private information to the public. Thus, legislatures should enact laws requiring social media websites to preemptively protect users' privacy by implementing default privacy settings that cause all content to remain private until the user actively chooses to make it public.

Part I of this paper explores the history of the internet and social media. Part II of this paper will analyze the social media website Facebook and its privacy settings. Part III will examine the background of privacy law in the United States, including protections granted by the Constitution and those contained in tort law. Finally, in Part IV, this paper will consider the implications of privacy tort law in the context of the social media site Facebook. This final section will also recommend changes to Facebook's default privacy settings, as well as potential legislation and other actions, that will generate greater privacy protection of social media users.

I. THE HISTORY OF THE INTERNET AND SOCIAL MEDIA

A. The Birth Of The Internet

In 1958, in response to the launch of Sputnik by the Unified Soviet Socialists Republic, President Eisenhower created the Advanced Research Projects Agency (ARPA) to focus on the advancement of science and technology.[1] The basic concepts of the internet were first developed in the mid-1960s by members of ARPA. According to Leonard Kleinrock, a member of ARPA's computer-science unit, the internet was born in the fall of 1969 when ARPA members successfully sent data between computers hundreds of miles apart.[2] Computer powerhouses Apple, Inc. and IBM introduced the first personal computers to the public in 1977 and 1981, respectively.[3] It was not until the 1990s, however, that the internet as we know it today quickly gained popularity with and use by the general population.[4] In 1991, the World Wide Web, a global information-linking device, was born at CERN in Geneva, Switzerland, necessitating the advent of browsers and transforming the internet into the dynamic tool as we know it today.[5]

Today, the internet serves as a complex multi-functional platform for communication, information gathering and sharing, entertainment, and shopping. In fact, the number of Americans with internet access has more than doubled since 2000.[6] According to a recent Nielsen report, approximately 274 million Americans – or nearly ninety percent of the

[1] Keenan Mayo & Peter Newcomb, *How the Web was Won: An Oral History of the Internet*, VANITY FAIR (Jul. 2008), *available at* http://www.vanityfair.com/culture/features/2008/07/internet200807; transcript of Leonard Kleinrock convo - http://curiosity.discovery.com/question/arpa-begin-network-computers.
[2] Mayo & Newcomb, *supra* note 1.
[3] Mayo & Newcomb, *supra* note 1.
[4] Steve Lohr, *For Impatient Web Users, an Eye Blink Is Just Too Long to Wait*, N.Y. TIMES, Mar. 1, 2012, *available at* http://www.nytimes.com/2012/03/01/technology/impatient-web-users-flee-slow-loading-sites.html?pagewanted=all.
[5] Mayo & Newcomb, *supra* note 1.
[6] Nielsen, *Detailing the Digital Revolution: Social, Streaming and More*, NIELSEN WIRE (Feb. 24, 2012), *available at* http://blog.nielsen.com/nielsenwire/media_entertainment/detailing-the-digital-revolution-social-streaming-and-more/.

population – now have access to the internet.[7] Americans spend on average three hours and fifty-eight minutes per week accessing the internet on a computer, while Americans age 25-34, 35-49, and 50-65 spend approximately six, six, and five hours per week on the internet, respectively.[8] Furthermore, nearly half of U.S. mobile subscribers, or nearly 100 million Americans, use smartphones, which provide easy access to the internet, as opposed to simple cellular phones that do little more than make and receive calls and text messages; this is a thirty-eight percent increase since February 2011.[9] Of those Americans who acquired a new mobile device between December 2011 and February 2012, more than two-thirds chose smartphones over simple cellular phones.[10] There is no doubt that the use and dependency on the internet in the U.S. will only continue to increase, especially as internet-ready devices, such as smartphones, tablet computers, and iPods, become more economical.

B. The Emergence Of Social Media And Its Impact

The internet's presence across the globe enables one to reach another person thousands of miles away within seconds in a variety of ways, one of which is social media. Merriam-Webster's dictionary defines social media as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)."[11] The term is further defined on the interactive online encyclopedia Wikipedia, itself a social media site, as "social

---

[7] *Id.*; U.S. & World Population Clock, U.S. CENSUS BUREAU (last visited Nov. 24, 2012 10:16 PM), http://www.census.gov/main/www/popclock.html.
[8] Nielsen, *State of the Media: Consumer Usage Report 2011*, NIELSEN WIRE, http://blog.nielsen.com/nielsenwire/mediauniverse/ (last visited Nov. 20, 2012).
[9] Nielsen, *Smartphones Account for Half of all Mobile Phones, Dominate New Phone Purchases in the US*, NIELSEN WIRE (Mar. 29, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us/; Milt Freudenheim, *As Smartphones Become Health Aids, Ads May Follow*, N.Y. TIMES, Apr. 1, 2012, *available at* http://www.nytimes.com/2012/04/02/technology/as-smartphones-become-health-aids-ads-may-follow.html.
[10] Nielsen, *Smartphones Account for Half of all Mobile Phones*, *supra* note 9.
[11] *Social Media Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/social%20media.

software which mediate human communication . . . [that, w]hen the technologies are in place, . . . is ubiquitously accessible, and enabled by scalable communication techniques."[12] These platforms allow anyone with access to the internet – regardless of class, education, age, or location – to simply, with the stroke of a key or a click of the mouse, share their photos, videos, opinions, and personal information and thoughts with the entire world.

According to Merriam-Webster, the first known use of the term "social media" was in 2004.[13] Today, the internet is replete with a variety of social media platforms – including but not limited to Twitter, Facebook, Pinterest, Wikipedia, LinkedIn, YouTube, Instagram, and MySpace – that facilitate sharing everything from photos and videos, to ideas about home decor, favorite recipes, life advice, and what one ate for dinner last night. In fact, in 2012, the number of social networking accounts worldwide surpassed 2.7 billion; this figure is expected to increase to over 4.3 billion by 2016.[14] There has also been a tremendous increase in the number of published and issued patents related to social networking.[15] As of the beginning of 2011, approximately 350 social networking patents had been issued, while over 3,500 patent applications had been published.[16] As of June 2012, 921 social media-related patents were projected to issue in 2012 alone.[17]

As the availability of social media has increased, so has society's use of social media. The world spends over 110 billion minutes, or twenty-two percent of all time spent online, on

