BALANCING ANONYMITY, POPULARITY, & MICRO-CELEBRITY: THE CROSSROADS OF SOCIAL NETWORKING & PRIVACY

Brian Kane

What a heavy burden is a name that has become famous too soon.[1]

[1] Quotation Book.com, Quotes by Voltaire, http://quotationsbook.com/assets/shared/pdf/author/7459.pdf (last visited Mar. 4, 2010). Voltaire (1694–1778) was the *nom de plume* of Francois-Marie Arouet, a French philosopher, by far the most popular of his approximately 178 separate pen names used by him. *See* 78 CAMBRIDGE ENCYCLOPEDIA, *Voltaire, Biography, Works, Legacy, the Pen Name "Voltaire", available at* http://encyclopedia.stateuniversity.com/pages/23135/Voltaire.html.

TABLE OF CONTENTS

I. INTRODUCTION

As social networking evolves, a sense of connecting coupled with a fear of being left behind encourages users to actively share information through these sites.[2] The intensity of the pressure cannot be discounted, particularly when considering that eighty-five percent of Internet users, ages 18–34, have visited Facebook, Myspace, or Twitter, and eighty-four percent of users, ages 18–29, check one of the social networking sites at least once a week.[3] From a privacy and information perspective, those are powerful numbers. These numbers are made more powerful when one stops to consider that one hundred percent of these users are voluntarily sharing their information.[4]

Consider for a moment the marketability of the information shared on each of those profiles, which conveniently show "friends"[5] who share the same interests, backgrounds, hobbies, and alma maters to start.[6] With these connectors in mind, Facebook solicits and pre-populates[7] information for your profile in three categories titled, Basic, Education, and Work.[8]

---

[2] *See* Ian Shapira, *In a Generation That Friends and Tweets, They Don't*, WASHINGTON POST, Oct. 15, 2009, *available at*: http://www.washingtonpost.com/wp-dyn/content/article/2009/10/14/AR2009101403961.html?wprss=rss_print/asection. Sometimes the encouragement can become intense social pressure, as in the case of Tomek Kott, who was the subject of a Facebook group entitled, "Tomek Kott Must Join Facebook." As pernicious as this group seems, he would remain blissfully unaware of it, unless he visited Facebook, or had friends who told him of it—which in this case is likely considering that Tomek's wife initiated the group. *Id.*

[3] *Id.*

[4] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, And Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 642 n.112 (2008) (citing James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 10–11 (2005)).

[5] Yet another form of not-so-latent encouragement, connections on these sites are termed "friends" to encourage connecting through this cheerful, happy designation. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1162–63 (2009).

[6] *Id.* at 1149.

[7] One of the innovative technologies Facebook possesses is the ability to use your links to other friends, or the information they have provided about you to gather more information about you. For example, when you friend someone, you can say how you know them—such as the high school you attended together. Facebook can then update your profile's information to reflect this gathered information. *See* Facebook, Facebook's Privacy Policy, http://www.facebook.com/policy.php (last visited Mar. 25, 2010).

[8] Facebook, Express Yourself: Set Up Your Facebook Profile, http://www.facebook.com/help/?guide=set_up_profile# (last visited Mar. 22, 2010).

Conveniently, through these profile prompts, a user can integrate instant messaging, photo sharing, twitter accounts, websites, and host of other information into their profiles.[9] Add in third party applications and the information accessible is virtually boundless.[10] But this information aggregation doesn't end with the limits of current social networks. Increasingly Web 2.0 is evolving into what is known as the semantic web.[11] As our online personas become more integrated with one another, information is willingly traded in return for "friends," status, and even micro-celebrity.[12] With the permanence that attends our uploaded lives, the law is increasingly considered to be a primary haven for the future of privacy.

But as society looks to the legal system for remedies, there can be no denying that the system is struggling to adjust to both the permanence and pervasiveness of information transfers via social networking sites.[13] The most significant hurdle to adequate legal privacy protection is often the information that participants willingly place onto the Internet about themselves,[14] particularly

[9] *See* Facebook's Privacy Policy, *supra* note 7.

[10] Grimmelmann, *supra* note 5, at 1146; *see also* Facebook, Build and Grow with Facebook: Bring Identity and Connections to Your Site or Application, http://developers.facebook.com/ (last visited Mar. 22, 2010).

[11] Jonathan Richards, *Google Could Be Superseded, Says Web Inventor*, TIMES ONLINE (London), Mar. 12, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article3532832.ece (last visited Mar. 2, 2010).

[12] Grimmelmann, *supra* note 5, at 1158 (noting that a stand-up comedian racked up 182,000 friends, and that Facebook has since capped the number of friends at 5000). A social networking site has emerged that expressly rewards the accumulation of friends. Foursquare, http://foursquare.com/learn_more (last visited Mar 22, 2010); *see also* Posting of David Armano to http://blogs.harvardbusiness.org/cs/2009/11/six_social_media_trends.html (Nov. 2, 2010, 09:54 AM).

[13] But Courts also recognize the utility of social networking. For example Australian Courts have permitted the service of documents on defendants' Facebook sites. Noel Towell, *Lawyers to Serve Notices on Facebook,* THE AGE, Dec. 16, 2008, *available at* http://www.theage.com.au/technology/biz-tech/lawyers-to-serve-notices-on-facebook-20090615-cbhe.html. New Zealand has similarly embraced Australia's lead. *Kiwi Judge Follows Australian Facebook Precedent*, THE AGE, Mar. 16, 2009, *available at* http://www.theage.com.au/technology/technology-news/kiwi-judge-follows-australian-facebook-precedent-20090615-ca5o.html.

[14] Consider a teacher who was fired because parents were upset over a picture in which the teacher is shown holding an alcoholic drink. Two questions are immediately presented: first, is it appropriate for a teacher to post this type of photo (vacation photos for friends to see) and second, is the response of the school/parent reasonable? Deidra Dukes, *Teacher Fired Over Facebook Posts*, myFOXphoenix.com, Nov. 11, 2009, http://www.myfoxphoenix.com/dpp/news/national/teacher_fired_facebook_111109 (last visited Mar. 22, 2010).

when contemplating the creation of micro-celebrities in the social networking context. Some protection may be afforded to those who have not placed the information on the Internet, but have had personal or private information about them placed onto a social networking site. Greater legal protection is due those whose information has been improperly accessed, an identity fraudulently assumed, or some other measure of deception to invade a user's privacy—provided the bad actor can be located and caught.[15]

This article will provide an overview of social networking, including its information collecting, sharing, and integrating capabilities. The second part will critique the developed privacy torts, and present an alternative. Part four will examine the limitations of several proposed solutions and weigh their likely effectiveness. The article will conclude by looking forward at likely solutions and prescriptions designed to enhance user privacy as he or she engages in social networking platforms.

