October 21, 2013

Privacy Issues in the Age of Social Media M&A

Amy A. Hinkler

Privacy in the Age of Social Media Mergers and Acquisitions

Amy A. Hinkler

INTRODUCTION

> *I'm just an average man/With an Average Life/I work from nine to five/Hey, hey, I'll pay the price/All I want is to be left alone/In my average home/But why do I always feel/I'm in the twilight zone/And I always feel like/Somebody's watching me/And I have no privacy/I always feel like/Somebody's watching me/Tell me is it just a dream?*[1]

With the help of Michael Jackson, Rockwell had one of the biggest pop hits of 1984. The mocking, paranoid voices on the track and Hitchcock-esque video made for a light-hearted hit that made drivers move in their seats and dance in traffic. As this hit was dominating the airwaves across America, "virtual reality" was a concept still at a distance from the human experience. Through the use of computer technology, people could experience an artificial environment that they could partially control.[2] The outcome of actions taken in virtual reality was locked somewhere inside of the IBM or fresh Macintosh; any effect of the simulated experience did not reach back into reality. It was, as defined, *artificial*. Fast-forward to 2013: "Virtual reality" is now just *reality*, and no, it is not just a dream – somebody really is always watching you!

Globally, people use computers, tablets, smart phones, and even eyeglasses[3] to connect to the world through the Internet, and use social media to communicate with friends and family, share photos and videos, follow the news, shop, learn, and so much more. When cork boards

---

[1] ROCKWELL FEAT. MICHAEL JACKSON, SOMEBODY'S WATCHING ME (Motown 1984).

[2] *Virtual Reality Definition*, Merriam-Webster.com, http://www.merriam-webster.com/dictionary/virtual%20reality (last visited March 6, 2013).

[3] Ryan Mac, *No One Is More Excited For Google Glass Than Facebook CEO Mark Zuckerberg*, FORBES.COM, Feb. 21, 2013, 10:09 AM, http://www.forbes.com/sites/ryanmac/2013/02/21/no-one-is-more-excited-for-google-glass-than-facebook-ceo-mark-zuckerberg/ ("While it was undoubtedly informal, the meeting of the minds from two of Silicon Valley's most powerful corporations showed that Facebook was ready to develop for Glass. According to Zuckerberg, Facebook has a team of three engineers, led by a former Google employee, waiting for the product to be shipped to them so they can start building applications.").

moved from the wall to the computer in the late 1970s, it would have required a whopping mental leap to imagine how social media, the millennial descendant of Bulletin Board Systems, would be so integrated into life today. [4]

While people have embraced technology, the Internet, and social media, deep-rooted concerns have also arisen relating to our privacy.[5] Increasingly, people are realizing that information that was once held closely as a piece of their personal identity is now quickly and easily broadcast over the Internet to unknown receivers.[6] There is a resounding sense of over-exposure and loss of control over privacy in identity and personal information being felt around the globe. Vinton Cerf has said "the Internet has created a platform for innovation,"[7] but we have also come to recognize that this incredible platform has "the potential of completely erasing the idea of privacy and anonymity."[8] The rise of the Internet is a fundamental departure from the past.[9] This loss of privacy and anonymity goes beyond what we traditionally would have thought of as "the Internet" – activities on Internet Explorer, Safari, or other Web browser – and

---

[4] Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 Miss. C. L. Rev. 227, 228 (2012) (footnote omitted). ("[T] he social media of the 1980s and early 1990s – known as Bulletin Board Systems (BBSes) – bears little resemblance to the social media of today…Like modern fare, BBSes allowed interactive online dialogue and entertainment…").

[5] Timothy J. Toohey, *Piracy, Privacy, and Internet Openness: The Changing Face of Cyberspace Law*, Understanding Developments in Cyberspace Law, July 2012, at 1, 7 *available at* 2012 WL 2244536. ("Consumers are expressing discomfort with the ads that are the economic lifeblood of many Internet sites, including Facebook.")

[6] *Id.* at 6. (claiming there is "little dispute that the Internet allows for the wide and sometimes uncontrolled dispersal of what in the past would have been private information regarding individuals.")

[7] Vinton G. Cerf – Profile, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, http://www.nist.gov/director/vcat/cerf.cfm (last visited March 5, 2013). ("Widely known as one of the 'Fathers of the Internet,' Cerf is the co-inventor of the architecture and basic protocols of the Internet… [and] serves on the NIST visiting board."). *See also* Robert Terenzi, Jr., *Friending Privacy: Toward Self-Regulation of Second General Social Networks,* 20 Fordham Intell. Proper. Media & Ent. L.J. 1049, 1050 (2010) (citation omitted).

[8] Terenzi, 20 Fordham Intell. Proper. Media & Ent. L.J. at 1052.

[9] Toohey, *supra* note 5, at 5.

into every phone call, text message, debit card swipe, GPS direction, and soon, every glance[10] as our human (and animal[11]) existence increasingly intertwines with the Internet.

Much has been said about government intrusion upon privacy since the First Congress proposed the Bill of Rights in 1789.[12] The focus of this paper, however, is intrusion by private parties, namely, the very social networks and third party associates Internet users blindly entrust private information to.[13] The protections extended to the people in this regard are less clear. The U.S. Constitution provides protection against certain government intrusions.[14] Ten state constitutions expressly declare a right to privacy.[15] The U.S. Constitution does not declare a right to privacy against intrusion by private actors, and to date, the courts have not extended any such interpretation. Congress has created protections, however limited, for certain private information, including financial information,[16] health information, and stored electronic

[10] Mac, *supra* note 2.
[11] Even pets have a social media presence! Dogster and Catster are online havens for pet-parents and their fur-babies to create profiles and connect with other members. *See* Dogster, http://www.dogster.com/dog-community/ (last visited March 6, 2012). *See also*, Catster, http://www.catster.com/cat-community/ (last visited March 6, 2013).
[12] *Primary Documents in American History: The Bill of Rights*, LIBRARY OF CONGRESS, http://www.loc.gov/rr/program/bib/ourdocs/billofrights.html (last visited Mar. 6, 2013).
[13] *See* Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 Stan. Tech. L. Rev. 7, 5 (Jul. 10, 2012) ("Most users click to accept privacy notices and consent declarations without reading or understanding them."). *See also* Jared S. Livingston, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting,* 21 Alb. L.J. Sci. & Tech. 591, 627 (2011) ("[A] recent poll indicates that almost one in every four Facebook users did not even know anything about privacy settings at all.").
[14] *See* U.S. Const. amend. I-X, XIV.
[15] National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/issues-research/telecom/privacy-protections-in-state-constitutions.aspx (listing Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington constitutions as containing express declarations of privacy rights). [hereinafter *NCSL*] *Accord* Fla. Const. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.").
[16] *See* Gramm-Leach-Bliley Act, 15 U.S.C.A. §§ 6801-6809 (West).

communications.[17] Still, the United States is without comprehensive national privacy legislation that protects personal information against intrusion by private commercial entities in the age of social media.[18]

It does not take more than a quick glance around at a subway stop in New York City, where straphangers incessantly swipe and tap at their smartphones, or a Starbucks in Anytown, U.S.A., where patrons are more likely to be accompanied by a laptop or tablet than a cup of coffee, to understand that the Internet is now an essential element of the daily routine. As of December 2012, eighty-one percent of Americans were connected to the Internet.[19] While social media have become deeply embedded in online communication, the laws governing remain abstract and have not evolved with the medium.[20]

Part I of this paper examines social media and its rise to prominence in users' lives;[21] how these "free" programs have become a multi-billion dollar industry; the very notion of information privacy; users' expectations of privacy and protection; as well as concerns emerging from the rise of social media. Part II examines the law as it relates to cyberspace: federal legislation in place to protect social media users' privacy; the role of the Federal Trade Commission ("FTC") in the regulation of social network practices and recent actions taken by the agency; a framework introduced by the White House in 2012, urging regulation; attention

---

[17] *See* Stored Communications Act, 18 U.S.C.A. §§ 2701-2712 (West).
[18] Jonathan D. Frieden, Esq. et al., *Putting the Genie Back In the Bottle: Leveraging Private Enforcement to Improve Internet Privacy*, 37 Wm. Mitchell L. Rev. 1671, 1683 (2011).
[19] Pew Internet & American Life Project, 2012 Post-Election Tracking Survey, conducted Nov. 14, 2012-Dec. 9, 2012, *available at* www.pewinternet.org.
[20] Scott Cleland, *Why U.S. Communications Law Is Obsolete*, DAILY CALLER, Jun. 25, 2012, 5:14 AM, http://dailycaller.com/2012/06/25/why-u-s-communications-law-is-obsolete/.
[21] *See* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship,* 13 J. COMPUTER-MEDIATED COMM., no. 1, art. 11, at 11, 2007, *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html ("Given that SNSs enable individuals to connect with one another, it is not surprising that they have become deeply embedded in users' lives.").

given to the issue by Congress; private causes of action that may be available to aggrieved users and recent cases; efforts that have been made to protect privacy in other parts of the world; and finally, a proposal for effective action in Congress to establish a right and extend adequate protection to Americans. Part III looks at the importance of privacy considerations in mergers and acquisitions ("M&A") of social media organizations and recent trends in technology deals. Specifically, this section examines the recent Facebook acquisition of mobile photography application ("app") Instagram, its successes and its failures with respect to user privacy, and looks to the future of the Facebook-Instagram relationship. Finally, this section proposes best practices for social media in future transactions, as they become more frequent. This paper concludes by discussing what type of regulatory scheme – if any – is best for the U.S. to align itself with other countries, protect those who value their privacy, but also retain the essence of "freedom" that drives innovation and development within our borders; what users can do to protect themselves; and how social media companies can do their part in preventing the need for oppressive regulation.

I. SOCIAL MEDIA

A. *Emergence of Social Networks*

Social network sites are technically defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list or 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."[22] In the laymen's terms, social networks today are Internet-based platforms that allow people to connect to one another for various purposes – business, personal, entertainment, educational, and the list goes on. While the

[22] *Id.* at 2.

term may evoke images of virtual cocktail parties or other networking events, the primary purpose on many of these platforms has not been to meet new people on the Internet, but to maintain relationships that were first established offline.[23]

Facebook's claim to fame may be that it is the world's largest social network with a user base of what amounts to about one-seventh of the world's population,[24] but it certainly was not the first in the modern Internet era. The first social network seemingly akin to those that dominate the industry today was Sixdegrees.com, which launched in 1997 and was functionally similar to other Web-based social networks used today.[25] Other sites in existence at the time allowed users to create a personal profile, list their friends and view each other's lists, but none integrated these functions into one service until Sixdegrees.com did in 1998.[26] The site ultimately did not survive,[27] but it was a sneak peek of what was just around the corner in the new world of online social media, beginning with the founding of MySpace in the fall of 2003[28] and the rapid development thereafter.[29]

Not far behind MySpace, which was popular among high school and college students but open to the public, was the early 2004 launch of Facebook.[30] Initially hosting a closed network

---

[23] *Id.* at 11 (citing Ellison, et. al., *The Benefits of Facebook "Friends": Exploring the Relationship Between College Students' Use of Online Social Networks and Social Capital*. 12 J. COMPUTER-MEDIATED COMM, no. 3, art. 1 (2007), *available* at http://jcmc.indiana.edu/vol12/issue4/ellison.html).

[24] Henderson, *supra* note 4, at 246 ("[It is] remarkable that a seventh of the world's population might soon be using a single online media resource"). *See also* news article announcing Fbook reached 1 billion users

[25] Boyd & Ellison, *supra* note 21, at 4.

[26] *Id.*

[27] *Id.* (citing reasons for SixDegrees' failure).

[28] Alex Williams, *Do You MySpace?*, NEW YORK TIMES, Aug. 28, 2005, *available at* http://www.nytimes.com/2005/08/28/fashion/sundaystyles/28MYSPACE.html?_r=0&pagewanted=print (last visited Mar. 6, 2013).

[29] Boyd & Ellison, *supra* note 21, at 7 (**"**From 2003 onward, many new SNSs were launched.").