[12] *Social Media*, WIKIPEDIA, http://en.wikipedia.org/wiki/Social_media.
[13] *Social Media Definition*, *supra* note 11.
[14] *Email Statistics Report 2012-2016*, THE RADICATI GROUP, INC. (Sara Radicati ed., May 2011), *available at* http://www.radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf.
[15] Mark Nowotarski, *Don't Steal My Avatar! Challenges of Social Networking Patents*, IPWATCHDOG (Jan. 23, 2011) http://www.ipwatchdog.com/2011/01/23/dont-steal-my-avatar-challenges-of-social-networking-patents/id=14531/ (where any patent application or issued patent that has the phrase "social network" anywhere in it is a social networking patent).
[16] *Id.*
[17] Roger Maxwell, *The Continuing (and Growing) Social Networking Patent Boom*, SOCIAL COMPASS (June 22, 2012), http://socialcompass.net/_blog/Social_Speak/post/The_continuingandgrowing_social_networking_patent_boom/.

social networking websites and blogs.[18] As of mid-2010, seventy-five percent of all internet users visit social media, a figure that increased by twenty-four percent in the preceding year.[19] In fact, visiting social media websites is now a more popular internet activity than viewing pornography in at least the U.S. and United Kingdom.[20] Moreover, in April 2010, the average user spent six hours on social media, a seventy-percent increase from 2009.[21] Social media is not being accessed only for personal use; in April, 2011, seventy-three percent of small businesses reported using social media marketing.[22]

Furthermore, not only is social media use widespread across the globe, it spans generations. Although top social networking site Facebook is reportedly the most common method of communication among some college students in the U.S.,[23] the number of social media users aged sixty-five and older grew one hundred percent in 2009.[24] In fact, this author's grandfather, who turned ninety-six in January 2013, joined Facebook in 2009 and continues to use it today.

---

[18] Nielsen, *Social Networks/Blogs Now Account For One in Every Four and a Half Minutes Online*, NIELSEN WIRE (June 25, 2010), http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/.
[19] *Id.*
[20] Andrew Couts, *Social Media Is Now More Popular Than Online Porn*, YAHOO! NEWS (June 30, 2011), http://news.yahoo.com/social-media-now-more-popular-online-porn-041648840.html; Bill Tancer, *Facebook: More Popular Than Porn*, TIME, Oct. 31, 2007, *available at http://www.time.com/time/business/article/0,8599,1678586,00.html*; Dan Whitworth, *Facebook More Popular Than Porn For UK Users*, BBC, Mar. 18, 2011, *available at* http://www.bbc.co.uk/newsbeat/12784325 (UK internet users spend 12.46 percent of internet usage on social media, as opposed to 12.18 percent on adult entertainment websites).
[21] Nielsen, *Social Networks/Blogs Now Account For One in Every Four and a Half Minutes Online*, *supra* note 18.
[22] Matt Krautstrunk, *Looking to Acquire Customers? Think Search Over Social*, GOOGLE LEAD SERVICES (May 24, 2011), http://www.googleleadservices.com/Blog/?p=212. Although only fifty-four percent of these businesses found social media marketing to be effective, as society becomes more internet savvy, both businesses and consumers will become more adept at using social media to their advantage. *See also* David Navetta, *The Legal Implications of Social Networking: The Basics (Part One)*, INFO LAW GRP. (June 11, 2011), http://www.infolawgroup.com/2011/06/articles/social-networking/the-legal-implications-of-social-networking-the-basics-part-one/.
[23] Kandace Harris, *Using Social Networking Sites as Student Engagement Tools*, DIVERSE EDUC., Oct. 16, 2008, *available at* http://diverseeducation.com/article/11837/.
[24] Joshua Norman, *Boomers Joining Social Media at Record Rates*, CBS (Nov. 16, 2010), http://www.cbsnews.com/stories/2010/11/15/national/main7055992.shtml. As further evidence of society's involvement in and use of social media, this CBS article generated four comments, 228 shares on Facebook, and 550 tweets on Twitter.

As is evidenced by these staggering statistics, social media has reached millions of internet users across all strata of the population. However, just as computer hacking became an inevitable consequence to the advent of the internet,[25] various illegal activity has arisen in response to the development and increased use of social media. A recent study attributes the thirteen-percent increase in identity theft in the U.S. in 2011 to the increased use of social media and smartphones.[26] In fact, while five percent of the general population fell victim to identity fraud in 2011, users of the social media website LinkedIn, which is aimed at connecting the business world, experienced the highest rate of identity fraud at ten percent.[27] Other social media websites that experienced higher-than-average rates of identity theft in 2011 include Facebook (5.7%), Google+ (seven percent), and Twitter (6.3%).[28] In fact, last summer, when at work in New York, this author received an e-mail notification from Facebook indicating that her account had been accessed from a location in Indonesia. Although a quick password change appears to have prevented any real threats, others may not be so lucky.

Moreover, companies, such as insurance giant Allstate, warn about publishing information online that indicates that you are not at home and invites burglars.[29] According to a 2010 study, sixteen percent of social media users in Australia post their whereabouts daily.[30]

---

[25] *See e.g.*, Mayo & Newcomb, *supra* note 1 (Robert Morris was the first person indicted under the Computer Fraud and Abuse Act. *See* U.S. v. Morris, 928 F.2d 504 (2d Cir. 1991). Morris wrote and released a computer worm that attacked and shut down computers' Unix operating systems.).
[26] Jennifer Waters, *Why ID Thieves Love Social Media*, WALL ST. J., Mar. 25, 2012, *available at* http://online.wsj.com/article/SB10001424052702304636404577293851428596744.html (approximately twelve million Americans were victims of identity theft in 2011).
[27] *Id.*
[28] *Id.*
[29] *See, e.g.*, *5 Social Media Strategies to Deter Burglary, Theft*, ALLSTATE (Feb. 14, 2012, 5:13 PM), http://blog.allstate.com/5-social-media-strategies-to-deter-burglary-theft/; *Social Media Updates Could Lead to Burglary*, FARMERS CARES (Sept. 20, 2012), http://www.farmers-cares.com/social-media-updates-could-lead-to-burglary (former employee of Farmers Insurance for thirty-three years warns social media users about the potential risks of posting personal information online); *see also* Michelle Manetti, *How Social Media Can Put Your Home At Risk For Thefts*, HUFFINGTON POST, http://www.huffingtonpost.com/2012/10/11/social-media-increase-home-thefts_n_1958392.html (last updated Oct. 12, 2012).
[30] Manetti, *supra* note 29.