II. SOCIAL NETWORKING AND BEYOND

A. Not All That New

Social networks have been in existence for as long as people have existed. Importantly social networks have existed in beneficial as well as toxic forms for centuries. Perhaps among the most beneficial of social networks was Paul Revere's midnight ride network,[16] while among the most toxic was Typhoid Mary's.[17]

---

[15] In a case pursued by the Idaho Office of Attorney General, the office tracked an offender through twelve different servers beginning in the United States, through Australia and Indonesia, until the trail went cold in Russia. One of the frequent frustrations of enforcement entities is that the trail goes cold.

[16] Two men were responsible for raising the militia—Paul Revere and William Dawes, only Paul Revere succeeded. The explanation for this is that Revere was an expert social networker who knew the right doors to knock on to keep the word spreading, while Dawes knocked on doors of people he knew, but they did not necessarily continue to spread the message. Brian Uzzi and Shannon Dulap also note that this distinction was made in Malcolm Gladwell's, *The Tipping Point*. Brian Uzzi & Shannon Dunlap, *How to Build Your Network*, HARV. BUS. REV. 53–63, Dec. 2005, *available at* http://hbr.org/2005/12/how-to-build-your-network/ar/1.

[17] Mary Mallon infected more than fifty people with Typhoid Fever, though never suffering from the disease herself. As the central node of this network, each of the victims was tied to Mary through her work within their households. Jennifer Rosenberg, *Typhoid Mary*, About.com, http://history1900s.about.com/

All social networks operate in the same manner. Members[18] are connected to one another through some commonality such as high school attended, college graduated, sports teams, interests, or hobbies.[19] The types of commonality to establish a tie are virtually limitless. The nodes are the individuals or personalities within the network, while the ties are the relationships that connect them.[20] The most basic social network thus, is a family. As we mature, our social networks become increasingly complex based on our backgrounds, social interests, careers and so on. Computers have enabled much more concentrated attention on social networks, particularly through the creation of computerized social networks. But this enabling and convenience also come with peril as the most frequent commodity traded within this privacy equation is information[21] for convenience.

With this backdrop, social networking on the Internet consists generally of at least three elements: (1) a platform on which a user may construct a profile using a system that is either open or closed; (2) an ability to share the profile with other users also having profiles (or in many cases to invite users to also construct profiles for sharing); and (3) the ability to navigate through the user's own profile as well as through other users' shared profiles.[22] Within the social networking context, the sharing and navigability of the profiles is often the most recognizable component. In sum, the driving force of social networking is

od/1900s/a/typhoidmary.htm (last visited Mar. 22, 2010).

[18] Technically the term within a social networking context is "nodes." Orgnet.com, Social Network Analysis, A Brief Introduction, http://www.orgnet.com/sna.html (last visited Mar. 27, 2010). This piece will simply identify "nodes" as members, users, or individuals for readability purposes.

[19] Sander J.C. van der Heide, *Social Networking and Sexual Predators: The Case for Self-Regulation*, 31 HASTINGS COMM. & ENT L.J. 173, 175–76 (2008).

[20] Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges and Promises of User-Generated Information Flows*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 741, 746–47 (2008).

[21] Worth noting, the information shared is not necessarily personal. A British survey recently found that fifty-seven percent of staff used Twitter, Facebook, or other networking sites, at times disclosing business information. The survey estimated that employers lost the equivalent of a week's worth of work per year on these sites. *The World This Week*, THE ECONOMIST, Oct. 31–Nov. 6, 2009, at 10.

[22] Grimmelmann, *supra* note 5, at 1142 (citing Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM., art. 11 (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

information exchanges between users—this information becomes the single most important asset of the social network site.[23]

B. A Concise History of Online Social Networks

It is easy to argue that the creation of social networks was a primary impetus behind the development of the Internet.[24] The earliest uses of networked computers focused on enabling users to communicate with one another.[25] The launch of Sputnik led to an immediate need for scientists in particular to share research and information between one another.[26] Among the earliest identifiable social networking sites was The WELL, which was created by Stewart Brand and Larry Brilliant in 1985.[27] The next social networking efforts focused on the creation of webpages and chatrooms which users could link together through sites such as Geocities[28] and Tripod.[29] These gave way to

[23] *See* Grimmelmann, *supra* note 5, at 1149, 1193.

[24] Consider that one of the first uses of a network and e-mail enabled users to communicate with one another while sharing time on a mainframe computer. Ian Peter, *The History of Email*, NET HISTORY (2004), http://www.nethistory.info/History%20of%20the%20Internet/email.html (last visited Mar. 22, 2010).

[25] *Id.*

[26] KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (Simon & Schuster 1998).

[27] *See* TheWell.com, Learn About the Well, http://www.well.com/aboutwell.html (last visited Mar. 22, 2010); Katie Hafner, *The Epic Saga of The Well*, WIRED, May 1997, *available at* http://www.wired.com/wired/archive/5.05/ff_well_pr.html (noting that The WELL is likely considered an anomaly in the context of social networking in that it requires a real name and paid membership to participate. Notably, the founders of the Electronic Freedom Foundation met each other through The WELL, and formed to represent other WELL users in a lawsuit against the Secret Service); John Perry Barlow, *A Not Terribly Brief History of the Electronic Frontier Foundation*, Electronic Frontier Foundation (1990), http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/not_too_brief_history.html (last visited Mar. 25, 2010); *see* Cliff Figallo, *The WELL: Small Town on the Internet Highway System*, Electronic Frontier Foundation (1993), http://w2.eff.org/Net_culture/Virtual_community/well_figallo.article (last visited Mar. 9, 2010) (noting that the Electronic Frontier Foundation was born from The Well free speech movement); Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

[28] Created in 1995 by Beverly Hills Internet, Geocities was once the Facebook of the Internet, rising to the top of Internet usage statistics. Businesswire.com, Beverly Hills Internet, Builder of Interactive Cyber Cites, Launches 4 More Virtual Communities Linked to Real Places, http://findarticles.com/p/articles/mi_m0EIN/is_1995_July_5/ai_17190114/ (last visited Mar. 22, 2010). Geocities was purchased by Yahoo near the height of its popularity, but has since been shuttered. CNN MONEY, Yahoo! Buys GeoCities, http://money.cnn.com/1999/01/28/technology/yahoo_a/ (last visited Mar. 22, 2010).

[29] Tripod, like Geocities, was created in 1995 and eventually was purchased

Sixdegrees.com[30] and Classmates.com,[31] the most direct predecessors of current social networking sites because they allowed for users to join and link with others based upon a common node such as high school or college attended, or a common hobby.