[30] *Id.* at 8.

exclusive to Harvard students, Facebook later rolled out to other universities, high schools, corporations, and finally, all citizens of Earth.[31] Early on, the nature of Facebook's "closed" networks that required e-mail addresses at university domains provided a sense of privacy and exclusivity.[32] The apparent "verification" through the requirement of institutional issue e-mail addresses was like a security blanket for users navigating the obscure borders of social networks for the first time.[33]

B. *The Audience*

A recent Pew Research Center survey concluded that sixty-seven percent of Internet users in America are engaged in social networking.[34] Surveying demographic categories of gender, race/ethnicity, education attainment, household income, and urbanity, the results indicate that social media use is fairly evenly spread across all demographic categories, with the exception of age, substantiating the ubiquitous appeal of social media.[35] Women, Hispanics, those with some college education attained, annual household income below $30,000, and urban residents lead all demographic categories in use by a small margin. The greatest margin between the highest and lowest reported use of social media in any category was just nine percent.[36] The most disparate statistics lie in the age category: at the top are Internet users aged eighteen to twenty-nine, eighty-three percent of whom report engagement in social media, and at the bottom are users sixty-five and over, only thirty-two percent of whom report social media use. The greatest drop

---

[31] *Id.*

[32] For example, to join the Tulane University network, a student could register only if they provided a valid @tulane.edu e-mail address.

[33] Boyd & Ellison, *supra* note 21, at 8 ("[U]sers were also required to have university email addresses associated with those institutions, a requirement that kept the site relatively closed and contributed to users' perceptions of the site as an intimate, private community.").

[34] Pew Research Center, *The Demographics of Social Media Users – 2012*, Feb. 14, 2013, *available at* http://pewinternet.org/Reports/2013/Social-media-users.aspx.

[35] *Id.*

[36] *Id.*

in interest and engagement in social media use occurs between users aged thirty to forty-nine, reporting seventy-seven percent social media engagement, and those aged fifty to sixty-four, reporting just fifty-two percent.[37]

Internet users aged thirteen to seventeen were not included in the survey, however, it can be surmised by the tremendous interest of the youngest age group included in the survey coupled with social media policies requiring users affirm that they are at least thirteen years of age[38] that there is significant engagement in social media for Internet users in this age group, and probably younger, given there exists an "iTunes Kids" store with over 240 interactive game apps.[39] Children of today have never known a Web-free world – personal computers became mainstream in American homes in 1995, and Internet use by 1999,[40] around the time now college aged students were in diapers, and long before tweens were even a figment of their parents' imaginations.

C. *Business Models*

To understand the current movement for privacy protection, one must first understand the industry practices that have incited the movement.[41]

---

[37] *Id.*

[38] Frieden et al., *supra* note 18, at 1686 ("Most social network services, such as Facebook, MySpace, and Twitter, prohibit participation by children that are thirteen years of age or under, which makes them generally exempt from the requirements of [the Children's Online Privacy Protection Act].").

[39] ITUNES KIDS, https://itunes.apple.com/us/genre/ios-games-kids/id7010?mt=8 (last visited Mar. 7, 2013).

[40] *E-Commerce Emerges As Fastest-Growing Online Activity and Becomes More Central To Internet Consumer Experience, According To 1999 America Online/Roper Starch Cyberstudy*, TIMEWARNER.COM, Nov. 11, 1999, *available at* http://www.timewarner.com/newsroom/press-releases/1999/11/ECommerce_Emerges_As_FastestGrowing_Online_Activity_11-11-1999.php [hereinafter *AOL Cyberstudy*].

[41] *See* Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building A Social Movement and Creating Corporate Change*, 36 N.Y.U. Rev. L. & Soc. Change 215 (2012) (describing the rise in Internet privacy concerns as a social movement).

"It's free and always will be."[42] Social networking sites like Facebook, itself valued just under $70 billion at the end of January 2013,[43] are valued based upon the number of active users on the network.[44] In lieu of paying the networks a membership fee, users compensate the networks for their services with personal information.[45] Jennifer Stoddart, Privacy Commissioner of Canada, has said these networks have "helped transform personal information into a commodity."[46] Users provide demographic information, data about habits and preferences, and even information about their friends, when they first sign up for the service a social network provides, every time they log on and use the service, and even when they are online but not logged on to the social network.[47] This personal information translates into advertising dollars, and ultimately revenue for social networks.[48] Thus, when Facebook announced in October 2012

---

[42] FACEBOOK, www.facebook.com (last visited Mar. 10, 2013).

[43] Brad Stone, *While Facebook Pivots to Mobile, Investors Remain Jittery*, BLOOMBERG BUSINESSWEEK, Jan. 30, 2013, http://www.businessweek.com/articles/2013-01-30/while-facebook-pivots-to-mobile-investors-remain-jittery.

[44] Katheryn A. Andresen, *Marketing Through Social Networks: Business Considerations – From Brand to Privacy*, 38 Wm. Mitchell L. Rev. 290, 294-294 (2011).

[45] *See* Jared S. Livingston, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting,* 21 Alb. L.J. Sci. & Tech. 591, 623 (2011). Courts, however, have been unwilling to make this leap from logic to law, even refusing to recognize registered users of social networks as "consumers" because they have not paid a fee for the service. *In re Facebook Privacy Litigation*, 791 F.Supp.2d 705, 715, 717 (N.D.Cal. 2011) ("Plaintiffs' contention that their personal information constitutes a form of 'payment' to [Facebook] is unsupported by law.").

[46] *Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites*, 74 Sask. L. Rev. 263, 265 (Nov. 22, 2010) [hereinafter *Legal Obligations*] (statement of Privacy Comm'r Jennifer Stoddart, Office Privacy Comm'r Can.). Jennifer Stoddart, Privacy Comm'r, Office Privacy Comm'r Can., *Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites*, 74 Sask. L. Rev. 263, 265 (Nov. 22, 2010).

[47] Natasha Singer, *You For Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, Jun. 16, 2012, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0 (describing the process by which information about other Web browsing activities is tracked through the use of cookies, "bits of computer code placed on browsers to keep track of online activity.").

[48] Somini Sengupta & Nick Bilton, *Billion Users Raise Stakes At Facebook for Revenue*, NEW YORK TIMES, B1, Oct. 15, 2012, *available at* 2012 WLNR 21136731.

that it had reached one billion active users worldwide the month before, this was not a celebration of a sentimental milestone, but a major fiscal achievement and message to advertisers and investors alike that Facebook was the preeminent social network to invest in. [49]

Social networks and their advertisers are able to convert personal information into cash with the help of data aggregators, dubbed "Big Data," which FTC Chairman Jon Leibovitz calls the "unseen cyberazzi."[50] Database marketing is a multi-billion dollar industry, led by Arkansas-based Acxiom Corporation, which maintains the world's largest commercial database on consumers.[51] Acxiom is not a household name like Facebook, but maintains a database of personal information on about 190 million people in the U.S. that the company has been collecting for forty years.[52] Companies like Acxiom develop profiles on individuals based on all of the information they collect, then use ranking systems to classify the consumer as "high-value" or "low-value" prospects, or even "waste," and then places them in more detailed socioeconomic categories.[53] This detailed approach allows advertisers to place an apt appeal directly before the target social media user. Such close surveillance that could arguably impinge on consumers' privacy to a point of harm may raise red flags to consumers, but in the U.S., these practices are "perfectly legal."[54]

In 2008, J.P. Morgan analyst Imran Khan anticipated that privacy issues would begin to subside for social networking sites.[55] Perhaps this was just optimistic investor relations-talk to encourage investment in social media in a global economy on the brink of disaster, because Mr.

---

[49] *Id.*
[50] Singer, *supra* note 47.
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *See* Joshua Gliddon, *Report Finds Nothing But Net Profits,* Austl. Fin. Rev. 34, Jan. 4, 2008, *available at* 2008 WLNR 28765318.

Khan's prediction could not have been further from the outcome. 2008 ushered in a new era of online advertising that would bring more attention and concern to privacy issues in social media than ever before. As a result of diminished advertising budgets during the Great Recession, social media were challenged to heighten their value to advertisers.[56] Social networks began offering behavioral targeting to its advertisers,[57] a practice the FTC has defined as "the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."[58]

Advertisers took the bait, reportedly paying 2.68 times more in 2009 for behavioral ads than traditional online ads.[59] This trend has continued, evidenced by Facebook's launch of Facebook Exchange in the summer of 2012. Exchange tracks users' online behavior beyond their activity on Facebook and allows advertisers to offer real-time ads tailored to users' interests based on "past intent" garnered through the use of cookies.[60] Location-based advertising practices are also on the rise, using GPS technology with social network apps on mobile devices to deliver targeted advertising to users based on their location.[61] Location-based advertising is also expected to become a multi-billion dollar industry in the near future, with 2015 spending

---

[56] Ozer, *supra* note 41 at 235-36.
[57] *Id.* at 236.
[58] Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 Nw. J. Tech. & Intell. Prop. 1, 11 (2009) (footnote omitted).
[59] Ozer, *supra* note 41 at 237.
[60] Chris Horton, *Facebook Sells Your Data to Promote Online Ad Retargeting*, SOCIALMEDIATODAY, Social Customer blog, posted Jul. 11, 2012, http://socialmediatoday.com/chris-horton/602381/facebook-sells-your-data-promote-online-ad-retargeting.
[61] *See* Terenzi, *supra* note 8 at 1050. *See also* Ozer, *supra* note 42 at 237 ("The economic slowdown has also influenced companies to explore location-based services and location-based advertising, utilization of geolocation services to deliver even more targeted advertisements based on a consumer's physical location, as new revenue sources.").

projected to be $1.5 billion.[62] Behavioral and location-based advertising practices are touted by social media executives as a benefit to users. Some argue this is necessary in order for social media to continue to offer services to users free of charge.[63] Others find it to be a deepening of the already alarming encroachment into the zone of users' privacy. Facebook's progressive integration into all aspects of users' online experience, allowing third party advertisers direct access to users' information, has been called "a fundamental transformation of the very nature of the service they are providing, from social networking site to guerilla advertising and marketing site."[64]

A deluge of new features designed to dig deeper for personal information and monetize have been introduced to top social media platforms recently, including Facebook's Exchange and Gifts programs;[65] Twitter's partnership with American Express, which will encourage Tweeters to purchase special offers with just a stroke of the hashtag;[66] and most recently, Facebook's re-designed News Feed, which promises to supersize the ads the company has already determined are "news" for its users.[67] These shifts indicate that social networks have quickly evolved from merely interpersonal communication channels to corporate advertising vehicles that capitalize on private information and close relationships.

---

[62] Ozer, *supra* note 41 at 238.
[63] *See* Determann, *supra* note 13, at 15.
[64] Renay San Miguel, *Facebook Critics: Does Behavioral Advertising by Any Other Name Smell as Foul?*, TECHNEWSWORLD (Apr. 21, 2010, 3:14 PM PT), http://www.technewsworld.com/story/69829.html (quoting Ginger McCall, Chief Counsel, The Electronic Privacy Information Center.).
[65] *See* Stone, *supra* note 44.
[66] Shira Ovide, *Twitter, Amex to Collaborate on E-Commerce Sales on Twitter*, WALL ST. J. DIGITS BLOG, Feb. 11, 2013, 6:00 PM, http://blogs.wsj.com/digits/2013/02/11/twitter-amex-to-collaborate-on-e-commerce-sales-on-twitter/.
[67] Somini Sengupta, *Facebook Shows Off New Home Page Design, Including Bigger Pictures*, N.Y. TIMES, Mar. 8, 2013, at B4, *available at* 2013 WLNR 5735142.

D. *Users' Expectations of Privacy and Protection*

"Perhaps privacy is essentially contested – most everyone agrees that we should have it, but has different ideas of just what it is."[68] In the ubiquitous 1890 Warren and Brandeis article, *The Right to Privacy*, it was described as "the right to be let alone."[69] In 1967, Alan Westin described individual privacy as "the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public."[70] These definitions both point to a perennial "right" that encompasses an element of personal control that survives no matter the time or technology. In the sphere of social media, where personal information is the sought-after commodity, the expectation is generally that users should be able to control *who* can access and collect *what* information about them.

Some argue that social media users do not have a reasonable expectation of privacy in their personal information by virtue of creating a social media account or profile; the very purpose of joining social networks, they reason, is to share information with others.[71] The terms *social* media and *social* networking validate this argument without the need for in-depth analysis, but others are unhesitating in pointing to the exception: the many "zones of privacy" in which we control what information is shared with whom.[72] In some zones, where information may be

[68] Henderson, *supra* note 4, at 232.
[69] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. rev. 193 at 195 (1890) (citation omitted).
[70] Alan F. Westin, *Privacy and Freedom* 42 (1967).
[71] Livingston, *supra* note 45 at 13.
[72] Henderson, *supra* note 4 at 233. *See also* Warren & Brandeis, *supra* note 70 at 198-99 ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness-stand); and even if he has chosen to give them express, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the

sensitive for either personal or safety reasons, we have a greater expectation of privacy than in others, where we may be more willing to share particular information with certain trusted individuals, and in yet in other zones, where we freely share information without much thought or restriction, we have no reasonable expectation of privacy. In essence, there is a sliding scale of the level of privacy people expect in their communications and personal information. The structure of social networks like Facebook, which purports to allow users to keep certain information private, supports that the concept of various zones of privacy is universal, even natural. Sharing may modify, but does not necessarily destroy privacy.