Likewise, a whopping forty percent of British users publish their holiday plans online, while more than thirty percent post their ordinary weekend plans.[31] In 2010, police busted a burglary ring in New Hampshire that used Facebook to determine when their victims were not home.[32] More than fifty break-ins were reported, and over one hundred thousand dollars worth of property was recovered.[33] Allstate suggests that even a simple "check-in" at a restaurant or shop on Foursquare may invite an unwanted guest to one's home.[34]

Furthermore, the U.K. publication *Daily Mail* recently reported that insurance companies and financial institutions are cracking down on "grossly negligent" and "reckless" claimants whose loss was the result of posting information on social media sites.[35] Joel Winston, chief privacy officer at the consumer risk-management company ID Analytics, recently stated that, "[t]he new ways in which people can communicate with each other create new risks."[36] As these risks multiply and intensify, so must the precautions taken by social media users and providers, as well as the U.S. government.

II. FACEBOOK AND ITS PRIVACY POLICY

A. A Background Of Facebook

Facebook was founded in 2004 and was one of the first, if not *the* first, social media to gain widespread use across the world.[37] Facebook states that its "mission is to make the world

[31] *5 Social Media Strategies to Deter Burglary, Theft*, *supra* note 29.
[32] *Burglary Ring Targets Facebook Users in New Hampshire*, NECN, Sept. 10, 2010, http://www.necn.com/09/10/10/Burglary-ring-targets-Facebook-users-in-/landing.html?blockID=307943&feedID=4206.
[33] *Id.*
[34] *5 Social Media Strategies to Deter Burglary, Theft*, *supra* note 29.
[35] Paul Bentley, *Scammed Facebook Users Lose Insurance Claims Because They Post Too Much Information Online*, DAILY MAIL, Aug. 23, 2012, *available at* http://www.dailymail.co.uk/news/article-2192377/Scammed-Facebook-users-lose-insurance-claims-post-information-online.html (last updated Aug. 24, 2012).
[36] Waters, *supra* note 26.
[37] *Key Facts*, FACEBOOK, http://newsroom.fb.com/Key-Facts (last visited Nov. 24, 2012).

more open and connected."[38] Facebook has become a single platform for a variety of uses; according to the site, people use Facebook "to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[39] Facebook is also used by both new and established businesses to connect with current customers, to attract new customers, and to advertize products and sales, and these benefits are actively promoted by Facebook itself.[40]

Facebook has experienced steady, worldwide growth since its inception. It surpassed ten million users in the U.S. in November 2006, and has since hit that mark in the U.K. (April 2008), France (January 2009), Spain (May 2009), and Germany (November 2009).[41] According to Nielsen, Facebook overtook MySpace as the most popular social media site in 2009.[42] In April 2010, a study revealed that, despite being based in the U.S., Facebook is more popular in Italy than in any other country around the world; the English-speaking countries U.S., U.K., and Australia are numbers two, three, and four, respectively.[43] Facebook also topped Google-owned Orkut as the most-visited social network site in Brazil in 2011.[44] As of September 2012, Facebook has an average of 584 million active users on its website daily, and 604 million active users of its mobile products each month.[45] With one billion active users as of October 2012, approximately eighty-one percent of which are located outside the U.S. and Canada, Facebook is also arguably the biggest and most influential social media website in the world.[46]

---

[38] *Id.*
[39] *Id.*
[40] *Facebook for Business*, FACEBOOK, https://www.facebook.com/business/overview (last visited Nov. 25, 2012).
[41] Nielsen, *Global and Social: Facebook's Rise Around the World*, NIELSEN WIRE (May 17, 2012), http://blog.nielsen.com/nielsenwire/global/global-and-social-facebooks-rise-around-the-world/.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Key Facts*, *supra* note 37.
[46] *Id.*

B. Facebook's Privacy Policy

Privacy has been a concern with Facebook since its birth. In 2012, Facebook creator and CEO, Mark Zuckerberg, stated that "[Facebook performs] privacy access checks literally tens of billions of times each day to ensure [that it is] enforcing that only the people you want see your content. These privacy principles are written very deeply into [Facebook's] code."[47] When a user signs up for a Facebook account, the user must first agree to the site's Terms and must confirm that the user has read the Data Use Policy.[48] These policies state, *inter alia*, that some information, including photos and status updates, may be made available to the public, even if this is not intended by the original poster.[49] Studies show, however, that a majority of internet users do not read the fine print when signing up for services such as Facebook.[50] In fact, Facebook's Terms alone consist of 4,579 words, or over six, single-spaced pages when transferred to a Word document – too long for most users to read, especially those eager to start using the product.[51] Furthermore, likely unbeknownst to many users, when signing up for a Facebook account, a user agrees to make certain information public, unless the user actively changes this setting. Facebook considers the following information public: name, gender, username, user ID (or account number), profile picture, cover photo, and the user's networks

[47] Mark Zuckerberg, *Our Commitment to the Facebook Community*, THE FACEBOOK BLOG (Nov. 29, 2011, 12:39 PM), http://blog.facebook.com/blog.php?post=10150378701937131.
[48] FACEBOOK, www.facebook.com (last visited Nov. 26, 2012).
[49] *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms ("When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).").
[50] *Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, CONSUMER REPORTS MAGAZINE, June 2012, *available at* http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm; Rebecca Smithers, *Terms and Conditions: Not Reading The Small Print Can Mean Big Problems*, The Guardian (May 11, 2011), http://www.guardian.co.uk/money/2011/may/11/terms-conditions-small-print-big-problems (only seven percent of people in the U.K. read the full Terms and Conditions when making a product or service purchase online).
[51] *Statement of Rights and Responsibilities*, *supra* note 49.

(i.e., where the user went to school, where the user works or used to work, etc.).[52] Until a user changes this setting, this information is automatically made public to everyone.[53]

Facebook's attempts to educate users about its privacy settings do not end with forcing users to agree to its Terms. When a new Facebook user creates an account, the user is first directed to a welcome page on which "Get to know your privacy settings" is the second item in a list of several suggested actions for the new user.[54] The "Privacy Tour" informs new users that it is possible to control the audience for posts made by the user, but provides little additional details. Instead, the user can click on a link to "learn more," which redirects the user to Facebook's Help Center[55] – a confusing web of information and policies that even this author, a Facebook member since 2004, has difficulty navigating.

After much controversy,[56] Facebook's default privacy setting allows a user's posts and photos to be viewable by both the user's friends and all friends of each of the user's friends.[57] Although this default setting does not automatically make users' information entirely public, it can quickly lead to broad dissemination of private information. For instance, if a user posts information for his ten friends to see and each of his friends has one hundred friends, then a post intended for ten would instead be visible by one thousand people under Facebook's default privacy settings.