1. From MySpace To Facebook

Nodes of commonality became the impetus for the most recent evolution of social networking sites.[32] MySpace was launched in 2004 and within two months tallied more than 1 million members.[33] MySpace connects people through profiles, photos, videos, mobile devices, instant messaging, games and music interests.[34] Approximately a month after MySpace was created, Facebook was launched.[35] The interest in Facebook, although upon creation intended only for students at Harvard was met with enthusiasm equal to MySpace's. Within the first day, 1,200 students had joined, and within the first month half the

by Lycos. Tripod bears little similarity to its original appearance or capabilities, now serving primarily as a web hosting service. Wikipedia, Tripod.com, http://en.wikipedia.org/wiki/Tripod.com (last visited Mar. 22, 2010).

[30] With a name clearly based on the cult game "Six Degrees of Kevin Bacon" wherein a player links any actor or actress within six other actors or actresses to Kevin Bacon, as well as the prediction of Italian inventor Gugliermi Marconi that in the future everyone would be connected within 5.83 contacts. Sixdegrees.com was founded in 1997. *See* Doug Bedell, *Meeting Your New Best Friends Six Degrees Widens Your Contacts In Exchange For Sampling Websites*, THE DALLAS MORNING NEWS, Oct. 27, 1998, http://www.dougbedell.com/six degrees1.html; Patrick Reynolds, *About the Oracle of Bacon*, http://oracleof bacon.org/help.php (last visited Mar. 28, 2010).

[31] *See* Classmates.com, About Classmates Online, Inc., http://www.class mates.com/cmo/about/;jsessionid=ZGJZPN1BE3NBMCQKWZTCT5Q?_requesti d=2195417 (last visited on Mar. 28, 2010) (detailing the way in which users connect via Classmates.com).

[32] *See* Sweetbusinesses.com, Why Social Networking Sites are so Popular, http://www.sweetbusinesses.com/2009/12/27 (last visited Mar. 22, 2010).

[33] MySpace, MySpace Press Room Fact Sheet, http://www.myspace.com/press room?url=/fact+sheet/ (noting MySpace launch date of Jan. 2004) (last visited Mar. 28, 2010); MySpace, MySpace Press Room Timeline, http://www.myspace. com/pressroom?url=/timeline (MySpace gets 1 millionth member) (last visited Mar. 28, 2010).

[34] MySpace Press Room Fact Sheet, *supra* note 33.

[35] Facebook, Facebook Press Room Factsheet, http://www.facebook.com/press/ info.php?factsheet (noting Facebook was founded in Feb. 2004) (last visited Mar. 28, 2010); *see also* John Markoff*, Who Founded Facebook? A New Claim Emerges,* N.Y. TIMES, Sept. 1, 2007, *available at* http://www.nytimes.com/2007/ 09/01/technology/01facebook.html (noting that although Mark Zuckerberg is largely recognized as the creator of Facebook, there are several others making the same claim).

undergraduate students at Harvard had joined.[36] A little over a year and a half later, Facebook claimed membership of virtually eighty-five percent of the students within the 882 colleges permitted access.[37]

Both Facebook and MySpace enjoy staggering numbers of members and visitors, which now number over 150 million in the United States alone.[38] Considering the number of users on each of these sites, it is also worth noting that the average user spends more than 20 minutes per visit to either Facebook or MySpace.[39] Considering the massive numbers of users on these sites, privacy emerges as the five hundred pound gorilla in the room as the most valuable component of users is their information;[40] users are placing a premium on the protection of their information.[41] But these social networks are on the threshold of even more significant evolutions making the balance between available information and protection of privacy even more precarious.

2. No Secret Is Safe

The technological evolutions are a significant part of the appeal of social networking sites. Using Facebook as an example, the network is established as an open platform, meaning that anyone can develop an application for use within Facebook.[42]

[36] Sarah Phillips, *A Brief History of Facebook*, GUARDIAN, July 25, 2007, *available at* http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia.

[37] Posting of Michael Arrington to http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook/ (Sept. 7, 2005) ("85% of college students use facebook"). Most likely the more significant number out of these statistics is that sixty percent of the eighty-five percent were logging in daily to check their Facebook accounts. *Id.*

[38] In August 2009, Facebook had more than ninety-two million discrete users in the United States, while MySpace had more than sixty-four million. Knowledge@Wharton, *Early Tremors: Is It Time For Another Social Network Shakeout?*, Oct. 14, 2009, http://knowledge.wharton.upenn.edu/printer_friendly.cfm?articleid=2354.

[39] Jack Marshall, *Top Social Networking Sites in September 2009*, CLICKZ, Oct. 13, 2009, http://www.clickz.com/3635292.

[40] *See* Erica Naone, *Unmasking Social-Network Users,* TECHNOLOGY REVIEW, May 6, 2009, http://www.technologyreview.com/web/22593/?a=f; Posting of Michael Arrington to http://www.techcrunch.com/2009/06/04/the-true-value-of-social-networks-the-2009-updated-model/ (June 4, 2009) (illustrating the value of a social networking users personal information).

[41] *See* Startups, *Security Concerns Over Facebook*, Aug. 21, 2007, http://www.startups.co.uk/667884290838292224 4/security-concerns-over-facebook.html (noting the concern of individuals and employers regarding private information that can become available through Facebook).

[42] Facebook, Developers, Get Started, http://developers.facebook.com/get_

This open platform does not come without its perils, because some of the applications may be hacked.[43] But the open platform also enables connectivity throughout the Internet.[44] Facebook introduced Beacon as a partnership with forty-four other sites in November 2007 as a means through which a user logged into Facebook would send a notification of what other sites he or she was visiting.[45] In other words, if you were on a site using Facebook Beacon, such as eBay, then your auction listings could be found through your Facebook profile.[46] Similarly, if a Facebook member made a transaction through a connected merchant for the purchase of a game,[47] or video[48], their Facebook profile would be updated with that information.[49]

With this type of connectivity, concerns about privacy immediately arose.[50] Although the Beacon service came with an opt-out, it was an opt-out that many users never fully recognized,

started.php (last visited Mar. 28, 2010) (Facebook has, however, identified three core skills for potential developers: "(1) Well versed in a coding language supported by Facebook; (2) Basic understanding of the Internet, SSH, MySQL, and Unix; and (3) Web hosting familiarity and a host site.").

43 Brian Krebs, *Researcher: Hackers Hijack Some Facebook Apps*, THE WASHINGTON POST, Oct. 15, 2009, *available at* http://voices.washingtonpost.com/securityfix/2009/10/hacked_facebook_apps_lead_to_m.html (noting that malicious strings of code were inserted following the development of the application discussed, and that generally when Facebook learns of these instances, the application is removed while the malicious code is investigated); *see also* Developers, *supra* note 42 (noting the open nature of app design for Facebook).

44 Grimmelmann, *supra* note 5, at 1147.

45 *Id.*; *see also* Lane v. Facebook, Inc., No. C 08-3845, slip op. at 1 (N.D.Cal. Oct. 23, 2009).