Facebook C.E.O. Mark Zuckerberg has remarked that privacy is no longer a "social norm" in the social media era.[73] This attitude suggests that users are indiscriminately sharing their information without heed, simply because they do not care. There is no acknowledgement accompanying such assertions of the fact that consumers lack reasonable alternatives to the compromising terms offered by social networks, and also lack support from the law. Access to social media services is generally offered on a take-it-or-leave-it basis, with no room for negotiation over terms. Perhaps in response to such declarations made by social media, President Obama firmly concluded in his introductory letter to the privacy framework released by the White House in 2012:

> One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion

---

particular method of expression adopted…Neither does the existence of the right depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression…In every such case the individual is entitled to decide whether that which is his shall be given to the public…The right is lost only when the author himself communicates his productions to the public…").

[73] Toohey, *supra* note 5 at 10.

> that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.[74]

E. ***Privacy Policies and Terms of Use***

User agreements in social media generally fall into one of two very distinct categories. First, there are lengthy, verbose agreements containing broad terms favorable to the provider, including forum selection and arbitration clauses, choice of law provisions, and a set of the most circumscribed rights for the user that a brilliant legal mind could fashion.[75] These agreements walk a fine line of enforceability. They fit the profile of a contract of adhesion, which is a standardized contract drafted by the party in superior bargaining position, without the opportunity for negotiation by the assenting party.[76] A party can accept all of the terms of this contract, or walk away. California courts, which hear the majority of social network privacy policy disputes because of the forum selection clauses found within user agreements,[77] have

---

[74] *Consumer Data Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation In The Global Digital Economy*, February 23, 2012, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. [hereinafter *Framework for Protecting Privacy*]

[75] For example, Facebook's Statement of Rights includes "[w]e reserve all rights not expressly granted to you," although a reader would be hard pressed to find *any* valuable rights expressly granted to them in any of the numerous Facebook policies and subdivisions. FACEBOOK, *Statement of Rights and Responsibilities*, 19(10) Other, last revised Dec. 11, 2012, *available at* http://www.facebook.com/legal/terms.

[76] *Comb v. PayPal, Inc.*, 218 F. Supp. 2d 1165 (N.D. Cal. 2002) (finding an arbitration clause in PayPal's user agreement to be both procedurally and substantively unconscionable and thus, an invalid contract of adhesion).

[77] FACEBOOK, Statement of Rights and Responsibilities, (16)(1), last revised Dec. 11, 2012, *available at* http://www.facebook.com/legal/terms ("You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a *state or federal court located in Santa Clara County*. The *laws of the State of California will govern* this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. *You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California* for the purpose of litigating all such claims.") (emphasis added). *See also* INSTAGRAM, Legal Terms, Governing Law and Venue, effective Jan. 19, 2013, *available at* http://instagram.com/about/legal/terms/ ("These Terms of Use are *governed by and construed in accordance with the laws of the State of California*…For any action at law or in equity relating to the arbitration provision of these Terms of Use, the

discretion whether to sever unconscionable terms from the contract or invalidate the whole contract if there is a finding of unconscionability in the terms and circumstances of the agreement.[78]

In the second category are those where a void exists in place of the aforementioned verbose agreement.[79] Social networks may not include privacy terms within a user agreement or contract so that it may avoid any risk of action by the Federal Trade Commission ("FTC"). The FTC is the federal government's eye over unfair or deceptive trade practices and has the power to bring enforcement actions where a network has a privacy policy in place, but does not adhere to it.[80] If a social network does not make any representation about privacy to users, then there can be no misrepresentation.[81] Operating without a privacy policy, however, does not release a social network from the FTC's watch entirely. Without the detailed terms prevalent in most agreements, choice of law and forum selection clauses, in particular, a provider also risks being pulled into court far from Silicon Valley, facing a privacy tort action in one of the thirty-seven jurisdictions that recognize tort claims for invasion of privacy.[82]

Excluded Disputes or if you opt out of the agreement to arbitrate, you *agree to resolve any dispute* you have with Instagram exclusively in a state or federal court located *in Santa Clara, California*, and to *submit to the personal jurisdiction of the courts located in Santa Clara County* for the purpose of litigating all such disputes.") (emphasis added).

[78] *Circuit City Stores, Inc. v. Mantor*, 335 F.3d 1101, 1109 (9th Cir. 2003).

[79] This is less common, and ordinarily only encountered within a short time of a social network's launch. In January 2013, for instance, new users of the Lift app for iOS were not presented with terms of use or a privacy policy upon registration, but after completing the process could opt to be notified when a privacy policy was developed and implemented.

[80] *See* Toohey, *supra* note 5 at 7.

[81] Livingston, *supra* note 45 at 618 ("[B]ecause the FTC's role is enforcement rather than regulation, firms have an incentive to exclude protection provisions in privacy policies--if there is no representation about privacy, there cannot be any misrepresentation about privacy, and the FTC is a mere toothless enforcer.") (footnote omitted).

[82] Tort action for invasion of the right of privacy is currently recognized in Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan,

That social networks offer "privacy policies" can be misleading, inducing an unknowing user to believe that social networks have an interest in protecting their personal privacy. Social networks do not have an interest in keeping users' personal information private from third parties authorized to access the data. On the other hand, social networks do have an interest in keeping users' personal information secure from uninvited intruders. A network with lax security protections would not only risk action from the government for data security breach (an area divorced from the topic of privacy, for purposes of this paper), but would also risk losing its single most valuable asset – users' personal data. This distinction is crucial, but is difficult for many social media users to recognize in the midst of policy overload.

No matter the reason – laziness, click-happiness, poor vision, ineptness, impulsiveness, general lack of concern, insatiable appetite for immediate gratification, ignorance, valuing free media more than privacy – the fact is that consumers are not reading privacy policies. Users do not know their rights or obligations under the contracts they have entered with social media, and do not even realize the actual cost of their "free" memberships. "There are indications that consumers' seeming lack of concern about privacy issues stems more from *unawareness* rather than from *informed unconcern*."[83]

A common trait among all terms of use and privacy policies is the tremendous burden on the user to know what they have agreed to. Understanding that people do have an innate desire for privacy and a variable expectation within different zones, this paper reasons that the prime explanation for blind acceptance of terms is the sheer burden on the user, including (1) the length

---

Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, and West Virginia, as well as a Minnesota federal court. Additionally, Oklahoma, New York, Utah, and Virginia provide for statutory tort actions for appropriation, one of the four common law privacy torts. *See* Restatement (Second) of Torts § 652A (1977), Reporter's Note (West).

[83] Gindin, *supra* note 58, at 50 (emphasis added).

and complexity of the policies, (2) the oppressiveness of the terms without room for negotiation, and (3) the ease with which a user can sidestep reviewing the policies and get right to the "goodies."

Studies show that it would take the average consumer up to 293 hours per year just to skim the privacy policy at each Web site they visited, and up to 304 hours to actually read them.[84] Assuming a person takes in a restful eight hours of sleep each night and works a forty-hour week, this amounts to over ten percent of an individual's unscheduled time in one year. These figures do not attempt to measure the amount of time it would take the average consumer to then *understand* the policies, if they could at all.[85] For a mobile user operating from a smart phone, it could take up to 150 clicks just to read one of these policies.[86] It is unreasonable for anyone – an industry, the courts – to expect the average consumer can and will devote the time and focus necessary to thoroughly review these agreements upon registration, and again every time there is a change to the terms.

Presuming one could and would read the terms of each social media agreement they are presented with, there remains little incentive to do so. As previously discussed, the policies set forth by social media firms are pro-drafter, and leave consumers in a position to accept the terms in full to gain access to the service they want and/or need, or reject them and function without the service. Negotiation does not exist in this arena. Unless they come as a mob (discussed later

[84] Ozer, *supra* note 41, at 225 (footnote omitted).
[85] Given privacy policies are drafted by attorneys, it could take a semester of law school for most users to develop even a superficial understanding the agreements they have so freely assented to. I would like to take this opportunity to thank Professor Marc Edelman for teaching me everything I *never* wanted to know about the Facebook End User Agreement I blindly accepted as an early adopter in 2004.
[86] Maurer School of Law: Indiana University, Bloomington, 2012 WL 2290589 at 4 (F.T.C.) (Mar. 21, 2012) [hereinafter *FTC Bloomington Statement*] (statement of Comm'r Julie Bill, Federal Trade Commission).

in this paper), the lone consumer lacks bargaining power, so they come to the table already defeated. It is not necessarily a failure to read the terms that undermines market pressure on social media to alter their terms to be mutually beneficial, but a failure to bargain collectively rather than assenting individually.[87]

Finally, the procedure for accepting terms is featherweight in comparison to the smothering tonnage of the terms that are a click away on a registration page. The common form of agreement online is what is a called a "clickwrap agreement."[88] When a user takes an affirmative step to use a service online, they are required to give consent to certain conditions (the privacy policy and terms of use, alone with any additional agreements governing the service). Giving consent does not occur after an elaborate procedure or verifying the new user has read every term of the policies, but simply with a click of a button, usually a box of some fashion that reads along the lines of "I agree." From there, the user can proceed into their new social media home. Such an expeditious registration process does not square with the heft of the terms, which are generally enforceable despite the obvious unfairness, nor the severity of the potential effects of the terms. Clickwrap agreements may sound more like unilateral contracts that courts should be unwilling to enforce if for no other reason, on public policy grounds, but generally courts have recognized them as binding, enforceable contracts because the user has "agreed," even if they have not actually read the terms.[89]

---

[87] *Contra* Livingston, *supra* note 45 at 626 (footnote omitted).

[88] See Kevin W. Grierson, *Enforceability of "Clickwrap" or "Shrinkwrap" Agreements Common in Computer Software, Hardware, and Internet Transactions,* 106 A.L.R.5th 309, 317, n.1 (2003), for an explanation of "clickwrap" agreement formation.

[89] *See ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (acknowledging the enforceability of standardized electronic contracts where a user must take some action to indicate they agree). *See also* Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 Berkeley Tech L.J. 577, 579 (2007) ("Courts have unanimously found that clicking is a valid way to manifest assent since the first clickwrap agreement was litigated in 1998 in *Hotmail Corp. v.*

F. ***Escalating Privacy Concerns***

The rapid development of high speed Internet and now the integration of mobile technology have caused the privacy alarm to sound. This is not the first time Americans have been frightened by the effect of technology on individual privacy, but it may be the most urgent cry for attention yet.

In 1890, it was snapshot photography that was on the cutting edge of technology and prompted Justice Brandeis and Samuel Warren to address the threat to privacy by the development. Well over a century later, their words are as fitting today as they were then: "Recent inventions and business methods…have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[90] Any boundaries that existed between private people and the public domain in 1890, particularly between consumers and producers, are now either extinct or deeply endangered. Comparing the current climate, FTC Commissioner Julie Bill said, "[t]he Internet Revolution makes snapshot photography…look like child's play."[91]

Privacy concerns span lack of anonymity, third-party access to information without express consent, "trusted" third parties being targeted by criminal hackers, total exposure in areas where there once was an expectation of privacy, appropriation and the loss of control over the value of personal identity, effect on employment, control over reputation, physical safety, and even harms yet unfathomable. Most alarming is that the law, meant to keep order and

---

Van$ Money Pie, Inc." "The user's failure to read, carefully consider, or otherwise recognize the binding effect of 'I agree' will not preclude the court from finding assent to the terms.").

[90] Warren & Brandeis, *supra* note 69 at 195.

[91] FTC Bloomington Statement, *supra* note 876 at 3.

protect, is not on par with technology and does not provide the type of protection one might expect it to.

III. THE LAW

Social media have evolved at breakneck speed, whereas the law has remained relatively static in the United States.[92] Without comprehensive national privacy legislation, cyber law remains fragmented and inconsistent across industries and states.[93] Operating on self-designed policies without underlying guidance creates confusion for Internet firms and users both. With guidelines determined by law, social media policies would be more consistent across sites, which would provide a more secure and predictable experience for users concerned with privacy.

American lawmakers have consciously avoided pushing sweeping legislation that would affect the industry, instead leaving it generally to self-regulate. The effect on commerce is positive, encouraging innovation within U.S. borders and promoting competition, the benefits of which are usually passed along to consumers. Yet a void of federal baseline legislation has left consumers with few avenues for redress when their privacy has been violated.[94] Any benefit users receive from healthy market competition is negated by their vulnerability without protection of law. Privacy violations are usually intangible harms, making it difficult for users to show standing or damages in order to bring claims.