---

[52] *Advanced Privacy Controls: What is Considered "Public Information?"*, FACEBOOK, http://www.facebook.com/help/260276693997558/#!/help/?faq=167709519956542.
[53] *Id.*
[54] This author confirmed this process by using a fake name to create a new Facebook profile on November 26, 2012.
[55] *Help Center*, FACEBOOK, www.facebook.com/help.
[56] Facebook has come under fire multiple times during its short lifetime for its changing default settings with respect to various privacy issues.
[57] Although this author was unable to find a source indicating that this is Facebook's default setting, the author confirmed this fact when she created a new Facebook account on Nov. 26, 2012.

Furthermore, Facebook provides "simple and powerful tools" that are available to users to protect themselves when using the site.[58] A user can apply a single privacy setting to all posts, making them viewable by the public, only friends, only the user, or a custom group.[59] Moreover, before a user hits enter to publish information on Facebook, the user can choose the audience to which he or she wishes to make that information available.[60] This action is made easy for the user: a globe icon indicates that the post is for the public, an icon of two people indicates that the post is for just the user's Facebook friends, a padlock icon indicates that the post is just for the user, and a bolt icon allows the poster to set a custom audience for the post.[61] The same tools allow a user to control the privacy on their entire Facebook page, or Timeline.[62] A user's Facebook account will remember the last privacy setting used and will use that setting for subsequent posts unless manually changed.[63] This is not necessarily true, however, when using Facebook via a mobile device.[64] Furthermore, a recent Consumer Reports study found that nearly thirteen million Facebook users have never set the privacy controls on their Facebook account and are unfamiliar with Facebook's privacy tools.[65]

Additionally, although a Facebook user can control the audience of the content he or she posts, the user cannot easily control the audience that can see a photo or post published by someone else in which the user is "tagged." For example, if User A posts a photo and "tags" User B in the photo, if User A's privacy settings are such that the photo is available to be viewed

---

[58] *Safety and Privacy*, FACEBOOK, http://newsroom.fb.com/Safety-and-Privacy (last visited Nov. 24, 2012).
[59] *Basic Controls: Where Are My Privacy Settings?*, FACEBOOK, http://www.facebook.com/help/325807937506242/.
[60] *Id.*
[61] *Sharing and Finding You On Facebook*, FACEBOOK, http://www.facebook.com/#!/about/privacy/your-info-on-fb; *How Privacy Works When You Share: Can People See Who I'm Sharing With?*, FACEBOOK, http://www.facebook.com/help/260276693997558/#!/help/459934584025324/.
[62] *Sharing and Finding You On Facebook*, *supra* note 61.
[63] *Privacy Basics: What's The Default Audience For Things I Share?*, FACEBOOK, http://www.facebook.com/help/260276693997558/.
[64] *Id.*
[65] *Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, *supra* note 50.

by the public, then anyone can view the photo, even if User B's account is set to limit views by only User B's Facebook friends.[66] Likewise, if User B posts a status on Facebook, and User A comments on B's status, the public will then see User B's status because A's comment will be made available to the audience that A has chosen.[67] This may result in wider dissemination of information than intended, as twenty-eight percent of Facebook users share all or almost all of their photos and posts with more than just their Facebook friends.[68] Considering the growing use of social media and the increasing sophistication of those inclined to use social media for illegitimate means, one must consider whether current laws adequately address the potential harms arising from disseminating private information of social media users.

III. BACKGROUND OF PRIVACY LAW IN THE UNITED STATES

A. General Background

Privacy is an essential and highly-regarded concept to American society. In attempting to define the importance of the right of privacy, authors Ellen Alderman and Caroline Kennedy posited that, "[w]hy we as Americans so cherish our privacy is not easy to explain. . . Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized."[69] In the U.S., an invasion of privacy is recognized as injurious because "the right to privacy is an integral part of our humanity."[70]

---

[66] *When I Share Something, How Do I Choose Who Can See It?*, FACEBOOK, http://www.facebook.com/help/260276693997558/#!/help/?faq=120939471321735.
[67] *Id.*
[68] *Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, *supra* note 50.
[69] LORI B. ANDREWS, EL AL., GENETICS: ETHICS, LAW & POLICY 787 (2010) (citing ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xii-xiii (1995), available at http://books.google.com/books?id=OFK4bI50kgcC&pg=PT12&lpg=PT12&dq=%22caroline+kennedy%22+%22right+to+privacy,+it+seems,+is+what+makes+us+civilized%22&source=bl&ots=9s8gMsHUe0&sig=chKfG74BSMQQBTWA4alI0iUvRRI&hl=en&sa=X&ei=BpOJUd-eCe_L0gH044GIAg&ved=0CFMQ6AEwBA).
[70] Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998); 62A AM. JUR. 2D. *Privacy* § 1 (2013).

Unlike other areas of law, there is no single comprehensive, substantive act or group of laws that govern the right of privacy, and the right is not explicitly enumerated in the U.S. Constitution. As a result, there is disagreement over the nebulous boundaries of the right of privacy. As early as 1890, legal scholars – including eventual Supreme Court Justices Samuel Warren and Louis Brandeis – began to recognize this right.[71] Warren and Brandeis sought to determine "whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[72] Decades later, in his dissenting opinion in *Olmstead v. United States*, Justice Brandeis wrote that,

> as against the government, the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[73]

The Supreme Court first explicitly recognized a Constitutional right of privacy in 1965 in *Griswold v. Connecticut*.[74] Throughout the twentieth century, recognition of the right of privacy grew: by 1964, at least thirty states recognized a right of privacy, and, by 1971, nearly all U.S. jurisdictions recognized the right.[75] Today, this area of law is a patchwork of acts, statutes, and common laws from various areas in the legal field, which together create a right of privacy in nearly all – if not all – U.S. states.

In general, the right to privacy is the expectation that information – including but not limited to information about a person's private affairs and actions, photos, and video – provided

---

[71] *See, e.g.*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).
[72] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890).
[73] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[74] Thomas B. Kearns, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy* Concerns, 7 WM. & MARY BILL RTS. J. 975, 978-79 (1999) (citing Griswold v. Connecticut, 381 U.S. 479 (1965)).
[75] Cox Broad. Corp. v. Cohn, 420 U.S. 469, 488 (1975) (citing WILLIAM L. PROSSER, LAW OF TORTS 804 (4th ed. 1978)).

in a private setting will not be made public, and prevents others from intruding on that right.[76] The right to privacy affords a person the ability to choose who is privy to personal information, and who they wish to exclude.[77] The right also grants persons physical privacy in their person and personal spaces.[78] The law recognizes information to be private when "well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity."[79]