46 Facebook, Press Release, Leading Websites Offer Facebook Beacon for Social Distribution (Nov. 6, 2007), http://www.facebook.com/press/releases.php?p=9166 (last visited Mar. 28, 2010).

47 Posting of Mike Monteiro to http://weblog.muledesign.com/2007/11/facebook_you_owe_me_one_christ.php (Nov. 20, 2007 11:22 PM); *see also* Corvus Elrod, *Gamefly Launches Facebook Beacon,* THE ESCAPIST, Nov. 16, 2007, *http://www.escapistmagazine.com/news/view/79037-Gamefly-Launches-Facebook-Beacon* (noting that Gamefly is a Beacon Participant).

48 The Laboratorium, http://laboratorium.net/archive/2007/12/10/facebook_and_the_vppa_uhoh (Dec. 10, 2007, 1:14 AM) (pointing out that Facebook and Blockbuster likely violated the Video Privacy Protection Act because Beacon notifications disclosed the movies that users were purchasing.); *see also* 18 U.S.C. § 2710 (1988); *Lane*, No. C 08-3845, at *1.

49 Grimmelmann, *supra* note 5, at 1147 (Grimmelmann uses the example of using Epicurious.com to search for a recipe.).

50 *Lane*, No. C 08-3845, at *1; Harris v. Blockbuster Inc., 622 F. Supp.2d 396, 397 (N.D.Tex. 2009); *see also* 18 U.S.C. § 2710 (1988).

and therefore ignored as yet another annoying pop-up.[51] Worse yet for privacy minded web users, the window appeared in the lower right hand corner of the computer screen, and disappeared on its own after approximately ten seconds.[52] Facebook equated inactivity with regard to the pop up opt-out window as consent.[53] In response to this outcry, Facebook modified the default setting on Beacon to become an opt-in, and permitted users more control over their use of Beacon.[54] Ultimately, Facebook turned Beacon off as a means of settling a class action lawsuit,[55] but it appears to have returned bigger, better, and under a new name: Facebook Connect.

Facebook Connect creates greater interplay among sites and users than Facebook Beacon, but has failed to attract Beacon's privacy concerns.[56] One of the primary marketing points of Facebook Connect is that it allows other web sites to use Facebook's log-in API.[57] This means that when a user logs into a participating website, a user may be simultaneously logging into

[51] Grimmelmann, *supra* note 5, at 1148; *see also* Monteiro, *supra* note 47; My Heart's in Accra, http://www.ethanzuckerman.com/blog/2007/11/15/facebook-changes-the-norms-for-web-purchasing-and-privacy/ (Nov. 15, 2007, 12:42 PM).

[52] My Heart's in Accra, *supra* note 51.

[53] *Id.* Silence as consent is particularly intriguing within this context because depending on the circumstances, legally you reach opposite conclusions. In the scenario most akin to privacy, that of search and seizure for example, silence does not equate consent. *See* Gates v. Texas Dep't of Protective and Regulatory Servs., 537 F.3d 404, 420 (5th Cir. 2008); United States v. Shaibu, 920 F.2d 1423, 1426 (9th Cir. 1990). But silence definitely carries numerous meanings with it. *See* Commonwealth v. Dravecz, 227 A.2d 904, 906 (Pa. 1967); Maria L. Ontiveros, *Adoptive Admissions and the Meaning of Silence: Continuing the Inquiry Into Evidence Law and Issues of Race, Class, Gender, and Ethnicity*, 28 SW. U. L. REV. 337, 341–45 (1999).

[54] Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, *available at* http://www.nytimes.com/2007/11/30/technology/30face.html?_r=2&scp=1&sq=&st=nyt.

[55] As part of the settlement, Facebook agreed to turn Beacon off and pay $9.5 million to create a foundation which will promote online privacy and security. Jacqui Cheng, *Facebook Beacon Shines for Last Time as Part of Settlement*, ARSTECHNICA, http://arstechnica.com/web/news/2009/09/facebook-beacon-shines-for-last-time-as-part-of-settlement.ars (last visited Mar. 28, 2010).

[56] Posting of Josh Catone to http://www.sitepoint.com/blogs/2008/07/24/facebook-connect-is-beacon-done-right/ (July 24, 2008, 11:23 AM).

[57] *See* Rafe Needleman, *Facebook Connect Officially Open*, CNET NEWS, Dec. 4, 2008, http://news.cnet.com/facebook-connect-officially-open/?tag=mncol;txt. API is known as the application programming interface, which enables software programs to communicate with one another; in simplest terms, Facebook has opened its log-in system to any website wishing to use it. *See* Posting of Ray C. He to http://developers.facebook.com/news.php?blog=1&story=225 (last visited Mar. 28, 2010).

their Facebook account to provide an update of their activities on the users' Facebook page.[58] The benefits to users and web merchants are twofold. First the user does not have to create site specific log in information.[59] Second the web provider streamlines their transaction process and gains the marketing power of Facebook's automatic updating feeds.[60] This is a daunting perspective from a privacy standpoint because more than ninety million Facebook users can now automatically connect with more than fifteen thousand Facebook merchants.[61] But this connectivity may be only the portion visible above the water.

C. Limitless Connectivity

Connectivity is no longer limited to computers. Virtually every facet of our lives is now connected. Computers can connect to televisions to enable remote watching of programming using mobile devices such as the iPhone.[62] Electricity usage can even create an accumulation of information about a user. Consider for example, "smart grid" technology that collects your habits including the fact that on Friday and Saturday nights, you turn on the lights in your house at 2:30 a.m., and then shares that information with your car insurance company.[63]

Most people generally recognize that cell phones have global positioning (GPS) capabilities. For example, when you dial 911, even if you don't know where you are, the responders do.[64] But this capability has recently been applied in a way that significantly threatens personal privacy. In New York City for

[58] Posting of Ray C. He, *supra* note 57.

[59] Needleman, *supra* note 57.

[60] *See* Facebook Developers Wiki, *Publishing Feed Stories to Facebook,* http://wiki.developers.facebook.com/index.php/Publishing_Feed_Stories_to_Facebook (last visited Mar. 28, 2010).

[61] *See* Needleman, *supra* note 57 (discussing Facebook users); Facebook, Facebook Connect Help Center, http://www.facebook.com/help/?page=730 (select "What Sites Support Facebook Connect?") (discussing merchants on Facebook) (last visited Mar. 31, 2010).

[62] *See* Josh Catone, *iPhone TV: Top iPhone Apps for Live Streaming Television*, MASHABLE: THE SOCIAL MEDIA GUIDE, Aug. 8, 2009, http://mashable.com/2009/08/08/iphone-live-tv/ (last visited Mar. 28, 2010).

[63] *See* Posting of Bob Sullivan to http://redtape.msnbc.com/2009/10/would-you-sign-up-for-a-discount-with-your-power-company-in-exchange-for-surrendering-control-of-your-thermostat-what-if-it.html#posts (Oct. 9, 2009, 05:00 CT).