Market challenges aside, a critical consideration in developing privacy policy in the U.S. is maintaining a balance between protecting privacy rights of individuals against private actors, which are not explicit in the Constitution, and maintaining the integrity of express First Amendment rights of free speech and information.

---

[92] Henderson, *supra* note 4, at 244.
[93] Toohey, *supra* note 5.
[94] *See* Toohey, *supra* note 5, at 7.

A. *Federal*

The federal statutes currently in effect that provide remedies to individuals for privacy infringement are the Children's Online Privacy Protection Act ("COPPA"),[95] the Electronic Communications Privacy Act of 1986 ("ECPA"),[96] and a subdivision of the ECPA, the Stored Communications Act ("SCA")[97]. The enactment of these federal statutes is noteworthy as an indication that Congress recognizes the importance of privacy, enough to legislate on specific issues. However, the limited scope of these laws falls far short of providing the basic protection of the right to privacy or create a uniform statutory cause of action for the general public against private violators.

The ECPA was enacted to extend existing restrictions on government wiretaps to private electronic data transmissions.[98] The SCA prohibits Internet service providers, including social media, from disclosing users' electronic communication and records held by the providers to governmental entities, but does not prohibit disclosure to private entities.[99] This creates redundancy, prohibiting by statute what the Fourth Amendment already safeguards against, but passes over protecting private information from the prying eyes of private parties, which is the wrong now at the heart of the movement for privacy protection.

COPPA imposes substantial obligations on Web site operators in their dealings with children under the age of thirteen.[100] Its purpose is to give parents a degree of control over what type of information is collected from their children and for what purposes the data can be processed, control adults would like to have over information collected about themselves. This

[95] Children's Online Privacy Protection Act, 15 U.S.C.A. §§ 6501-6506 (West).
[96] Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2510-2522 (West).
[97] 18 U.S.C.A. §§ 2701-2712 (West).
[98] 18 U.S.C. § 2511 (2008).
[99] *See* Henderson, *supra* note 4, at 245-46.
[100] 15 U.S.C. § 6501(1).

Act is deficient in its scope because only aims to protect children under thirteen years old, rather than the general public, or even children of all ages. Despite its applicability to Internet data collection activity, COPPA falls short of having an impact on data collection practices in social media, as most social networks prohibit children under the age of thirteen from registering for service.[101] Also, enforcement of COPPA falling within the province of the FTC, a government entity, severs the connection between the action of the wrongdoer and the injury to the individual whose privacy the object of the violation. What is a very personal intrusion is addressed in the most impersonal manner.

1. The Federal Trade Commission

The FTC was created by the Federal Trade Commission Act of 1914 to prevent unfair methods of competition in commerce, but its role has been expanded by subsequent laws giving the agency broad authority over anticompetitive practices. [102] Most relevant to the FTC's role in regulating social media is the 1938 prohibition against unfair and deceptive acts or practices.[103]

The FTC has taken action against several social media organizations for deceptive and unfair practices in recent years, including GoogleBuzz, for deceptive privacy practices during the launch of the social network, and Facebook, for making unilateral changes affecting information users indicated they wanted keep private. Without notice, the changes made this private information public. Users were told their information would not be shared with advertisers, though it ultimately was. The social network also made an agreement that it would take down photos and videos of users who had deleted their accounts, though it never did.[104] The Facebook

[101] *See* Frieden, *supra* note 18 at 1686.
[102] 15 U.S.C.A. § 41 (West). *See also* About *the Federal Trade Commission*, FEDERAL TRADE COMMISSION WEBSITE, http://www.ftc.gov/ftc/about.shtm, last modified Jan. 5, 2012.
[103] 15 U.S.C.A. § 57a (West).
[104] FTC Bloomington Statement, *supra* note 86, at 3.

action concluded in a settlement agreement in 2011.[105] Arguably one of the most significant terms of this settlement is the requirement that Facebook implement a comprehensive privacy program that will be monitored by an independent auditor for twenty years.[106] By the time this supervision ends, Facebook will have spent more than half of its existence under the watchful eye of what is, in essence, a social media parole officer. Such repressive terms may substantially deter other organizations from engaging in similar practices.

The FTC does not provide for private actions to be brought by individuals; rather, it encourages industry self-regulation and litigates on behalf of the people when the Commission finds it necessary.[107] Recognizing the need for some intervention in the arena of Internet privacy and consumer protection, the FTC has set forth a framework for privacy protection.[108] This framework is not a mandate, but a set of industry best practices and guidelines. The three broad principles of privacy the FTC has highlighted are (1) privacy by design, (2) simplified choice, and (3) greater transparency. [109]

Privacy by design is to be a self-imposed proactive measure, encouraging built-in privacy and security protections for products. Companies are encouraged to consider whether they need to collect all of the data about consumers they currently are collecting, and also determine whether they are retaining the information longer than necessary for their purposes.[110] Simplified choice is the most talked-about of the recommendations the FTC released,

---

[105] *In the Matter of Facebook, Inc., a corporation*, F.T.C. File No. 092 3184 (2011) (agreement and consent order). *Available at* www.ftc.gov/os/caselist/0923184.
[106] *Id*.
[107] FTC Bloomington Statement, *supra* note 86, at 3.
[108] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, F.T.C. Final Commission Report, released Mar. 26, 2012, *available at* www.ftc.gov/os/2012/03/120326privacyreport.pdf. [hereinafter *FTC 2012 Report*]
[109] *Id. See also* FTC Bloomington Statement, *supra* note 86.
[110] FTC Bloomington Statement, *supra* note 86, at 4.

encouraging development of Do-Not-Track mechanisms. This feature would give users the opportunity to choose whether or not they want to allow particular websites to collect information about them for marketing or other purposes.[111] This feature reflects the idea of varying personal zones of privacy, and by shifting control to an individual, indirectly recognizes privacy as a right.

The third principle set forth by the FTC, greater transparency, would address the "fear of the unknown" concern. This principle encourages companies to be plain with information about data collection practices. If social media take action and incorporate this principle into their practices, users can anticipate a shift to shorter user agreements with terms they can understand. Assuming readers are not currently reading the terms they agree to because of the length and complexity of the agreements, this change will likely result in more users reading the terms, understanding the practices and questioning them, possibly opting to *reject* them, putting pressure on social media firms to hone in their information-sharing practices. This may be a long line of reasoning, but it is not unthinkable. If adopted as an industry mantra, "greater transparency" has the potential to have a truly transformative effect on the relationships between social media and their users.

These principles are just that; they encourage industry self-regulation and do not provide a basis of action or regulation under the laws the FTC is charged with enforcing.[112] The FTC has taken years to develop this plan, and the outcome remains uncertain, given the industry that is encouraged to self-regulate is one that has a track record of bad behavior, requiring the FTC to

[111] *Id.* *But see* Toohey, *supra* note 5, at 11 (arguing this feature may fall short of appeasing consumers because it only prevents a site from providing the user's private information to third parties for advertising on other websites, but will *not* block ads from first party sites).
[112] *See* Toohey, *supra* note 5, at 11.

take action to prevent any further harm from being inflicted on consumers.[113] Whether directly or indirectly, the FTC does not appear to have been lost on this fact, as the report has also called on Congress to enact baseline privacy protection.[114]

2. The White House

Just ahead of the release of the FTC final report on privacy framework, the Obama Administration ("the Administration") also issued a proposed framework for privacy legislation.[115] The framework is intended to expand consumer privacy protection in order to "preserve consumer trust…while promoting innovation."[116] From the outset, this framework is in neutral territory, addressing the two leading concerns of both sides of the privacy debate, that delicate balance of protecting the rights of individuals without stifling innovation. The hallmark of this proposal is the Consumer Privacy Bill of Rights, and the Administration has called for Congress to pass legislation that would apply the framework "to commercial sectors that are not subject to existing Federal data privacy laws."[117]

The Administration's proposal is flawed in one critical way: it does not explicitly recognize an *individual's right* to privacy. Rather, the Administration seeks to promote regulation and strengthen the enforcement power of the *government*. "As part of consumer data

---

[113] Serving some credit to data-driven industry self-regulating is the Digital Advertising Alliance, a voluntary group of advertising and media organizations, that has set out to inform consumers about industry practices, encourages users to take an active, educated role in controlling their personal data to the extent possible while also embracing the benefit of sharing some information. This organization goes a step beyond simply informing, and allows consumers to take action by opting out of certain data collection activities on member sites. *See Digital Advertising Alliance Announces 'Your AdChoices' Consumer Education Campaign*, PRNEWSWIRE.COM, Jan. 20, 2012, http://www.prnewswire.com/news-releases/digital-advertising-alliance-daa-announces-your-adchoices-consumer-education-campaign-137749828.html.

[114] *FTC 2012 Report, supra* note 108. *See also* Toohey, *supra* note 5, at 11.

[115] *Framework for Protecting Privacy*, *supra* note 74.

[116] *Id.* at 1.

[117] *Id.* at i.

privacy legislation, the Administration encourages Congress to provide the FTC (and state attorneys general) with specific authority to enforce the Consumer Privacy Bill of Rights."[118] The Consumer Privacy Bill of rights effectively addresses the need for an individual to have control over personal information they share as an active online consumer, but fails to provide for a civil cause of action that would be supported by a federal law. In line with recent proposals made in Congress, discussed below, this structure allows the government to impose sanctions, but the individual who has actually been harmed is not given the opportunity to directly confront the offender and demand compensation for their injury. Stopping short of declaring a right to privacy forecloses meaningful change for consumers.

3. Congress

Heeding messages from the FTC, the White House, and even the Supreme Court, Congress has been addressing Internet privacy concerns. The 112th Congress introduced numerous bills including: the Do Not Track Me Online Act ("to direct the [FTC] to prescribe regulations regarding the collection of data and use of information obtained by tracking the Internet activity of an individual");[119] the Best Practices Act ("to foster transparency about the commercial use of personal information, provide consumers with meaningful choice about the collection, use, and disclosure of such information");[120] the Commercial Privacy Bill of Rights Act of 2011 ("to establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the [FTC]");[121] the Consumer Privacy Protection Act of 2011 ("to protect and enhance consumer privacy");[122] the Location Privacy Protection Act of

[118] *Id.* at 2.
[119] H.R. 654, 112th Cong. (2011).
[120] H.R. 611, 112th Cong. (2011).
[121] S. 799, 112th Cong. (2012).
[122] H.R. 1528, 112th Cong. (2011).

2012 ("to address voluntary location tracking of electronic communications devices");[123] and the Mobile Device Privacy Act ("to require disclosures to consumers regarding the capability of software to monitor mobile device usage[] [and] to require the express consent of the consumer prior to monitoring").[124] The intended purpose of each bill sounded like the last, and addressed consumer concerns that have already been on the public stage for years. The most noteworthy in terms of timeliness are the Location Privacy Protection Act of 2012 and the Mobile Device Privacy Act. As previously discussed, social media and the advertising industry have already adapted their data collection and use plans to bombard our increasingly mobile society with ads on the go.

Members of Congress supplied immeasurable resources, courtesy of American taxpayers, to creating these bills, introducing them, fighting for them – and not a single bill (of those noted here) was enacted.[125] The problem with all of these proposals, the location-centric bills, included, is that they all propose too little protection, too late. When our lawmakers are crafting specific laws aimed at particular practices that have already offended and harmed the public, it is too late, the harm has been done. New, more harmful practices are already coming around the virtual corner. Congress is being reactive rather than proactive, and when the Internet moves at "lightning speed" as advertised, piecemeal legislation provides no protection at all. Notably absent among all of the proposed legislation was a declaration of the right of privacy against private actors.

[123] S. 1223, 112th. Cong. (2011).
[124] H.R. 6377, 112th Cong. (2012).
[125] *See generally* GOVTRACK, http://www.govtrack.us (providing abstracts and status on bills introduced in Congress).

The 113th Congress is now in full swing, and as of March 2013, three bills related to social media have been introduced.[126] Each of the three addresses a topic that is marginally collateral to the issue of protection personal privacy rights in social media (prohibiting employers from requiring employees to provide their access credentials to personal social networking accounts; a plan for conducting research on cybersecurity; and combating trade barriers that threaten the openness of the Internet). Last November, Rep. Darrell Issa of California posted draft legislation online for the Internet Moratorium Act of 2012, which would impose a two-year moratorium on any new laws, rules, or regulations relating to the Internet, including privacy.[127] The story became front-page fodder, but in light of the inability of Congress to craft and pass any significant changes to law that would protect the public from recurring privacy violations, there may be merit to Rep. Issa's proposition.

C. *States and Private Action*

Without a constitutional right to privacy or thorough federal legislation to rely on, consumers must turn to the state laws to seek recovery for privacy harms. Even further limiting the redress available to aggrieved users are the terms they have agreed to in order to gain access to the social media sites that have caused their injury.[128]

---

[126] H.R. 537, 113th Cong. (2013); H.R. 756, 113th Cong. (2013); and H.R. 889, 113th Cong. (2013).