There are two aspects of the right of privacy: (1) a constitutional right of privacy, which protects persons against unlawful government invasion, and (2) a general private right of privacy, which exists primarily in tort law and protects against invasions by non-government actors.[80] Although not explicitly laid out in the U.S. Constitution,[81] the Supreme Court has found that the right of privacy against governmental intrusion is a fundamental constitutional right.[82] This right is one of the penumbra of rights afforded by the Constitution.[83] The Fourth Amendment protects the privacy of an individual against unwarranted government search and seizure.[84] The Court has also held that a person's "liberty," as protected by the Due Process Clause of the Fourteenth Amendment, constitutes, *inter alia*, "a right of personal privacy, or a guarantee of certain areas or zones of privacy."[85] Courts have not laid out the exact metes and bounds of this constitutional protection, but the Supreme Court has held that several individual

---

[76] 62A AM. JUR. 2D. *Privacy* § 1 (internal citations omitted).
[77] *Id.*; *see also* Zellinger v. Amalgamated Clothing, 683 So.2d 726, 732 (2d Cir. 1996) (citing Easter Seal Soc'y For Crippled Children & Adults v. Playboy Enters., Inc., 530 So.2d 643, 646 (4th Cir.1988)).
[78] Kearns, *supra* note 74, at 978-79.
[79] 16B AM. JUR. 2D *Constitutional Law* § 650 (2013) (citing Int'l Fed'n of Prof'l & Technical Eng'rs v. Superior Court, 165 P.3d 488 (Cal. 2007)).
[80] 16B AM. JUR. 2D *Constitutional Law* § 650.
[81] Roe v. Wade, 410 U.S. 113, 152 (1973).
[82] *See, e.g.*, Roman Catholic Bishop v. Superior Court, 42 Cal. App. 4th 1556, 1567 (Cal. Ct. App. 1996) (citing *Griswold*, 381 U.S. at 484-86).
[83] *Griswold*, 381 U.S. at 483; *see also* 16A AM. JUR. 2D *Constitutional Law* §§ 417, 651.
[84] U.S. CONST. amend. IV.
[85] U.S. CONST. amend. XIV, § 1; Roe v. Wade, 410 U.S. 113, 152 (1973); *see also* 16B AM. JUR. 2D *Constitutional Law* § 650 (citations omitted).

rights, including those related to marriage and procreation, are to be protected.[86] Furthermore, the Constitution protects privacy only in instances where there is an expectation of privacy.[87] As with other federal rights, the states are permitted to provide citizens with broader privacy protection than that bestowed by the Constitution.[88] In fact, state courts have not shied away from protecting individuals from "highly offensive intrusions" into their private lives.[89]

While the Constitution protects an individual's privacy from intrusion by the government, it does not, however, expressly protect a person's privacy from other individuals.[90] Rather, that area of privacy law manifests in state tort law.[91] Under tort law, an individual is subject to liability for the harm that results from invading the right of privacy of another individual.[92] Invasion of the right of privacy can occur in four main ways: (1) unreasonable intrusion upon one's seclusion, (2) appropriation of an individual's name or likeness, (3) public disclosure of private information, and (4) publication that unreasonably places an individual in a false light before the public.[93] Each of these privacy torts can be applied to invasions of privacy on the internet, especially those involving social media sites, but none adequately protect social media users.

---

[86] Carey v. Population Svcs., Int'l, 431 U.S. 678, 684 (1977) (citing Loving v. Virginia, 388 U.S. 1, 12 (1967) (marriage); Skinner v. Oklahoma, 316 U.S. 535, 541-542 (1942) (procreation); Eisenstadt v. Baird, 405 U.S. 438, 453-54 (White, J., concurring) (contraception); Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (family relationships); Pierce v. Soc'y of Sisters, 268 U.S. 510, 535 (1925) (child rearing and education)) (additional citations omitted).

[87] 15B AM. JUR. 2D *Computers and the Internet* § 24 (2013).

[88] 16B AM. JUR. 2D *Constitutional Law* § 654 (citing State v. Mariano, 114 Haw. 271 (Ct. App. 2007)

[89] George B. Delta & Jeffrey H. Matsuura, LAW OF THE INTERNET § 9.01 (2013) (citing PROSSER, *supra* note 75, at § 117).

[90] 16B AM. JUR. 2D *Constitutional Law* § 650 (citing Jenkins v. Rock Hill Local School Dist., 513 F.3d 580 (6th Cir. 2008)); 62A AM. JUR. 2D *Privacy* § 2.

[91] 16B AM. JUR. 2D *Constitutional Law* § 650; 62A AM. JUR. 2D *Privacy* § 2 (citing Prudential Ins. Co. of Am. v. Cheek, 259 U.S. 530 (1922); Katz v. U.S., 389 U.S. 347 (1967)); *see* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 546 appx. (2013) (listing twenty-eight separate privacy statutes)..

[92] Restatement (Second) of Torts § 652A (2012).

[93] *Id.* These four wrongs are the four main forms of privacy tort law; others may appear in court opinions or legal scholarship. *Id.* § 652A cmt. b.

The first tort, intrusion of one's seclusion, occurs when an individual "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . ."[94] In order for liability to attach, the intrusion must be highly offensive to a reasonable person.[95] The intrusion can be physical, can occur using one's senses, such as by spying into one's house, or some other form of investigation or examination, such as opening another's mail.[96] The intrusion itself makes the act tortious, and what the offender does with the private information he procures is irrelevant.[97]

The second privacy tort arises when one appropriates another's name or likeness for his use or benefit.[98] This tort protects an individual's right to his own identity.[99] This tort typically occurs when one's name or likeness is used, without permission, in advertising or for some commercial purpose, but is typically not limited to commercial appropriation.[100]

The third privacy tort occurs when one invades and publicizes a matter concerning another's private life.[101] Such publication, however, must be highly offensive to a reasonable person.[102] Liability also only attaches if the information is not of legitimate concern to the public.[103] Publication of the information must be more than a mere communication to another; there must be communication to the public at large or to many people so that the information is "substantially certain" to become public knowledge.[104]

---

[94] *Id.* at § 652B.
[95] *Id.*
[96] *Id.* at § 652B cmt. b.
[97] *Id.*
[98] Restatement (Second) of Torts § 652C.
[99] *Id.* at § 652C. cmt. a.
[100] *Id.* at § 652C. cmt. b (noting that some states do limit this right to use in commercial contexts only).
[101] *Id.* at § 652D.
[102] *Id.*
[103] *Id.*
[104] Restatement (Second) of Torts § 652D cmt. a.