[64] *See* FCC, Wireless 911 Services, http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html (last visited Mar. 30, 2010).

example, when police officers arrest a suspect, they are now logging the International Mobile Equipment Identity number, which is unique to each phone.[65] This reflects a growing fascination with the accumulation of data about people. If privacy is approached as a limitation on other people's access to an individual,[66] then the increasing accumulation of information about people is particularly troubling.

D. Augmented Reality

The ever increasing accumulation of information may present the most pressing problem with regard to privacy on the Internet. Consider for moment that you are walking down a street, you observe someone taking a cell phone photo. What individuals don't realize is that through tagging[67] of your photo on the Internet and the use of facial recognition software,[68] the person who has taken the photo now knows your name, your political affiliation, religious organizations, as well as what blogs you read, and a list of your "friends" on Facebook.[69] Even those with the least to hide within society would likely balk at this aggregation of information.[70] But this capability is emerging

[65] *NYPD Tracking Cell Phones*: *Report*, NBC NEW YORK, Oct. 8, 2009, http://www.nbcnewyork.com/news/local-beat/NYPD-Tracking-Cell-Phones-Report-63744882.html. Interestingly, this tactic's usefulness may be limited because Chinese made cell phones sold in India all have the same number, and other overseas phones have fake numbers. *Id.*

[66] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

[67] *See* Flickr.com, Help: Tags, http://www.flickr.com/help/tags/#37 (last visited Jan.30, 2010) (tagging is a means by which users can identify the participants, location, or other details of a photo).

[68] *See* Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1871–72 (2007) (discussing facial recognition software such as Polar Rose, which takes a tagged photo, matches faces with the tagged photo by searching the Internet, and tags the new photo).

[69] Jamais Cascio, *Seeing Too Much*, *How the Advent of "Augmented Reality" Threatens Civilization*, 304 ATLANTIC MONTHLY 34, n.4 (Nov. 2009), *available at* http://sks.sirs.es.vrc.scoolaid.net/cgi-bin/hst-article-display?id=SNY5270-0-6545&artno=0000298403&type=ART&shfilter=U&key=Internet%20filtering%20software&title=Seeing%20Too%20Much&res=Y&ren=N&gov=N&lnk=N&ic=N.

[70] In fact, someone of this sort without any affiliation may wind up shunned by prospective friends, business leads, and others based on their lack of involvement, or involvement in unpopular conservative causes. *Id.* In the article, a targeting and censorship of people based on contributions to political campaigns such as Sarah Palin's or an SUV ban are used as examples of how the technology can be used to block or target through the use of filters these individuals. *Id.*

under the banner of "Augmented Reality."[71]

Augmented Reality may be only a piece of what is being called the semantic web.[72] Google has expressly stated that one of its primary limitations is that it does not have enough information about people.[73] Primary in its quest for more information is Google's capability to cross index a user's web searches with cookies left by the sites visited by the same user.[74] This cross referencing will thereby enable Google to offer advertisers the ability to more specifically target their goods and services.[75] In its most aggressive posture, this capability may enable what is known as "transaction hijacking," where the platform will sense when a user's purchase is imminent, and leap in with an offer from a competitor for a lower priced, or better product, or some other combination of options.[76]

E. Easily Mined, Aggregated & Searched

As information gathering has taken off, concern over it has mirrored it.[77] Consider thirty years ago, if you were to accumulate the information that can be accumulated on a simple thumb-drive, likely consisting of about two gigabytes of information, which is the equivalent of twenty yards of books on a shelf.[78] Now imagine that replicated throughout the Internet for people, a series of waypoints containing information about people that you could manually search.[79] You would probably

[71] *Id.*

[72] *See* Richards, *supra* note 11.

[73] Caroline Daniel & Maija Palmer, *Google's Goal: To Organise Your Daily Life*, FIN. TIMES (London), May 22, 2007, http://www.ft.com/cms/s/2/c3e49548-088e-11dc-b11e-000b5df10621.html.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306–08 (The Univ. of North Carolina Press, 1989), *available at* http://books.google.com/books?hl=en&lr=&id=YIZjmNfmuX0C&oi=fnd&pg=PR13&dq=Protecting+Privacy+in+Surveillance+Societies,&ots=Zzd0IFvFUB&sig=6gLst_v5AvCfh_UyGJHGO5bbWfo#v=onepage&q=&f=false (click "contents", and then click the page number) (noting that privacy concerns and advocacy arose almost simultaneously with the realization of the data collecting power of the U.S. Government through the use of mainframe computers); *see also* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES AND PUBLIC POLICY, 70 (The Univ. of North Carolina Press) (1995).

[78] James S. Huggins' Refrigerator Door, How Much Data Is That?, http://www.jamesshuggins.com/h/tek1/how_big.htm (last visited Mar. 31, 2010).

[79] But this should not be read to discount the importance of the information, or the type of information. For example, most information on the Internet

feel pretty good about your privacy because it would be so labor intensive to put together an accurate picture from massive collections of information such as this.

But computers have completely streamlined this process through the use of databases, cross platform search engines, file sharing, and most significantly social networking.[80] Now all it takes to learn about someone is a name and perhaps some distinguishing piece of information such as their college attended, or who they work for, and a search engine.[81] More directly, a quick search following an employee calling in sick may lead to the discovery of posted information leading to that employee's termination.[82]

Externally, this appears to be a privacy nightmare, until one realizes that much of the information has willingly been placed on to the Internet by the "victim." This action must become part of the privacy equation. This also exhibits why privacy determinations are rife with subjective flaws. For example, our grandparents' definition of privacy, particularly with regard to intimate details, differs from our parents', whose definition differs from the current generation, and so forth.[83] In other

about people falls into one of two categories: Personal Identifying Information, and Demographic or Preference Information. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, 20 (1998), *available at*: http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[80] *Id.* at 39–40.

[81] *See* Gina Trapani, *How to Track Down Anyone Online,* LIFEHACKER, Dec. 3, 2007, http://lifehacker.com/329033/how-to-track-down-anyone-online. Consider a simple Google search for a person with only a name and a city or state. Often, that search will return the person being searched for within the first page of results. *See generally*, Google, www.google.com.

[82] *See Woman Loses Benefits over Facebook Photos*, MSNBC, Nov. 22, 2009, http://www.msnbc.msn.com/id/34089972/ns/world_news-weird_news/?GT1=43001 (noting that a woman diagnosed with severe depression had her sick leave benefits terminated after posting photos of herself on vacation and with Chippendale's dancers on her Facebook page); *see also* Ismat Sarah Mangla, *Fired for Facebook: Don't Let It Happen To You*, CNN MONEY, Apr. 21, 2009, http://moneyfeatures.blogs.money.cnn.com/2009/04/21/fired-for-facebook-dont-let-it-happen-to-you/ (noting that a 22 year old "tweeted" about a job offer stating that Cisco had offered her a job, and that she was weighing whether the "fatty paycheck" was sufficient to mitigate the commute and hatred of the work; a Cisco employee saw the post and the job offer was rescinded). The Internet is rife with stories of individuals getting fired for Facebook posts and pictures. A simple search through Google returns numerous scenarios involving web postings that are later read, and end almost universally in termination of the employee. *See generally,* Google, www.google.com.