[127] *See* KEEPTHEWEB#OPEN, http://keepthewebopen.com/iama (last visited Mar. 6, 2013).

[128] *See Williams v. America Online, Inc.*, 2001 WL 135825 (Mass. Super. Ct., Feb. 8, 2001) (The only cases where courts have refused to enforce clickwrap agreements were instances in which the user was not required to assent to the terms in order to use the service or was asked to assent to the terms only after downloading or accessing the product. In this case, AOL moved to dismiss the case brought against them in Massachusetts state court based upon the user contract's forum selection clause. The court denied AOL's motion because the contract containing the clause was not available for users to view or accept until *after* they had begun to download AOL's program.). *See also* Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 Berkeley Tech L.J. 577, 583 (2007) ("Courts will give more careful consideration to arguments…in the case of forum selection clauses[] that the term is unfair or unreasonable.").

Silicon Valley, situated in the southern region of the San Francisco Bay Area, Northern California, is the home of tech giants and social media startups. It is no coincidence then, what little case law exists on the point of privacy in social media has come out of the Ninth Circuit, the Northern District of California, San Francisco County, and Santa Clara County courts. Anyone subscribing to services from one the social media giants (such as Facebook, LinkedIn, Instagram, or Twitter) has agreed to litigate their claims in this part of the country by accepting the sites' terms of service containing forum selection clauses and choice of law provisions requiring users to bring any complaint they may have to California courts that will apply California law to the dispute.[129] It would be misleading to say California law on privacy in social media is "rich," but it is comparatively well developed for this reason.

Since Warren & Brandeis first explored a natural and common law right to privacy in *The Right to Privacy*, a majority of states have come to recognize a common law right of privacy, including California.[130] Considering social media firms, the villains in privacy disputes brought by users, choose to have disputes litigated in California, it may come as a surprise that California is the only state recognizing an inalienable right of privacy in its constitution that is not limited

[129] *See* FACEBOOK, Statement of Rights and Responsibilities (16)(1), last revised Dec. 11, 2012, *available at* http://www.facebook.com/legal/terms (limiting the forum for disputes to state or federal courts within Santa Clara County and applicable law to that of California). *See also* LINKEDIN, User Agreement (8)(1), last revised Jun. 16, 2011, *available at* http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag (limiting the forum for disputes to federal and state courts within Santa Clara County "except as otherwise agreed by the parties or as described in the Arbitration Option" and applicable law to that of California). *See also* INSTAGRAM, Legal Terms, Governing Law and Venue, effective Jan. 19, 2013, *available at* http://instagram.com/about/legal/terms/ (limiting the forum for disputes to federal and state courts within Santa Clara County and applicable law to that of California). *See also* TWITTER, Terms of Service, (12)(B), effective June 25, 2012, *available at* https://twitter.com/tos (limiting the forum for disputes to federal and state courts within San Francisco County and applicable law to that of the state of California).

[130] Restatement (Second) of Torts § 652A, cmt. a (1977).

to government actors, but also applies against private intruders.[131] California is also a leader in protective Internet privacy legislation.[132]

In addition to bringing claims under statutory provisions in California, social media users can also allege violations of the common law right to privacy, recognizing four distinct torts: (1) unreasonable intrusion upon the seclusion or solitude of another, (2) appropriation of another's name or likeness for the defendant's advantage (3) unreasonable publicity given to another's private life (public disclosure of private facts), and (4) publicity that unreasonably places another in a false light before the public.[133] These four wrongs are the most commonly recognized, and have been incorporated into the Restatement (Second) of Torts ("Restatement").[134]

At a glance, the two most regularly committed privacy torts by social media and its cyberazzi associates are intrusion upon seclusion and misappropriation of name or likeness. This is not to say publicity given to public life or false light torts never occur, as certain practices,

---

[131] *See* Cal. Const. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").
[132] California passed its first Internet privacy law in 2003, the Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), which requires Websites collecting personal data to post conspicuous privacy notices on the sites, no matter where they are located, so long as the site it accessible to someone in California. The highlight of this law, in recognizing consumer rights, is that it allows for a private action to be brought against a violator. *See* Frieden, *supra* note 18, at 1690-91. OPPA has also withstood the test of time and rapid technological development. Last year, the California Attorney General's officed announced that OPPA would be enforced against mobile applications, as well. *See* Ozer, *supra* note 41, at 248-49. California's Shine the Light Law, Cal.Civ.Code §1798.83 (2006), also passed in 2003, was one of the first attempts to address data brokerage by allowing consumers to demand a record of disclosures a business has made of their personal information to third parties, including the type of information shared and who the third parties are. The design flaw in this law is that is places the burden on the user to discover after the fact what has been shared about them, but in 2003, this was groundbreaking for the very fact that it addressed data collection and brokerage. *See also* California Right of Publicity Statute, Cal.Civ.Code § 3344 (2012).
[133] *See Fraley v. Facebook, Inc.*, 830 F.Supp.2d 785, 806 (N.D.Cal. 2011). *See also* Restatement (Second) of Torts § 652A (1977).
[134] Restatement (Second) of Torts § 652A (1977).

such as the Facebook Beacon or Sponsored Stories programs, could result in actions under these theories, but the offenses commonly complained of fall into the two former categories, related to cookies and tracking and claim of ownership over user content for advertising purposes.

The Restatement defines the tort of intrusion upon seclusion occurring when "[o]ne who intentionally intrudes, physically *or otherwise*, upon the solitude or seclusion of another or his private affairs or concerns."[135] The standard for determining whether the intruder is liable is whether "the intrusion would be *highly offensive* to a *reasonable person*."[136] The calls from the government for privacy protection, the attention given to the issue in mainstream media, and the number of privacy cases brought against technology companies should all indicate to the courts that these practices are in fact highly offensive to reasonable people.[137] Yet, this standard has been a difficult hurdle for plaintiffs to clear in some jurisdictions.[138] California courts have been more inclined to find plaintiffs have met this standard in pleading.[139]

---

[135] Restatement (Second) of Torts § 652B (1977) (emphasis added)
[136] *Id.* (emphasis added)
[137] *E.g., Did the Internet Kill Privacy?*, CBS News, Feb. 6, 2011, *story and video available at* http://www.cbsnews.com/8301-3445_162-7323148.html.
[138] *See Oppenheim v. I.C. System, Inc.*, 695 F.Supp.2d 1303 (M.D.Fla.2010) (holding that a debt collector repeated phone calls to plaintiff did not rise to the level of outrageous and unacceptable conduct under Florida tort law for invasion of privacy, which had not adopted Restatement § 652B and had a narrower definition of intrusion); *see also Boring v. Google, Inc.*, 598 F.Supp.2d 695 (W.D.Pa.2009) (holding plaintiffs failed to allege under Pennsylvania law that Google's taking photographs of plaintiff's home from their private drive to use in the company's 360 degree street-level views sufficient facts to establish the intrusion could cause shame or humiliation to a person of ordinary sensibilities); *see also Busse v. Motorola, Inc.*, 351 Ill.App.3d 67 (Ill.App.2004) (holding individual pieces of information retrieved from customer records by cell phone service providers and transferred to a research firm were not facially revealing, compromising, or embarrassing to plead intrusion upon seclusion).
[139] *See Charvat v. NMP, LLC*, 656 F.3d 440 (C.A.6, 2011) (holding telemarketing companies' thirty-three unsolicited phone calls to plaintiff's home over a three-month period, late at night or early in the morning and thirty of the calls coming after plaintiff requested to be placed on defendant's do-not-call list, could be found to outrage or be highly offensive to a reasonable person); *see also Hernandez v. Hillsides, Inc.*, 142 Cal.App.4th 1377 (Cal.App.2006) (holding that the mere placement of a camera in plaintiffs' office could constitute an invasion of privacy

Under California common law, to state a cause of action for misappropriation, a plaintiff must plead (1) the defendant used plaintiff's identity, (2) the appropriation of plaintiff's name or likeness was to the defendant's advantage, commercially or otherwise, (3) lack of consent from the plaintiff, and (4) injury from the appropriation.[140] In *Fraley v. Facebook*, plaintiffs alleged that Facebook's Sponsored Stories, a feature placing users' names, photos, and the fact that they "like" something of an advertiser and places the information in news feeds of users' friends, was misappropriation under California's Right of Publicity Statute. Under § 3344, plaintiffs must additionally prove (5) the use of plaintiff's name or likeness by defendant was a knowing use, and (6) there was a direct connection between the alleged use and the commercial purpose.[141] The court found that plaintiffs had sufficiently alleged facts supporting all of the elements, and denied Facebook's "newsworthy" First Amendment defense to the claim, because even the plaintiffs' "liking" material on Facebook was newsworthy, it is Facebook's commercial purpose that "removes them from the scope of § 3344(d)'s newsworthy privilege." It was in this case that plaintiffs quoted Facebook CEO Mark Zuckerberg as saying "[n]othing influences people more than a recommendation from a trusted friend. … A trusted referral is the Holy Grail of advertising."[142] It was Facebook's own touting of Sponsored Stories as the event the advertising industry had been waiting for that swayed the court to determine that Facebook was knowingly using plaintiffs' identities for commercial gain, and the injury to plaintiffs was measurable by the revenue Facebook received from using their identities in this capacity.

---

because it allowed defendants to activate the surveillance system without plaintiffs' knowledge and could lead to unwanted access to private data about them.)

[140] *See Fraley v. Facebook*, *supra* note 133, at 803.

[141] *Id.* (citations omitted)

[142] *Id.* at 808 (citing plaintiffs' Second Amended Complaint ¶ 43).

There has been a gradual reduction in the force of the right of publicity since the *Zacchini* case was decided by the Supreme Court in the late 1970s, the courts - particularly Judge Kozinski in the Ninth Circuit – showing a preference for First Amendment exceptions to allow free use of information and facts that are relevant and used as a benefit to society.[143] This trend may shift, as more misappropriation actions are brought against social media, where plaintiffs can prove by the social networks' business models themselves that these companies are knowingly appropriating members' identities for their own gain, and that this is a very valuable revenue stream for the networks. The outcome in *Fraley* demonstrates the courts' willingness to protect users' privacy in these circumstances.

The privacy offenses that actually occur, especially in the age of social media, are beginning to go beyond the four categories provided for in the Restatement and by state courts. The clever intrusion techniques of social media and Big Data are requiring plaintiffs to make creative arguments fitting the unique circumstances of hidden and intangible Internet intrusions into the traditional categories of privacy torts that have served plaintiffs who have been able to see or otherwise be made aware of the invasions on their privacy. As a result, we may begin to see new forms of tort liability arise in dicta, and eventually, the Restatement.[144]

---

[143] *See, e.g., JTW Corp. v. Jireh Publishing*, 332 F.3d 915 (6th Cir. 2003); *see also Samsung Electonics America, Inc. v. White*, 989 F.2d 1512 (9th Cir. 1993) (dissenting opinion written by Judge Kozinski).

[144] Restatement (Second) of Torts § 652A cmt. c (1977). Just as developing technology prompted Brandeis and Warren to consider protections and recourse available in 1890, which led to the causes of action for privacy violations we have today being recognized by courts, developing technology and practices in 2013 may lead to yet another set of standards for modern tort liability.

D. *Global Efforts*

1. European Union

The European Union (EU), taking an approach to privacy far different from that of the United States, adopted the EU Data Protection Directive ("Directive"), which went into effect in December 1995.[145] While the U.S. has exercised restraint in enacting broad federal legislation related to privacy,[146] instead addressing narrow issues as they arise, the Directive is omnibus legislation that has now been governing for almost two decades of rapid technological development.[147]

The Directive contrasts from the U.S. approach in two fundamental ways. First, it establishes privacy as a fundamental right.[148] The Obama Administration has made a step to lead lawmakers in this direction with its 2012 Consumer Privacy Bill of rights and privacy framework, but it has yet to become a right recognized by law.[149] Second, the Directive establishes an "opt-in" scheme for consent to personal data processing, meaning that by default, the consumer has

---

[145] Alexander B. Blumrosen, *The Proposed EU Data Protection Regulation*, 41 ABA INT'L LAW NEWS, no. 4, Fall 2012, *available at* http://www.americanbar.org/publications/international_law_news/2012/fall/proposed_european_union_data_protection_regulation.html.