One is liable under the final privacy tort, false light, when he publicly reveals information that places the injured party in a false light before the public.[105] Under this tort, the information must be untrue, and must place the injured party in a false light that is highly offensive to a reasonable person.[106] The actor must also have had knowledge of the information's falsity or he must have acted in reckless disregard in publicizing the information and placing the other in a false light.[107] Publication of the information must meet the same requirements as for the tort of publicity of one's private life.[108] This tort is distinguishable from defamation.[109]

In addition to the Constitution and tort law, privacy law is governed by statute in some areas of the law. In the healthcare field, for example, the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of individuals' health-related information and has built-in privacy controls.[110] Similarly, the Gramm-Leach-Bliley Act requires transparency from financial institutions regarding their information collection practices and restricts the use of personal information.[111] Such statutes clearly define privacy law as it applies in certain legal fields, which would otherwise be subject to the arguably unpredictable, uncertain, and limited privacy protections under the Constitution and tort law. This paper proposes doing the same in the social media sphere.

---

[105] *Id.* at § 652E.
[106] *Id.* at § 652E, cmt. a.
[107] *Id.* at § 652E.
[108] *Id.* at §§ 652E cmt. a, 652D cmt. a.
[109] *Id.* at § 652E cmt. b.
[110] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at 45 C.F.R. pts. 160, 164 (2011)); Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SVCS. (May 2003), at 1-2, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.
[111] Gramm-Leach-Bliley Act, Pub.L. 106–102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6809); *Gramm-Leach-Bliley Act*, BUREAU OF CONSUMER PROT., http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act (last visited Feb. 12, 2013). The Fair Credit Reporting Act (FCRA) also prohibits a financial institution from using or sharing a consumer's information unless that consumer "opts out" of the privacy protection. Fair Credit Reporting Act, 15 U.S.C.A. § 1681 et seq.

B. Privacy On The Internet

The development of the internet created a new and constantly evolving realm of privacy law. Particular complex issues arise here because dissemination of personal data is an inherent and necessary aspect of social media sites, but threats to privacy are exacerbated by the increasing prevalence and use of social media sites.[112] While the U.S. Constitution's privacy protections, as briefly outlined above,[113] protect an internet user from unwarranted government intrusion with respect to the internet, these protections do not extend to an individual's privacy online from other individuals.[114] Rather, an individual's online privacy is governed by tort law, as well an amalgamation of statutes, which together do not fully define this new realm of the law.

While well-developed statutes, such as the aforementioned HIPAA,[115] govern privacy in other areas of the law, there is no single statute that clearly defines one's right to privacy from private individuals with respect to information on the internet. There are several federal statutes that provide individuals with protection for internet-related information. The Electronic Communications Privacy Act (ECPA), for example, is one of the broadest statutes that applies to today's electronic environment.[116] The ECPA covers both voice and data communications, as well as electronically-stored communications, and prohibits the interception of, access to, and disclosure of such communications.[117] In recent years, however, the EPCA has been scrutinized due to its amendment by the Patriot Act,[118] which broadened the scope of permissible

[112] *See supra* Part I.A.
[113] *Supra* Part III.A.
[114] 62A AM. JUR. 2D *Privacy* § 2. Although the issue of individuals' right to privacy from unwanted government intrusion is also currently of public concern, it is beyond the scope of this paper.
[115] *Supra* Part III.A.
[116] 18 U.S.C.A. §§ 2510-22, 2701-11 (2012).
[117] *Id.*; Delta & Matsuura, *supra* note 89, at § 9.01.
[118] USA Patriot Act (2001), Pub. L. No. 107-56, 115 Stat. 272.

surveillance of electronic communications.[119] Furthermore, the Children Online Privacy Protection Act (COPPA) regulates the collection of data related to internet users under the age of thirteen.[120]

The Fair Credit Reporting Act (FCRA) regulates the ability of financial institutions to share customer's credit-related data with its affiliates.[121] Specifically, the FCRA requires that financial institutions provide customers with disclosure, notice, and an opt-out option before such information is shared.[122] Although the FCRA was originally enacted in 1970, well before widespread use of the internet, it is applicable more today than ever due to widespread online banking and the ease with which data miners can collect and process electronic information. While the FCRA's application in the internet context is largely untested, the Federal Trade Commission, the primary enforcer of the FCRA, filed a federal complaint against data collector Spokeo, Inc. alleging violations of the FCRA.[123] Ultimately, however, the parties reached a settlement and FCRA rules were left unlitigated in the internet context.[124] Because this patchwork of regulations has not stemmed the flow of harms resulting from inadvertent disclosure of private information on social media sites, such as Facebook, this paper proposes rules that could preemptively eliminate unintended disclosure of private information.

[119] Delta & Matsuura, *supra* note 89, at § 9.01.
[120] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 *et seq.*; Delta & Matsuura, *supra* note 89, at § 9.03.
[121] 15 U.S.C. § 1681 et seq. (1970).
[122] 15 U.S.C. § 1681.
[123] Complaint at 3-11, United States v. Spokeo, Inc., No. 2:12-cv-05001 (C.D. Cal. 2012), *available at* http://www.ftc.gov/os/caselist/1023163/120612spokeocmpt.pdf.
[124] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), *available at* http://www.ftc.gov/opa/2012/06/spokeo.shtm.

IV. PRIVACY LAW IN THE FACEBOOK CONTEXT

A. Application of Privacy Law To Individuals' Facebook Use

Privacy torts are Facebook users' principal source of legal recourse against individuals who invade their privacy online. The four relevant privacy torts are intrusion of solitude, appropriation of one's name or likeness, public disclosure of private facts, and false light.[125] While both the tort of appropriation of one's name or likeness and the false light tort can arise from the use of social media, the privacy torts of intrusion into one's privacy and the public disclosure of private facts are most relevant where a Facebook user views and/or publicizes another user's private information without his permission.

The latter two torts both require an intrusion of *private* information. Whether information is private, in turn, depends on whether a user has a reasonable expectation of privacy. Thus, whether a cause of action is available depends on whether users have a reasonable expectation of privacy with respect to information posted on Facebook.

Social media websites, such as Facebook, inherently are information-sharing forums where users are expected to share personal information.[126] As a result, Facebook users often knowingly and deliberately share personal information on the site.[127] It is unclear, however, when this sharing of private information crosses over to the public sphere because a user no longer maintains a reasonable expectation of privacy under the law. If information is shared with two people, is it public? What if it is shared with ten close friends? Or one hundred?[128]

[125] Restatement (Second) of Torts § 652A.
[126] *Social Media Definition*, *supra* note 11.
[127] Delta & Matsuura, *supra* note 89, at § 9.03.
[128] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920-21 (2005).