[83] Even ten years ago, Professor Allen contemplated whether individuals had any expectation of privacy anymore using reality shows, Oprah, and Jerry

words, as we contemplate privacy, societal norms must come into play, which creates a generational dynamic with regard to how privacy is defined.

F. Unintended Consequences

The largest dilemma posed by the intersection of social networking and privacy is that of unintended consequences. Much of the technology has been developed for appropriate purposes, but nefarious uses of otherwise nobly purposed inventions abound. Consider for example that MySpace was originally created as a way for local bands to cultivate fan bases, line up gigs and share information.[84] Facebook was created to permit students at Harvard to connect with one another.[85] One of the similarities between these sites is that they operate on open platforms, which enable users to develop applications that then run within the social networking site.

The same sharing and adaptive technology that make the Internet such a useful piece of society makes it an equally troubling tool from the privacy perspective. Consider the following data accumulation examples:

- Banks collect information based on the stores you shop at and based on where you shop, the cardholder's credit limit is raised, lowered, or remains the same.[86]
- Students at M.I.T. created a Facebook application that surveys your profile and friends and predicts your sexual preference.[87]
- Consider purchasing your spouse[88] or child[89] a gift that

Springer as her basis, given the intimacies shared within the context of each of those and similar shows. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 736–37 (1999).

[84] *See* Randomhistory.com, "A Place for Friends:" A History of MySpace, http://www.randomhistory.com/2008/08/14_myspace.html (last visited Mar. 31, 2010).

[85] John Cassidy, *ME Media: How Hanging Out on the Internet Became Big Business*, THE NEW YORKER, May 15, 2006, at 50, *available at* http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy?currentPage=1.

[86] Mike Stuckey, *AmEx Rates Credit Risk by Where You Live, Shop*, msnbc.com, Oct. 7, 2008, http://www.msnbc.msn.com/id/27055285/.

[87] *See* Dan Macsai, *MIT's Facebook "Gaydar"-Is it Homophobic?*, FASTCOMPANY, Sept. 21, 2009, http://www.fastcompany.com/blog/dan-macsai/popwise/mits-facebook-gaydar-it-homophibic.

[88] *See* Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, WASHINGTON POST, Nov. 30, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112

is then posted as an update to your Facebook profile.

Each piece of information referenced above is readily provided by the user. For example, the M.I.T. application analyzes the list of friends, which is accessible even through an otherwise private Facebook profile, to determine the sexual preference of men.[90] From a privacy standpoint, this is particularly troubling because it removes control of one's intimate information[91] and places it into the discretion of the public domain. Equally difficult is the identification of a solution.

III. THE PROBLEM WITH PRIVACY TORTS

A. "When you come to a fork in the road . . . Take it."[92]

The law has contemplated the existence of privacy from its earliest reported commentaries. Consider the famous saying, "A man's home is his castle."[93] The concept of individuals having places into which the government or others could not intrude resonated within legal circles, and became one of many themes, which emerged through the Bill of Rights.[94] The basis for privacy was revisited in the landmark article, *The Right to Privacy*, in which privacy was equated with the "right to be let alone."[95]

902503.html (detailing the ruining of a surprise by a husband who purchased a diamond ring intended as a Christmas present for his wife from the website Overstock.com when the purchase was made into a headline through the newsfeed feature on Facebook and broadcast to 500 classmates at Columbia University, 220 other friends on the site, and his wife).

89 Mike Monteiro purchased a video game for his children which was also broadcast through Beacon onto his Facebook profile. The gift was ruined because along with all of his other friends, his children also saw the purchase. Monteiro, *supra* note 47.

90 Macsai, *supra* note 87.

91 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487 (2006).

92 YogiBerra.com, Quotes From Yogi Berra, http://www.yogiberra.com/yogi-isms.html (last visited Jan. 23, 2010).

93 *See* Semayne's Case, 77 Eng. Rep. 194, 196 (1604). The actual text used by Sir Edward Coke is, "That the house of everyone is to him as . . . his castle and fortress, as well for his defence against injury and violence, as for his repose." *Id*.

94 *See* U.S. CONST. amend. III; U.S. CONST. amend. IV; U.S. CONST. amend. V; U.S. CONST. amend VI. It could be argued that nearly half of the Bill of Rights concerned individual privacy, using as a base Coke's acknowledgement that a person's residence serves as a haven or repose from government. *See Semayne*, 77 Eng. Rep. at 196 (K.B. 1604).

95 Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citing THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888)). Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering*

This application of privacy was intended to address increases in the numbers of newspapers, cameras, and other intrusive technologies.[96] Most importantly, Warren and Brandeis argued that the common law provided "the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[97] This concern rings hauntingly familiar when placed against the backdrop of the Internet and social networking.[98] Through the Internet, Brandeis and Warren's greatest fears with regard to camera are realized, because through the prevalence of cameras in cell phones, tiny webcams, small handheld video recorders and the like, it is impossible to walk down the street with being a potential photographic target.[99] Although we cannot overlook one difference since 1890—in many cases those asserting a privacy interest are also the same individuals publicizing their information on the Internet.[100]

It is this disconnect between privacy interests and information sharing that make privacy regulation particularly difficult online.[101] Privacy on the Internet has been summed up as a failure in terms of self-regulation.[102] Users fail to protect their

the Law of Confidentiality, 96 GEO. L.J. 123, 129–30 (2007).

96 Richards & Solove, *supra* note 95, at 128–29. Brandeis and Warren were particularly troubled with the intrusive potential of the snap camera, developed by Kodak in 1884. *Id*. *See also* Robert E. Mensel, *"Kodakers Lying In Wait": Amateur Photography and the Right of Privacy in New York, 1885-1915*," 43 AM. Q. 24, 27–28 (1991).

97 Warren & Brandeis, *supra* note 95, at 198.

98 This very notion would be revisited by the Ninth Circuit in the Major League Baseball Drug Testing Case, wherein the Court set forth the requirements and limitations on computer search warrants. U.S. v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 993–96 (9th Cir. 2009).

99 In response to this threat Congress has adopted a video voyeurism laws. *See* Video Voyeurism Prevention Act of 2004, 18 U.S.C.A § 1801 (2004). But even statutes do not protect one who ventures out into public. State v. Glas, 54 P.3d 147, 150–51 (Wash. 2002); *see* 149 CONG. REC. S12,022-23 (daily ed. Sept. 25, 2003) (statement of Sen. Leahy); Warren & Brandeis*, supra* note 95, at 210–11.