[146] Paul M. Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902, 910-11 (2009) ("The divergent evolution of U.S. and European law raises the question of why these legal systems took different paths at the fork in the regulatory road. The puzzle is all the more intriguing because an omnibus bill for the private and public sectors, Senate Bill 3418 (S. 3418), was on the table, however briefly, during the formative period in the United States for information privacy. As originally introduced by Senator Samuel Ervin on May 1, 1974, S. 3418 had a broad jurisdictional sweep. It would have established requirements for "[a]ny Federal agency, State or local government, or any other organization maintaining an information system that includes personal information.") (citation omitted.).

[147] Determann, *supra* note 13, at 8 ("US Congress rejected broad privacy legislation in 1974 but has been addressing data processing activities only with respect to specific, compelling threats via general consumer protection laws and narrowly crafted statutes.").

[148] Frieden, *supra* note 18, at 1700.

[149] *See Consumer Data Privacy In A Networked World*, *supra* note 74.

the right to control whether their personal information is disseminated for processing.[150] This default applies to all personal data; separate provisions do not exist for the treatment of financial or medical data, or any other form.[151] The U.S., on the other hand, has enacted free-standing legislation for the handling and processing of certain types of personal information,[152] but still functions on an "opt-out" basis, which by default leaves the consumer without control over whether information collected can be processed.[153] This may seem like an obvious change the U.S. should make in placing control over personal information into the hands of American consumers, but it is important to consider the effects on the technology industry in enacting such sweeping pro-consumer regulation.

The Directive has been both inhospitable toward industry and ultimately, inadequate for consumer protection.[154] The broad regulatory scheme is burdensome to Big Data, and the general prohibition on data processing discourages development of companies within the EU member states.[155] In refusing to enact such sweeping legislation, the U.S. has been friendlier to social media start-ups and related businesses. It is no coincidence, then, that "most meaningful innovation in the… social media age has been coming from US companies."[156] The Directive has been inadequate for consumer protection because of irregular application and enforcement. It does not have the force that a congressional act in the U.S. would. EU member states remain largely autonomous (particularly where the country is a significant contributor to the EU's

[150] Blumrosen, *supra* note 145.
[151] *Id.*
[152] *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (regulating privacy of personal information in the financial services industry).
[153] Frieden, *supra* note 18, at 1701.
[154] *See* Blumrosen, *supra* note 145 ("[T]here are as many different privacy laws in the EU as there are member states, leading to confusion, lack or transparency for individuals, and significant costs for compliance for business.").
[155] Determann, *supra* note 13, at 12.
[156] *Id.*

overall health and wealth), and rather than superseding privacy laws within each member state, the Directive merely set a floor for national legislation.[157] Furthermore, there has been a lack of enforcement of privacy laws within the member states.[158] Without enforcement, laws are hollow, treating the rights they purport to establish and protect as trivial.

The EU Directive, while progressive at the time it was passed, does not address many of the specific concerns that have grown out of the development of social media and the way these organizations, along with data aggregators and brokers, collect and use personal data.[159] These shortcomings have lead to a proposal for a sweeping overhaul of the Directive, the General Data Protection Regulation ("Proposed Regulation").[160] While the United States shows no inclination of passing omnibus legislation, the Proposed Regulation addresses universal areas Congress would be apt to consider as it explores regulating commercial Internet privacy. Such issues include newly recognized fundamental rights such as "the right to be forgotten" and "the right to data portability," and increased sanctions against companies that are not in compliance.[161]

The most talked-about of these changes is the right to be forgotten. The European Commission has recognized a lack of understanding among teens and young adults in how their personal information is used, who it is available to, and what the potential consequences of sharing this information with the world through social media can be – either immediately or in

---

[157] *See* Blumrosen, *supra* note 145.

[158] Determann, *supra* note 13, at 8 ("European data protection laws have not historically differentiated much with respect to particular threats, industries, or types of data. They have remained relatively static over the years. Enforcement by data protection authorities has been lax throughout much of the European data protection laws' history and private enforcement has been nearly non-existent.") (citations omitted).

[159] Blumrosen, *supra* note 145.

[160] *See Commission proposes a comprehensive reform of the data protection rules*, EUROPEAN COMMISSION, Jan. 25, 2012, *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[161] See Blumrosen, *supra* note 145, for a comprehensive overview of the proposed changes.

the future, particularly with respect to employment.[162] If passed, this legislation will allow people to demand information about them, excluding certain public information, be deleted by the commercial organizations holding the personal data.[163] (The Proposed Regulation also includes an exception for the data processor where it has a "legitimate interest" in holding the information.[164] The question then, is who determines what is a *legitimate* interest?) The proposal of this right has been met with skepticism and criticism, including that it will affect the rights of others, specifically the right to information, because it will allow users to demand erasure of information about them, "including text and pictures created by other friends, family, and other users' account."[165] There is a degree of reasonableness, though, in what appears to be such a broad grant of power to individuals to potentially re-write history.[166] When a Facebook user deletes their profile and deletes their profile and discontinues use of the service, they should be able to demand erasure of all of the files and information *they* provided either to or on the platform, rather than Facebook storing the information for an indefinite amount of time, as is current practice under the site's terms.[167] (To no surprise, Facebook was one of the first companies to respond to the Proposed Regulation, indicating it wanted more information about the *scope* of data users would be able to control.[168]) When a user opts to delete their profile in

---

[162] *EU Proposes "Right to Be Forgotten" by Internet Firms*, BBCNEWS.COM (Jan. 23, 2012, 8:20 ET), http://www.bbc.co.uk/news/technology-16677370 [hereinafter *BBCNEWS.COM*].
[163] *Id.*
[164] Blumrosen, *supra* note 145.
[165] Determann, *supra* note 13, at 19.
[166] There is a sharp distinction between allowing *user-generated information* to be deleted upon request and allowing an individual to have *public records or news records* deleted, which has been addressed in the Proposed Regulation. The average social media user is not creating content that becomes newsworthy or otherwise becomes part of the collective memory, so by limiting the right to be forgotten to user-generated information, there is little or no threat of erasing relevant history that exists in the public domain.
[167] FACEBOOK, *supra* note 75.
[168] BBCNEWS.COM, *supra* note 162.

full, they essentially revoke any consent they had given the social network upon registration with the site, and information or content held by the site should transfer back to the user. The proposed right to data portability also addresses this issue, as it would give the departing user the right to a full accounting of their personal data from the site.[169]

Another argument against the broad right to be forgotten is that it "would create a colossal administrative burden."[170] The burden of removing the information would be on the sophisticated organization that retains the data. If technology has been developed to so quickly and efficiently gather data, send it to an advertiser, and return targeted ads based on a user's data, surely there is technology – either now in existence or shortly forthcoming – that is capable of reversing the process, to delete an individual's data profile.

It is evident that the European Union places value on the privacy of its populace, but the question remains whether the direction it has taken in broad regulation is effective or even "better" than the approach taken by the U.S. The Proposed Regulation was introduced in early 2012, and if approved by both the EU Council and European Parliament, it still would not become effective for another two years. If the 1995 Directive remains policy until 2015, given the rate at which technology advances, it may already be too late to be a meaningful revision. Any shortcomings the EU regime may have, other parts of the world – including Latin America – look to its privacy policies for guidance in creating their own.

2. Latin America

The United States' neighbors to the south have been actively addressing privacy concerns since the Internet Age took off. In 2000, Argentina enacted personal data regulation and

[169] Blumrosen, *supra* note 145.
[170] Determann, *supra* note 13, at 20.

established an enforcement authority.[171] The Personal Data Protection Act establishes general principles of protection and rights of individuals, governs actions, provides for sanctions, and is the only Latin American policy "to have attained 'adequate protection' status pursuant to the EU Directive."[172] Mexico, like Argentina, provides both statutory regulation and an enforcement authority.[173] Having an enforcement authority to accompany these regulations is important to prevent harms from occurring, rather than requiring citizens to wait until after their privacy has been compromised to then seek recourse in the court system. Chile's approach to privacy protection is multi-faceted, with a constitutional right to privacy and data protection law enacted in 1999. Chile's legislation did not create an enforcement authority like neighboring Argentina's did, but an agreement between the country and the EU to increase protection may indicate that an enforcement agency is forthcoming.[174] Other Latin American countries that recognize a right of privacy in their constitutions are Brazil, Columbia, Paraguay, Peru, Ecuador, Panama, and Honduras.[175] A constitutional right to privacy that extends against intrusion by private entities is, theoretically, a step ahead of protection available to Americans, but without regulation accompanied by an enforcement authority, citizens of these countries, too, face similar hurdles going through the court system to seek compensation for harms that have already occurred.[176]

---

[171] Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, Vol. 41 No. 4, American Bar Association, International Law News, Fall 2012, http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] *Id.*

3. Saudi Arabia

Saudi Arabia is another country in which an individual's right to privacy is constitutionally recognized.[177] Although Saudi laws and regulations are still in their infancy, regulations enacted within the last decade are specific to telecommunications and cyberspace, and levy harsh penalties including hefty fines and even imprisonment upon violators.[178] Saudi Arabia is worth noting here, as the cultural emphasis placed on an individual's dignity, in a country recognized as business savvy and thriving, may encourage recognition of Saudi law as a model for privacy law in the near future.

F. *A Proposal For Federal Action*

When the First Congress drafted the Bill of Rights in 1789, they could not have foreseen the challenges Americans face today in preserving what little privacy we have. Even if they had, the outcome may still have been the same. The United States was formed as a refuge from tyranny at the hands of government, not data aggregators and social networks; the drafters may have found an explicit declaration of the right to privacy against private intrusion to be unnecessary. Fortunately for Americans living in the age of social media, our country was designed to be a dynamic democracy, built for change, and we are not fated to contemporary consequences of decisions made over 200 years ago.

What Americans lack in express Constitutional protection, we can gain with federal legislation that extends the protections of the Fourth Amendment, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"

---

[177] *See* John M.B. Balouziyeh & Amgad T. Husein, *The Legal Framework for Privacy and Data Protection in Saudi Arabia*, 41 ABA INT'L LAW NEWS, no. 4, Fall 2012, *available at* http://www.americanbar.org/publications/international_law_news/2012/fall/legal_framework_privacy_data_protection_saudi_arabia.html.

[178] *Id.*

to intrusions by private parties.[179] Security in one's "person" should be defined to encompass thoughts, ideas, actions and personal information, including digital data, to leave no ambiguity in application of the law. In a recent Supreme Court government-intrusion privacy case, Justice Alito wrote in a concurring opinion, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes[] [and] to draw detailed lines…in a *comprehensive* way."[180] Detailed and comprehensive legislation does not require a hefty omnibus bill establishing a regulatory authority and various enforcement mechanisms. It can be, and should be, as simple as declaring a right.

Through clear, concise, and emphatic language, the law must make known that privacy is an essential, incontestable right of the people as against all actors, not just government. Armed with an express *right* to privacy, the individual will not have to wait until they incur a tangible injury to take action. The showing of a violation of the right would be enough for the aggrieved to be heard by a court.[181] The law must be free of exclusionary clauses; no industry or niche group shall be exempt from liability for violating an individual's right to privacy, no matter how valuable the group may be to the economy.[182] Finally, the declaration of a right to privacy will

---

[179] U.S. Const. amend. IV.

[180] *United States v. Jones*, 132 S. Ct. 945, 964, 181 L. Ed. 2d 911 (2012) (emphasis added) (internal citation omitted).

[181] When bringing a common law tort claim, or even a statutory claim, plaintiff must show they have been damaged in some way, monetarily. Privacy is unique; because it is so personal, the harm may not translate to a dollar amount at all. It can also be a harm that the effect of is felt immediately, but will arise down the road.

[182] Granting immunity to a group of any kind trivializes the right of the individual, communicating that their privacy is "important," just not as important as the group immunized from action for violating the right. When this occurs, it negates the declaration of the right or protection, and leaves the people in the same shape as they were without the law. *See, e.g.*, Data Acountability and Trust Act of 2011, H.R. 1841, 112th Cong. (2011) (excepting from the force of the proposed law common carriers, including "interactive computer service.").

give the individual the power to enforce their rights and be directly compensated where a violation is found.[183] Meaningful federal legislation will focus entirely on the individual.

III. SOCIAL MEDIA MERGERS AND ACQUISITIONS

A. *M&A Considerations*

Generally, there are three phases within a typical M&A transaction, and sometimes a fourth: (1) the due diligence period, (2) the M&A contract, (3) the closing of the deal, and (4) the transaction is not consummated despite execution of the M&A contract.[184] As it relates to social media user privacy, the most critical of these phases is the due diligence period.[185] During this time, an acquirer must consider how well it will be able to integrate the target aquiree into its operations, from daily business activities, marketing strategies, and even corporate culture.[186] A major piece of the integration challenge is evaluating the *synergy* between the two companies and how they will merge into one through the transaction.[187]

To understand the motivations and actions taken by firms during mergers and acquisitions, there two primary goals to look to, particularly in social media: strategic positioning

---

[183] Unlike legislation that places enforcement power in an agency or other government official, and allows the government to impose sanctions/fines, but the individual who has actually been harmed is never monetarily compensated. *See, e.g.,* Data Accountability and Trust Act of 2011, H.R. 1841, 112th Cong., Sect. 4 (2011) (providing for enforcement but the FTC or the states, where "the attorney general, official, or agency of the State may bring a civil action on behalf of the residents of the State," but not a private cause of action by an individual.)