To determine whether a Facebook user has a reasonable expectation of privacy in information he or she posts on Facebook some suggest engaging in an empirical analysis.[129] This analysis examines the probability that the information would have become public had it not been for the alleged intruder's actions.[130] If it is likely that the information would be disclosed or become known by many people in the public, then the information is public and not protected by privacy tort law.[131] If, for example, the Facebook user's account settings are set to "Public" so that the user's profile can be viewed by any other Facebook user, then it is highly likely that the information would be disclosed to the public and thus the information is not considered private under the law. If, however, the Facebook user's profile settings are set to the mildly restrictive "Friends of Friends" setting, there is a lower chance that the information would be viewed by the public and the user may thus have recourse for intrusion of privacy under tort law. Finally, if the user's settings are set so that only his friends may view his profile, he is more likely to have recourse in tort law.

The line between public and private information has been drawn by courts in non-internet related cases. In *Kubach v. Multimedia WMAZ, Inc.*, the plaintiff, a man with AIDS, agreed to appear on local television to discuss the disease.[132] Because Mr. Kubach had only told sixty of his close friends and family about his condition, the television station agreed to digitize his face so that it was not recognizable to viewers.[133] In this case, the Georgia appellate court upheld the lower court's finding that, although Mr. Kubach revealed his condition to dozens of people, he did not reveal his AIDS diagnosis with the public and therefore had an expectation of privacy in

[129] *Id.* at 918.
[130] *Id.*
[131] *Id.*
[132] Kubach v. Multimedia WMAZ, Inc., 443 S.E.2d 491, 493 (Ga. Ct. App. 1994).
[133] *Id.*

that fact.[134] If a Facebook user can thus disclose personal information to dozens of his close family and friends and still hold a reasonable expectation of privacy in that information, then he may have recourse under tort law for invasion of privacy if Facebook's default settings do not provide access to such information beyond the user's friends.

Courts in other cases, however, have held that disclosure to others negates any expectation of privacy. Prior to the publication of consumer advocate Ralph Nader's book Unsafe at Any Speed, General Motors (GM) attempted to discredit and intimidate Nader.[135] To do so, GM employees posed as employees of a different company interested in hiring Nader, and interviewed Nader's close friends and family about his private views and beliefs on religion, politics, and other personal matters.[136] In finding against Nader, the court held that, although the information uncovered was of a personal nature, GM did not invade Nader's privacy because he had previously disclosed the information to others, thereby running the risk of further disclosure.[137] In cases that follow the *Nader* decision, courts find that "numerous disclosures . . . introduce[] the private fact . . . into the public domain such that he could not have had any reasonable expectation that this fact remained a private matter."[138] Thus, because most Facebook users have at least one – if not dozens – of Facebook friends, courts that follow the *Nader* line of thinking will find that any disclosure on Facebook is a public disclosure and that all information ceases to be private the moment it is posted to Facebook, regardless of the user's privacy settings. Changing the default privacy settings, however, would nonetheless help

[134] *Id.* at 500; *see also* Y.G. v. Jewish Hosp., 795 S.W.2d 488 (Mo. Ct. App. 2008) (holding that, when a couple disclosed their participation in in vitro fertilization treatment to only hospital employees and one of the plaintiff's mothers, the couple held a reasonable expectation of privacy in this fact).
[135] Nader v. Gen. Motors Co., 25 N.Y.2d 560, 565 (N.Y. 1970).
[136] *Id.*
[137] *Id.* at 570-71.
[138] *Kubach*, 443 S.E.2d at 502 (Andrews, J., dissenting).

decrease the risk that private information will be disseminated more broadly than intended in the first instance, thereby decreasing the risk of harm.

Consequently, the line between public and private disclosure for purposes of privacy law is not clear.[139] As a result, whether or not a Facebook user will have recourse under tort law for invasion of privacy on Facebook is unclear and unpredictable. If a plaintiff's Facebook settings are set to the restrictive "Friends Only" setting, she may not have a reasonable expectation of privacy in the information she posts to the site. Furthermore, if a user's Facebook settings allow the entire public to view her profile, but she did not know that her account was on that setting, she will not have recourse under tort law, even if she expected the information to remain private and viewable to only her friends. Moreover, because social media users voluntarily submit information to other users, courts generally have recognized a reduced level of expectation of privacy with respect to social media activity.[140] As a result, tort law is insufficient to protect Facebook users from invasion of privacy.

B. The Current Law Necessitates Additional Protections Of The Privacy Of Social Media Users

Because tort law provides insufficient protection of Facebook users' privacy, additional safeguards are necessary. Facebook has an average of 584 million active users on its website daily, and 604 million active users of its mobile products each month.[141] Although the private information of these millions of users may be protected when shared outside of the internet, they are left with little recourse if their privacy is invaded on Facebook.

---

[139] *See* Strahilevitz, *supra* note 128, at 946.
[140] *See, e.g., In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 111, 130 (E.D. Va. 2011) (a Twitter user does not have a reasonable expectation of privacy in his IP address or related data once he creates his Twitter account); People v. Harris, 945 N.Y.S.2d 505 (City Crim. Ct. 2012) (a Twitter user has no expectation of privacy once he creates his account); CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 22:11 (2012).
[141] *Id.*

Facebook users have demonstrated their concern with the site's privacy settings. In 2009, when Facebook modified its Terms of Service, including its privacy settings, the site's users protested.[142] Shortly thereafter, Facebook reverted to its prior terms.[143] Most recently, in late 2012, Facebook announced that it would overhaul its privacy controls.[144] Although many argue that Facebook's constant changes to its site, settings, and terms make it difficult for users to ensure that they keep up with the current privacy controls,[145] Facebook argues that it does so merely to keep up with its user's demands for improved privacy.[146] These outcries from Facebook users also indicates users' awareness of privacy concerns that attach to the use of Facebook, as well as their expectation of *some* level of privacy with such use. In fact, a 2000 report by the Federal Trade Commission (FTC) found that ninety-two percent of U.S. citizens are concerned about the privacy of their personal information online,[147] and a 2002 study by Harris Interactive found that sixty-three percent of adults surveyed feel that the existing privacy law is inadequate to protect against privacy invasions.[148] More than a decade after these surveys, these numbers have undoubtedly increased.