100 Note, HARV. L. REV., *supra* note 68, at 1876–77 (noting that the torts of intrusion upon seclusion, public disclosure, and false light could not be claimed when a photo is taken of someone in a public place and then uploaded onto the Internet).

101 Professor Ciocchetti astutely captures this disconnect in three words: (1) must, (2) rush, and (3) trust. This observation recognizes that users are willing to submit whatever information is asked for in order to facilitate their desired web surfing session. Ciochetti, *supra* note 4, at 561.

102 Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000).

information, and providers actively solicit and disseminate the information.[103] The law has approached privacy regulation in a piecemeal fashion designed to correct whatever the most notorious of the injustices of the day is.[104] Many computer users are forced to rely on the FTC or state attorney general.[105] Similarly, the law provides broad immunity for providers by removing liability from computer service providers for the postings of third parties.[106] More striking is the repeated inability of the legal system to address privacy claims using the privacy torts,[107] unfair trade practices,[108] or even trespass to chattels.[109]

This void within our ability to effectively protect ourselves and our information resonates throughout the World Wide Web. Most troubling is that Brandeis and Warren's "right to be let alone," as a privacy foundation all but disappears in today's hyper-connected environment. For example, cyberbullying[110]

[103] *Id*. at 1307–1308.

[104] *See* 15 U.S.C.A. § 6502(b)(1)(A)(i) (2000) (protecting personal information of children); *see generally* 15 U.S.C.A. § 6802(a) (2000) (financial institutions may not disclose nonpublic personal information without consent); *see also* Notice of Privacy Practices for Protected Health Information, 45 C.F.R. § 164.520(a)(1) (2008) (protecting medical information).

[105] Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies As Personal Information Protectors*, 44 AM. BUS. L.J. 55, 72–73 (2007) ("The only recompense available to Web site visitors suffering injuries stemming from information privacy violations rests on the small chance of an enforcement action brought by the FTC or by a state attorney general").

[106] 47 U.S.C.A. § 230(c)(1) (1998); *see* Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). For an example of direct liability being assigned to the user, *see* People v. Kochanowski, 719 N.Y.S.2d 441, 442 (2000) (Ex-lover created website including suggestive photographs with work and home phone numbers).

[107] *See In re* Doubleclick Inc., 154 F. Supp. 2d 497, 515–18 (S.D.N.Y. 2001).

[108] Steven Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cybersapce*, 16 BERKELEY TECH. L.J. 877, 908 (2001).

[109] *See* Bernstein, Litowitz, Burger &Grossmann LLP, *Privacy Law In The Internet Era: New Developments and Directions,* 632 PLI 195 (2001) (noting the failure of the legal system to specifically address invasion of privacy claims as torts, and the inadequacies of the current doctrines in use); In re Doubleclick., 154 F. Supp. 2d at 523–24.

[110] Cyberbullying is the term applied to harassment similar to that which would occur within the halls of a high school, but without providing the respite of the end of the school day, or a return home due to the permanence and pervasiveness of Internet and mobile media used. *See* Matthew C. Ruedy, *Repercussions of a MySpace Teen Suicide: Should Anti-Cyberbullying Laws Be Created?*, 9 N.C. J.L. & TECH. 323, 326–29 (2008) ("Cyberbullying can occur anywhere online"). Cyberbullying gained prominent notoriety with the Lori Drew/Megan Meiers suicide. *Id*. at 327–28. Lori Drew was convicted of violating the terms of use but that conviction was overturned on appeal. *See*

operates to make it so that one has no safe haven. Similarly, the ease with which pictures, emails and texts can be endlessly forwarded makes virtually every act or rumor permanent. Adding to the Internet's ability to pierce our most secretive havens is the proliferation of wirelessly connected mobile devices.[111] Finally, the cloak of anonymity provided by the Internet can make the blackest of hearts appear as sympathetic muses to the unsuspecting.[112] The Internet and its attendant technologies strikes at the heart of one's right to be let alone, if that is what is truly desired.

B. Torts Based on Relationships

Significantly, Brandeis and Warren's starting point was *Prince Albert v. Strange*,[113] through which a dichotomy of privacy emerged according to American application and English application of the law.[114] *Prince Albert* was decided primarily on the basis of the relationship that existed between the printer and the owner[115] of a series of etchings, which the printer then sought to sell reprints of.[116] The Court reached a fairly predictable result in holding that a printer, who had entered into a contract to print copies for a client, could not then print a larger quantity for sale.[117] Similarly, in *Pollard v. Photographic Co.*,[118] an English Court found that the relationship created between a photographer and his client precluded the photographer from

U.S. v. Drew, 259 F.R.D. 449, 451, 467–68 (C.D. Cal. 2009).

111 *See* Note, HARV. L. REV., *supra* note 68, at 1870.

112 *Id*. at 1889. Within the Drew case, the defendant, Lori Drew, created a fictitious teenage boy to prey upon the insecurities of Megan Meiers in an effort to learn Megan's thoughts about Drew's daughter. Drew apparently ended the fictitious teen's relationship with Megan by stating, "the world would be a better place without you." Ruedy, *supra* note 110, at 324.

113 Prince Albert v. Strange, 41 E.R. 1171 (Q.B. 1849).

114 *See* Richards & Solove, *supra* note 95, at 158–59.

115 It is worth noting that the Court relied on Abernethy v. Hutchinson, 47 E.R. 1313 (Ch. 1825). *Prince Albert*, 41 E.R. at 1176–77. In that case, the Court prevented the publication of a series of lectures reported by a student. The court reasoned that it was a reasonable expectation of the lecturer that his extemporaneous speeches would not be taken from him by his listeners. *Abernethy*, 47 E.R. at 1315–18; *see also* JOSEPH STORY, COMMENTARIES ON EQUITY JURISPRUDENCE: AS ADMINISTERED IN ENGLAND AND AMERICA 264 (3d ed. 1843) (noting that when a person delivers a lecture "it is not competent for any person to publish the substance").

116 *Prince Albert*, 41 E.R. at 1173, 1179.

117 *Id.*

118 Pollard v. Photographic Co., (1888) 40 L.R. Ch.D. 345 (Ch. D.).

using the client's photograph in the photographer's Christmas cards.[119] As the English law emerged, the Court repeatedly found a duty of confidence by observing the nature of the underlying relationship between the parties.[120]

Conceptually, this reasoning should not seem foreign, particularly to attorneys. The law of privilege is primarily based on the confidentiality attendant to specific types of relationships.[121] In order to encourage trust and open communication, American law has generally recognized confidentiality between attorneys and their clients,[122] husband and wife,[123] clergy and their congregants,[124] and in some instances even between a reporter and his or her source.[125] More recently, the law has recognized a duty of confidence between an employee and his or her employer.[126] Analysis of the privacy torts using relationships as a foundation may be the appropriate basis for addressing the relationships created by the interactions within social networks.