[184] *See* Jack P. Jackson, *Recent Trends and Strategies in M&A Transactions,* M and A Deal Strategies, Sept. 2012, at 1, *available at* 2012 WL 3303270 (likening these phases to those of a marriage, from "courtship (due diligence period, an engagement (the M&A contract), the wedding (the M&A deal closes), and… in many cases, a divorce (typically the M&A contract is executed but the transaction is not consummated).").

[185] Dale S. Bergman, *Notable Factors and Trends in Recent M&A Deals*, M AND A DEAL STRATEGIES, Sept. 2012, at 7, *available at* 2012 WL 3303268 ("Ultimately, when an M&A deal fails, it is often because the buyer did not do its diligence. An acquirer needs to know exactly what it is buying, what liabilities it is assuming, and how to acquisition is going to affect the acquirer from a financial and operational point of view.").

[186] *Id.* at 4.

[187] Jackson, *supra* note 184, at 4.

and diversification.[188] A company seeking to merge with or acquire another is looking to take the best seat in its industry that it can, either by joining with another company that will put it in the top position, or joining with another in order to preclude the competition from gaining access to a market. In the context of social media, this may mean merging to become the largest social network on the planet, or acquiring a smaller network with outstanding technology to prevent another network from acquiring the technology first. The second goal, diversification, is important to a company so that it may develop its product or service base. Diversification supports growth and also serves as a safety net, should one stream of the firm become less lucrative than others. These goals tend to merge in social media M&A, but diversification may lead as the very vehicle by which firms secure a strategic position.

B. ***Recent Trends in Tech Deals***

Many technology companies, social media being no exception, are attempting to secure their strategic positions by acquiring "patent-rich" start-ups and lesser-known companies.[189] For firms with the requisite cash on hand, it is more practical to simply acquire a company that already has desirable technology than to invest time and capital into developing a similar product that will then have to battle it out with the existing technology for market share.[190]

This trend has a dual effect on the market. It encourages innovation by companies that are not revenue-driven but are incredibly valuable to larger firms looking to acquire technology based on the number of patents they hold.[191] The drawback is that acquisitions by larger firms narrow the market for providers. M&A attorney Dale Bergman calls this trend a "consolidation

[188] Bergman, *supra* note 185, at 2.
[189] Jackson, *supra* 184, at 2.
[190] *See* Bergman, *supra* note 185, at 2.
[191] Jackson, *supra* 184, at 2.

strategy."[192] The consolidation strategy presents a threat to users' privacy, because it leads to fewer choices of provider, and thus, fewer choices for terms of service. The larger and more sophisticated the social media firm, the more lawyers, the lengthier and more complex the terms.[193]

Recent high-profile deals have included e-Bay's acquisition of PayPal and Facebook's acquisition of Instagram, each an example of technology companies fighting to stay relevant in an evolving market by making a grab for specific technology. At the end of 2011, social media analyst Jason Keath reported that in the following year, Facebook was looking to continue acquiring small start-ups with "programming talent" that could carry the social network into the future.[194] "Their focus [was] innovation and not getting stuck in the MySpace death spiral."[195] With social media making a shift to mobile technology, Facebook, which has traditionally been a desktop-based platform,[196] was quickly losing its luster when it made the leap for Instagram.

C. *The Facebook-Instagram Fiasco*

Facebook, the "world's largest virtual nation"[197] is also the bad boy of social media; its reputation precedes it. "Well known for pushing the limits of user privacy,"[198] in 2010 the social

---

[192] Bergman, *supra* note 185, at 1.

[193] Compare ten-year-old Facebook's various lengthy policies, spread across multiple pages, each containing hyper-links to the others, FACEBOOK, *supra* note 76, with four-month-old Lift's borrowed, abbreviated terms, LIFT, Privacy Policy, *available at* http://lift.do/help/privacy-policy (last visited Mar. 23, 2013) and LIFT, Terms of Use, *available at* http://lift.do/help/terms-of-use (last visited Mar. 23, 2013).

[194] Jason Keath, *Top Social Media Acquisitions of 2011*, SOCIALFRESH.COM (Dec. 22, 2011), http://socialfresh.com/social-media-acquisitions-2011/.

[195] *Id.*

[196] Until the close of 2012, when it announced it is now primarily mobile. *See* Stone, *supra* note 43.

[197] Chris Taylor, *Facebook is No Longer A Democracy*, MASHABLE, Nov. 21, 2012, http://mashable.com/2012/11/21/facebook-no-democracy/.

[198] Gavin Heaton, *Instagram Rings Its Own Death Knell and Leaps to the Mainstram*, BUSINESS2COMMUNITY.COM, Dec. 18, 2012, *available at* 2012 WLNR 27218218.

network was ranked as the ninth-worst company on the American Customer Satisfaction Index… based in part on complaints about privacy and personal information protection."[199] Between 2011 and 2012, Facebook's user satisfaction further declined 7.6%.[200] Ahead of Facebook's initial public offering last year, business consulting firm Frost & Sullivan issued a report advising that if Facebook expected to see future growth, it would need to be cautious in its privacy practices.[201]

Instagram was the darling of social media, with "the loyalty of a growing community of creative people that distinguishe[d] it from other flash-in-the-pan-fads."[202] In April 2012, ahead of its acquisition by Facebook, Instagram was mobile-only social network and the most popular (with the exception of giants Facebook and Twitter), and was the sixth most downloaded iOS app with 30 million users.[203] Within one week of its 2010 launch, the mobile app network had almost 200,000 users,[204] and as of December 2012, claimed to have more than 100 million users who had uploaded more than five billion photos to the network.[205] Instagram offers but one service, photo filters, and does not generate any revenue from the photos.[206] The simplistic

[199] Ozer, *supra* note 41, at 221.
[200] Internet Social Media Industry Benchmarks, AMERICAN CUSTOMER SATISFACTION INDEX, http://www.theacsi.org (follow "ACSI Results" hyperlink; then follow "Benchmarks By Industry" hyperlink; then follow "Internet Social Media" hyperlink) (last visited Mar. 6, 2013).
[201] *See* Frost & Sullivan.
[202] Hayley Tsukayama, *With Instagram Deal, Facebook Shows It's Taking Rapid Shift to Mobile Platforms Seriously*, WASHINGTONPOST.COM, April 10, 2012, *available at* 2012 WLNR 2360364.
[203] *Id.*
[204] *Id.*
[205] Nicole Perlroth & Jenna Wortham; *Instagram Does an About-Face*, New York Times Bits Blog, Dec. 20, 2012, ts.blogs.nytimes.com/2012/12/20/instagram-does-about-face-reverts-to-previous-policy/ (last visited Mar. 3, 2013).
[206] Steven J. Vaughan-Nichols, *Facebook + Instagram = One Big Acquisition Flop*, COMPUTERWORLD, April 23, 2012, *available at* 2012 WLNR 8738509.

service has been called "a sanctuary from the noise of Facebook and Twitter."[207] With such enviable technology and user base, the sanctuary was bound to be short-lived.

Facebook's acquisition of Instagram, which is the largest acquisition of a purely mobile platform, was anticipated to be a $1 billion deal. It eventually closed at $735 million in early September 2012,[208] a steep price tag for "some Web 2.0 software for tweaking pictures."[209] This amounts to a cost of about $21 for each of Instagram's thirty-five million users at the time of closing. This deal, acquiring already valuable technology that has the potential to be further exploited,[210] demonstrates Facebook's aspirations to become a "one stop shop" for all things social media.[211]

The Facebook-Instagram deal is also an example of another trend seen in social media M&A, primarily in the many transactions to which Facebook as been a party: speedy transactions that close within a two or three day period,[212] a stark contrast from traditional transactions which are significantly longer. Facebook was already a global leader in photo sharing,[213] so why was the firm so aggressive with Instagram? Facebook was behind in the mobile race; this acquisition of mobile-only technology could put the network on the fast track to mobile relevance. Instagram had a vast and faithful member base and an untainted privacy reputation, all assets from which Facebook could stand to benefit. The urgency of the deal was likely due to the threat of competition: just weeks before Facebook swept the mobile mogul off

[207] Heaton, *supra* note 198.
[208] Nick Bilton, *Instagram Testimony Doesn't Add Up*, N.Y. TIMES, Dec. 17, 2012, at B1, *available at* 2012 WLNR 27150344.
[209] Vaughan-Nichols, *supra* note 206.
[210] Jackson, *supra* note 184, at 2.
[211] Frost & Sullivan.
[212] Jackson, *supra* note 184, at 2.
[213] Heaton, *supra* note 198.

of its feet with a $1 billion offer, Instagram had been in negotiations with Twitter.[214] Facebook's poaching practices would not be the only controversy surrounding this deal.

As news broke of the Facebook-Instagram deal, Instagrammers were on high alert for any changes to their terms, given Facebook's track record for privacy violations, and for good reason. Blogs were abuzz with warnings telling users if they did not want to see their Instagram photos to appear in ads, they should tighten their privacy settings, "and then hope Facebook doesn't change its privacy settings again."[215] One blogger accurately predicted that Instagrammers who were distrustful of Facebook practices and did not want the giant having access to their photos would move to another platform.[216] Loyal Instagrammers, content with their property and privacy "rights" under the original Instagram terms, knew it was only a matter of time before Facebook imposed its own controversial terms.[217]

Instagram saw its last day as the safe haven for privacy and property rights in social media on December 16, 2012. The following day, it released a new version of its privacy policy and terms of service, stripping users of the privacy and dignity that made the service desirable to those who take active interest in protecting their privacy. The revisions included terms (1) declaring photos uploaded by users could now be used by Facebook/Instagram, (2) allowing Instagram to share user information with Facebook as well as third parties, (3) granting Instagram licensing rights to the user's account username, likeness, photos and any associated metadata, and actions a users take on the site without any compensation to the user, applicable to all users, including minors, and (4) that paid advertisements may not always be labeled as

[214] Bilton, *supra* note 208 ("The sides had verbally agreed weeks earlier on a price for Instagram of $525 million in cash and Twitter shares.").
[215] *See* Vaughan-Nichols, *supra* note 206.
[216] *Id.*
[217] Heaton, *supra* note 198.

such.[218] The only way users could opt out of any of these terms would be to delete their account; accessing the service in any manner would serve as a user's assent to the new terms.[219] In addition to the changes in service and privacy terms, Instagram announced new terms governing legal remedies, which previously did not exist anywhere in the agreement.[220] These terms included a mandatory arbitration clause, forced waiver of rights to participation in class action lawsuits against the firm except in very limited circumstances, waiver of damages beyond $100, and a limit on statutes of limitation to one year.[221]

Recognizing that privacy concerns, on the rise in tandem with greater monetization of personal information, can damage trust between social media firms and their users and ultimately impact their bottom line, many companies are backtracking from unpopular changes in user terms that generate public protest to show they in touch with users and value their privacy.[222] Suggestions that social media firms are not concerned with reputational backlash because it is not a truly competitive market may now have been silenced by the immediate and powerful response Instagram received to its new terms.[223]

Instagram's about-face on terms of service was a welcomed blunder by other photo-sharing applications. Pheed, similar to Instagram, gives users the option to monetize their

---

[218] Jenna Wortham & Nick Bilton, *What Instagram's New Terms of Service Mean for You*, N.Y. TIMES BITS BLOG, Dec. 17, 2012, 5:02 PM, http://bits.blogs.nytimes.com/2012/12/17/what-instagrams-new-terms-of-service-mean-for-you/.
[219] *Id.*
[220] *Id.*
[221] Dan Levine, *Instagram Furor Triggers First Class Action Lawsuit*, REUTERS, Dec. 24, 2012, *available at* http://www.reuters.com/article/2012/12/24/us-instagram-lawsuit-idUSBRE8BN0JI20121224.
[222] Ozer, *supra* note 41, at 239.
[223] *See* Livingston, *supra* note 45, at 629 (suggesting that users will not substitute their preferred social network, thus social media is not a "truly competitive market.").

content by charging followers to see their photos.[224] This app gained more users than any other in the United States in one day during the week following Instagram's announcement, ranking as the ninth most downloaded app, even ahead of LinkedIn.[225] Another photo app, Flickr, was ranked around the 175th most downloaded app just before the Instagram announcement, and within days had moved into the high twenties on the same list.[226] Ordinary users and celebrities alike were quickly leaving the service. Under the new terms, celebrities who earn a living from their image and identity faced[227] losing control over their ability to earn a livelihood (or at least a portion of it), if the licensing term had been employed to sell their images.[228]

Instagram reversed its terms almost as quickly as it had announced them, blaming "confusing" language for a misunderstanding.[229] Founder and CEO Kevin Systrom deleted the language about displaying photos without compensation, but retained the terms that allow the site to place ads with user content and the mandatory arbitration clause.[230] Systrom announced the firm would go back to the drawing board and fully develop their plans for the future, "then come back to our users and explain how we would like for our advertising business to work."[231]

---

[224] Nicole Perlroth & Jenna Wortham; *Instagram Does an About-Face*, New York Times Bits Blog, 12/20/2012, ts.blogs.nytimes.com/2012/12/20/instagram-does-about-face-reverts-to-previous-policy/ (last visited Mar. 3, 2013).
[225] *Id.*
[226] *Id*.
[227] Users still face this prospect, as Instagram ultimately retained terms that grant the company a free and unlimited license to profit from users' content. *See* INSTAGRAM, Legal Terms, effective Jan. 19, 2013, *available at* http://instagram.com/about/legal/terms/.
[228] See *Zacchini v. Scripps-Howard Broadcasting, Inc.,* 433 U.S. 562 (1977) for a discussion of the common law right of publicity. This is the only Supreme Court decision on the right of publicity. Also see *Motschenbacher v. R.J. Reynolds Tobacco Co.,* 498 F.2d 821 (9th Cir.1974) for a discussion on the unauthorized use of celebrity photographs in advertising.
[229] Perlroth & Wortham, *supra* note 224.
[230] Levine, *supra* note 221.
[231] Perlroth & Wortham, *supra* note 224.