Critics of Facebook also deem the site's privacy settings inadequate.[149] Privacy advocates have also criticized social media sites in general regarding privacy concerns and the lack of clarity between public and private information.[150] The FTC has also expressed its

---

[142] Jessica E. Vascellaro, *Facebook's About-Face on Data*, WALL. ST. J. , Feb. 19, 2009, at B8, *available at* http://online.wsj.com/article/SB123494484088908625.html.
[143] *Id.*
[144] Doug Gross, *Facebook to Overhaul its Privacy Controls*, CNN (Dec. 12, 2012), http://www.cnn.com/2012/12/12/tech/social-media/facebook-privacy-changes/index.html?hpt=hp_bn5.
[145] *Id.* (analyzing user comments following article).
[146] Geoffrey A. Fowler & Amir Efrati, *Facebook Revamps Privacy Controls*, WALL ST. J., Aug. 25, 2011, at B6, *available at* http://online.wsj.com/article/SB10001424053111903461304576526623359582548.html.
[147] *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, FED. TRADE COMM'N (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
[148] *Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/survey/ (last visited May 1, 2013).
[149] Ben Worthen, *Facebook's Settings Don't Quell Critics*, WALL ST. J., May 27, 2010, at B1, *available at* http://benton.org/node/36352.
[150] Delta & Matsuura, *supra* note 89, at § 9.05.

growing concerns of the lack of privacy controls available to internet users, and released privacy guidelines for websites in 2012.[151] In fact, subsequent to the release of its report, the FTC filed a suit against Facebook alleging that the site deceived consumers by allowing information that they believed to be private be shared and made public.[152] Facebook eventually settled, agreeing to improve its privacy settings.[153] Despite these steps, the existing framework is inadequate and additional measures are needed to ensure the privacy safety of the users of Facebook and other social media platforms.

C. Proposed Measures To Ensure Privacy Of Social Media Users

In order to improve the privacy of social media users, several steps should be taken. First, because a frequent complaint among privacy advocates is that Facebook's privacy settings are difficult to navigate,[154] a law should be passed to make it mandatory that Facebook and other social media website's default privacy settings afford the user the greatest level of protection.

In light of studies finding that nearly thirteen million Facebook users have never set the privacy controls on their Facebook account and are unfamiliar with Facebook's privacy tools, changing the default setting would be impactful.[155] Indeed, this study indicates that approximately thirteen million users will use whatever default privacy settings are in place.[156] Thus, for these individuals, making default privacy settings more stringent would both decrease

---

[151] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers*, FED. TRADE COMM'N (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; Matt Jarzemsky, *Disney's Playdom Settles with FTC*, WALL ST. J., May 13, 2011, at B6, *available at* http://online.wsj.com/article/SB10001424052748703730804576319284000370692.html.
[152] Complaint, In Re Facebook, Inc., No. C-4365 (U.S. FTC Jul. 27, 2012), FTC File No. 0923184, *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf.
[153] Agreement Containing Consent Order, In Re Facebook, Inc., No. C-4365 (U.S. FTC Aug. 10, 2012), FTC File No. 0923184, *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[154] Gross, *supra* note 144.
[155] *Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, *supra* note 50.
[156] *Id.*

the risk of users unwittingly disseminating private information and would increase the chances of a recovery for privacy torts.[157]

Because information sharing is the basis for Facebook, it and other social media companies likely will not be in favor of such a law. With more stringent default settings in place, however, users would maintain the freedom to share information broadly if they choose to do so (and would thereby knowingly accept that risk that private information would be disclosed), while those who do not affirmatively accept that risk by changing their privacy settings would be protected. Such a law would also have educational value: More stringent default settings may make users think twice before changing the setting or posting the private information at all.

Finally, education of social media users about popular sites' privacy controls will improve their ability to control the dissemination of private information. In fact, in the wake of the recent Facebook privacy settings changes, several news outlets, including CNN and the Wall Street Journal, provided readers with a guide to understanding the new privacy controls.[158] This is especially important since many Facebook users often do not realize that what they share online is being shared with the world.[159] The government and users alike should also implore Facebook and other social media sites to provide users with guides on using the site's privacy controls and to make the mechanisms for changing the privacy settings straightforward and easy for the average user to understand and utilize.

---

[157] As discussed above, if Facebook's default privacy settings allow sharing of information with friends only, a user with a small number of friends may be able to recover under *Kubach* and its progeny may have a reasonable expectation of privacy. However, current default settings remain in place, a user who shared private information with friends would also unknowingly share that information hundreds of friends of friends and a court would be more likely to find the information was made public.

[158] Lorrie Faith Cranor, *A Guide to Facebook's Privacy Options*, WALL ST. J. (Mar. 10, 2013, 3:46 pm), http://online.wsj.com/article/SB10001424127887324880504578300312528424302.html; Gross, *supra* note 144; Matthew Lynley, *Managing Your Privacy with Facebook's New News Feed*, WALL ST. J. (Mar. 8, 2013, 12:04 pm), http://blogs.wsj.com/digits/2013/03/08/managing-your-privacy-with-facebooks-new-news-feed/.

[159] Cranor, *supra* note 158.

Finally, and arguably most importantly, social media users need to be educated about the privacy issues that attach to internet and social media use. This includes, but is not limited to, what privacy is, why it is important, how disclosure occurs, and how the user can control the unwanted dissemination of private information. This education can come from the government, non-profit organizations, or from social media companies themselves. Pursuant to the high percentage of college students who participate in Facebook and social media, some universities now educate students on safely using social networking sites.[160] In fact, in a recent study, a twenty-five percent of social media users said they falsified information in their profiles to protect their identity, up from ten percent a mere two years ago.[161] This education will hopefully encourage the public to become more active participants in protecting themselves when using the internet and social media sites. Nevertheless, in light of the fact that it is likely impossible to education everyone, a system under which users must affirmatively opt-in to making private information public should be legally required.

CONCLUSION

Over one hundred years ago, in recognizing the need for privacy protection in response to the emergence of newspaper circulation and mass media, Justices Warren and Brandeis observed that "[p]olitical, 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."[162] This has never been more true as the internet and social media make communication and information sharing across the globe possible with the simple stroke of a key.

The right to privacy is engrained in the American consciousness. Although social media users post personal, private information on the public internet, there is still an expectation that

[160] Delta & Matsuura, *supra* note 89, at § 9.03.
[161] *Facebook and Your Privacy: Who Sees the Data You Share on the Biggest Social Network?*, *supra* note 50.
[162] Warren & Brandeis, 4 HARV. L. REV. at 193.

the user will be afforded some level of privacy. Although tort law may theoretically provide a wronged social media user with recourse for invasion of privacy, it is inadequate. Given the widespread use of social media, especially of Facebook, and the general tendency to disseminate private information and potentially high costs, social media companies must take additional measures to safeguard their users. Compelling social media sites to set their default settings at the highest privacy level will help ensure that users do not inadvertently disseminate private information to the public.