Systom's statement is affirmation that Facebook was hasty in its rush for Instagram, and did not observe the due diligence period. The purpose of acquiring Instagram was clear from the very beginning – Facebook wanted the technology, the minds the behind the technology, the goodwill tied to the app, the user base it could fold into its own network population, and the opportunity to monetize what was already in near-perfect form. A damaging misstep, in the Facebook-Instagram transaction was failing to assess the *synergy* between the two organizations. At the core of all social media firms are their privacy values, which translate into their policies, and it is clear that there was no synergy between the two organizations in this fundamental area.

Systrom's message fell on deaf ears. Instagram's new terms were a total breach of faith for many of its following, and by the end of the week of the announcement, a class action lawsuit was filed in the Northern District of California, seeking declaratory and injunctive relief before the new terms would take effect and bar and claims users may have.[232] The complaint alleges the new terms breached the covenant of good faith and fair dealing implied in the original agreement that still governed the relationship between Instagram and its users; violations of California Civil Code § 3344, unlawful and unfair business practices under California's Unfair Competition Law ("UCL").[233] Specifically, the suit seeks: to have the new terms unilaterally granting Instagram a "transferrable and sub-licensable" license to users' content ("property") voided; a declaration that Instagram cannot make use of users' content without *express* authorization; options so that a user can control how their information and content is used for commercial purposes; a way for users to obtain exclusive control and possession of their content (upon cancellation of their membership with the service); and a declaration that users otherwise

[232] *Funes v. Instagram, Inc.*, *available at* 2012 WL 6640774 (N.D.Cal.) (trial pleading, filed Dec. 21, 2012).
[233] *Id.*

entitled to statutory damages under California's Right of Publicity Statute do not waive damages if this statutory right is violated by Instagram or any of its "sub-licensees."[234] The Complaint chronicles the events and statements made by Instagram in the days leading up to the filing of the suit, calling "[t]he purported concessions by Instagram in its press release and final version of the New Terms…nothing more than a public relations campaign to address public discontent."[235]

The *Funes* suit amounts to a rejection of Instagram's materially altered terms. Since there is no private bargaining between the parties, Funes seeks to have users' desired terms – what they would have counter-offered, had there been a negotiation with Instagram over the terms – forced by the judicial system. As of March 21, 2013 the *Funes* suit has not been dismissed. If the class is successful and the court ultimately grants the remedies sought, the story of Facebook's Instagram acquisition will have an entirely different outcome than Mark Zuckerberg had envisioned when he brokered the deal just last year. Social media will be forced to dedicate the time and resources necessary during the due diligence period of the transactions to assess consumer expectations and attitudes toward the acquirer and its future plans for the acquiree network. Otherwise, they will face the occasion for the transaction being devastated either by market backlash, legal intervention, or both.

It remains to be seen whether Instagram will ultimately be considered a wise decision for Facebook. Talked-about legislation, consumer empowerment, and the outcome of *Funes* could create hurdles for the company to generate revenue through advertising. In the short-term, in terms of dollars and presence, the transaction appears to have been a success. Facebook reported fourth-quarter revenue of $1.585 billion (a forty percent year-over-year increase) and $64 million

[234] *Id.* at ¶¶ 8(a)-(f).
[235] *Id.* at ¶ 20.

in net income.[236] The Facebook community also continues to grow, with the company nearing 1.06 billion active users at the end of 2012, even greater than a number that seemed impossible just a few months earlier.[237] The presumption made in this paper, that Facebook wanted and needed Instagram in part for its mobile technology, is substantiated by its latest cause for a celebration and press conference – more than half of Facebook users are now accessing the network from mobile devices.[238] Even if the company encounters more fallout from the acquisition of Instagram in the future, the procurement of mobile technology will have been the champion of the transaction.

D. *Proposed Best Practices*

The events that occurred as the result of a few terms being changed to a mere photo filter app illustrate the value society as a whole places on technology, the value individuals place on their privacy and identity, and the care social media organizations must take in mergers and acquisitions.

The due diligence period is the time companies take to determine whether the new relationship is going to work at all once the transaction is complete, and the steps that will need to be taken in order to make it to closing and beyond to unite the organizations. These steps must be worked out in detail at this vital point in the process, and research must be thorough. Facebook very aggressively approached Instagram with an offer far beyond the value of the app, and with a zealous plan in mind for monetizing the program, then apparently disregarded this critical stage of the process.

---

[236] Michael Gorman, *Facebook Finishes 2012 On A High Note: Q4 revenue $1.585 Billion, $64 Million In Net Income*, Endgadget.com, Jan. 30, 2013, 4:22 PM, http://www.engadget.com/2013/01/30/facebook-2012-q4-earnings/.
[237] *Id.*
[238] Stone, *supra* note 43. *See also* Gorman, *supra* note 236.

Given the attitude toward social media and its privacy policies, at the outset of an M&A transaction, counsel must dedicate adequate time and resources to examining the existing policies of both the acquirer and the target. During this time the terms should be reviewed for any red flags in either of the policies that an increasingly savvy consumer base is likely to decry and discard them. If the term is critical to the firm's ability to operate according to its business model, the firm should flag the term as a point for negotiating with users. (Negotiating will be an important part of this process, to be discussed in further detail.) If the term is not necessary, or the firm can make concessions to grant users more protection on the point, the term should be discarded or altered accordingly. Altering the term does *not* mean changing language from "we own your content" to "you grant us an unlimited, royalty-free, perpetual license to sub-license and sell your content, even after you cancel your membership." This means developing a pro-provider, pro-consumer compromise that will allow the social network to continue in its business purposes without compromising privacy and property rights of the users. In the example above, this may mean altering the term to read, "you grant us a non-exclusive license to sub-license your content, with your express consent per transaction, and a [reasonable percentage or dollar amount] royalty fee payable to you. This non-exclusive license is revocable upon cancellation of your membership, or may be extended with your express consent, beyond the life of your membership, revocable at any time thereafter." These terms are more amicable to the user, allow the firm to continue in its business practices, but also allow the user to retain control over their words, photos, or other actions on the network.

In addition to focusing on user concerns while reviewing existing policies and drafting a new one, the drafters must keep in mind that users are often confused by the number of privacy policies they encounter on a regular basis, and the length of these policies. In the past, it may

have been beneficial to social media firms to draft lengthy policies crammed with legalese to deter users from reading them. Users are now more aware of the general content of these policies, and are becoming less accepting, as the Instagram debacle demonstrates. It is in a firm's best interest to draft shorter policies friendlier to laypeople and limit the rigid terms that usurp users' rights so absolutely. This is a proactive step to avoid public backlash and the possibility of litigation coming out of a merger or acquisition that can already leave users on edge about the future of their service.

To address all of these points, those dedicated to reviewing and drafting privacy policies must pay attention to users' privacy needs and expectations. This is the "negotiation." A social media firm must be realistic in what they are acquiring, beyond the technology and the business itself, but the community that the site serves. Key issues to identify who the users are, why they are loyal to the service, what about the service appealed to them in the first instance, and what kept them coming back. An acquirer must also look internally, and consider the attitudes the users of the acquiree have toward the acquirer. The best way to do this is through consumer research, surveys, and a look at past legal actions or administrative complaints against each organization party to the transaction. (This task would have served Facebook well had it been done.)

Finally, with regard to any changes as a result of a merger or acquisition, the firm must notify its users of any changes well in advance of any changes taking place. While courts have generally enforced clickwrap agreements containing privacy policies in the past, it us unknown how long that will continue. It must be absolutely clear to the outside, particularly the courts, that users had notice of any terms and changes to terms.

CONCLUSION

The United States has been the envy of much of the world for our rejection of tyranny, recognition of human dignity and fundamental rights, and freedom to pursue success to the greatest degree. As a nation that has embraced technology as an extension of our reality, we now face the threat of tyranny, declining dignity and impairment of rights that are inherent to our being. These conditions are not the doing of an oppressive government, but of private entities that exploit the freedom and openness of our society. There is a delicate balance between over-regulating, which will subdue industry and discourage innovation, and under-regulating, allowing private enterprise to become so powerful that it hijacks individuals' rights. For all its efforts, the United States has yet to find this balance where the Internet and social media are concerned.

This problem can be immediately addressed with action from Congress, the sixty-seven percent of Americans connected to social media, and social media firms. Congress must focus on passing clear, indestructible legislation that establishes a fundamental right to privacy that protects against intrusion by private actors. The more legislative acts that arise on narrow issues, the further we become from finding a baseline of protection the will remain effective as technology evolves. If an individual is to waive their right in any circumstance, like during the registration process for a social network, there must be no question as to whether they understood the consequences or whether they assented at all. Any waiver of the right must also be revocable. An industry group or any other entity cannot be exempt from respecting the right. And from the right must follow the power of the individual to enforce their right against intruders, demand the intrusion cease, and that they be compensated for any resulting harm (assuming one can even be compensated for such an intrinsic harm). Federal legislation will

provide a standard for social media to design its privacy practices from, a standard for users' to set their expectations from, and an even standard for courts to apply, no matter the jurisdiction. This provides as much protection for social media as it does for the individual user. This will not unnecessarily burden social media and its privacy infringing affiliates in light of the potential for damage that current practices have on individuals, but will merely establish a very reasonable limit for these firms to work within.

Individuals must also take action to prove the value of personal privacy by leveraging themselves against social media to demand – and receive – what is expected and well deserved. Users must be vigilant and stay connected to one another – these are "social networks," after all. The outcome of *Funes v. Instagram, Inc.* and future class actions demanding equitable damages may cause enough uncertainty and fear for social media to have an effect on the industry's approach to M&A consolidation, privacy design, and overall business model. For a more immediate effect, users should commit to put down the smart phone, sign off from all social media, and protest in the most damaging way to social media, forcing these firms to acknowledge and respect individuals' privacy. The key to consumer action, no matter the avenue, is the mob mentality. One person – or even a million, now – whining while they continue to use Facebook is not enough. Any effort must be a collective action for social media, Big Data, advertisers, and all other related parties to see the damage on their balance sheets. Without users, social media does not exist.

As the primary offender, social media must be the principal leader in the movement for privacy protection. It will be painful, given the freedom and rapid success the industry has enjoyed, but it must completely rethink its business model and its relationship with consumers. When social media finds a way to produce revenue without exploiting users' privacy, or at least

develop a reasonable alternative that gives users the opportunity to make genuinely informed choice, the practices will necessarily trickle down to other sectors of commerce. As said before, this is a country that *encourages innovation*, and the minds brilliant enough to develop Sponsored Stories and location-based advertising are capable developing a less harmful way to drive revenue. This is not a call for social media to cease to exist or be profitable, nor is the purpose of this paper to create an expectation that social media can exist in a perfect world where there is no harm or compromise necessary. It merely calls for the industry to take the opportunity to self-regulate as the FTC has called for, mend its relationship with consumers, and re-take its position as a benefit to society rather than continuing down the road to tyranny.