C. The Big Four

In 1960, Prosser broke these broad concepts down into four identifiable torts.[127] Generally, there are four privacy torts

---

[119] *Id*. at 347,351–52, 354.

[120] *See* Richards & Solove, *supra* note 95, at 159–60.

[121] *See, e.g.,* Jaffee v. Redmond, 518 U.S. 1, 10 (1996) (stating that the need for confidence and trust is the basis for the psychotherapist-patient privilege, much like the attorney-client privilege and the spousal privilege).

[122] *See, e.g.,* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (noting that the attorney-client privilege is one of the oldest forms of confidential communication in order to encourage communication between the two).

[123] *See, e.g.,* Trammel v. United States, 445 U.S. 40, 44, 48–53 (1980) (noting the importance of spousal privilege in order to foster the sanctity of marriage).

[124] This is also known as the Priest-penitent privilege. Commonwealth v. Kebreau, 454 Mass. 287, 301–02, 909 N.E. 2d 1146, 1158 (2009) (quoting MASS. GEN. LAWS ch. 233 § 20A (2010)).

[125] Courts often wrestle with the legal basis for such confidentiality. For example, in *State v. Kiss*, the Idaho Supreme Court found that a qualified privilege existed protecting a reporter from being required to disclose the identity of confidential sources. 108 Idaho 418, 419, 421–23 (Idaho 1985). Differing majorities based the holding on the United States Constitution and the Idaho Constitution. *Id* at 419–24 (majority opinion) (Donaldson, C.J., concurring). One judge rested his decision on the common law. *Id*. at 424–28 (Bistline, J., concurring).

[126] *See, e.g.,* Food Lion, Inc. v. Capital Cities/ABC Inc., 194 F.3d 505, 515–16, 518–19 (4th Cir. 1999) (stating that employees videotaping from a restricted area breached the tort of loyalty to their employer).

[127] William L Prosser, *Privacy*, 48 CAL.L.REV. 383, 389 (1960).

recognized by the common law: Appropriation, Intrusion, Disclosure of Embarrassing Facts, and False Light.[128] But as ground breaking as the distillation of these torts were, the unintended effect may have been a stagnation in privacy law.[129] It is worth a brief review of the four privacy torts, to identify how they fall short considering current technology.

1. Appropriation

In simplest terms, appropriation is the use of someone's likeness for commercial purposes without their permission.[130] The earliest recognition of this tort was a legislative response to a New York case, holding that there was no law against the nonconsensual use of a woman's picture to sell flour.[131] The three most accepted defenses to appropriation are newsworthiness, consent, and that the individual is not identified.[132] Celebrities may be afforded even greater protection under this tort because their image is generally how a celebrity makes money.[133]

Given the numbers of people on the Internet, appropriation is commonplace, but it is uncertain whether much of the appropriation that takes place results in any damages. Most frequently appropriation disputes on the Internet center on the use of a domain name, which users would identify with another entity.[134]

---

128 *Id.*

129 Richards & Solove, *supra* note 95, at 152–53; *see also* Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1406 (1987) (noting that Prosser's identification of four privacy torts had "effectively frozen" further development).

130 Prosser, *supra* note 127, at 401–02.

131 Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 542–43, 552–53 (Ct. App. 1902), *superceded by statute*, NY Civ. Rights Law §§ 50–51 (2010), *as recognized in* Cuccioli v. Jekyll, 150 F. Supp.2d 566, 575 (2001) (stating that based on the statute, one may recover for the trade or commerce of one's likeness only to the extent that it occurs in New York State). Not all states required a law. In *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 78–80 (Ga. 1905), a Georgia Court found a common law right preventing the use of a person's picture to sell life insurance.

132 *See* Prosser, *supra* note 127, at 405, 411–13, 419.

133 *See* Carson v. Here's Johnny Portable Toilets, 698 F.2d 831, 835–37 (6th Cir. 1983); *see also* Midler v. Ford Motor Co., 849 F.2d 460, 461, 463 (9th Cir. 1988).

134 *See, e.g.,* Planned Parenthood Fed'n of Am., v. Bucci, No. 97 Civ. 0629, 1997 WL 133313, at *1 (S.D.N.Y. Mar. 24, 1997) (claim arose out of defendant registering domain name plannedparenthood.com); Pet Stop Prof'l Pet Sitting Serv. v. Prof'l Pet-Sitting Serv., No. 07-90-ST, 2007 WL 1876517, at *1–2 (D.Or. June 26, 2007) (allegations arose out of the registering of a domain

2. Intrusion Into Seclusion

Particularly relevant within the Internet realm and within social networking circles, is the privacy tort of intrusion.[135] Simply put intrusion is a physical, electronic or mechanical intrusion into someone's personal life.[136] The tort is committed by information gathering, no publication is required.[137] One of the clearest examples of intrusion is the opening of another person's mail, which could also directly correspond to the Internet through the opening of someone else's e-mail.[138] Similarly, within the Internet context, one cannot use a false identity to gather information about another if he or she had a reasonable expectation of privacy over that information.[139]

3. False Light

Making someone appear to be something that they are not, particularly if it casts the person in a negative or embarrassing light is the tort of false light.[140] False light contains two seemingly high hurdles. First, it must be offensive to a reasonable person.[141] Second, malice must be shown.[142] Given the dynamics of social life, depending on the false light, it may be difficult to show that a reasonable person would be offended.

name similar to that of plaintiffs' name).

[135] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see also* Shulman v. Group W. Prods, Inc., 955 P.2d 469, 477–79, 485, 490 (Cal. 1998) (adopting the Restatement approach, which establishes liability for intentional intrusions upon the solitude or seclusion of another or that person's private affairs if a reasonable person would consider the intrusion highly offensive).

[136] *See* 62A AM. JUR. 2D *Privacy* § 40 (2009). Intrusion is akin to trespass, so much so that the two torts, trespass and intrusion, are simultaneously pled. *See* John J. Walsh, Steven J. Selby & Jodie L. Schaffer, *Media Misbehavior and the Wages of Sin: The Constitutionality of Consequential Damages for Publication of Ill-Gotten Information*, 4 WM. & MARY BILL RTS. J. 1111, 1119–23 (1996).

[137] *See* Andrew F. Caplan & Robert J. Donovan, *The Ethical Investigation of Fidelity Claims Protecting Privacy,* 10 FIDELITY L.J. 63, 70 (2004).

[138] *See, e.g.,* Roth v. Farner-Bocken Co., 667 N.W.2d 651, 657-58, 661 (S.D. 2003) (holding that an employer could be held liable for intrusion upon seclusion for opening a former employee's mail).

[139] *See, e.g.,* State v. Patel, No. 26683-4-III, 2008 WL 5377826, at *4–6, *8–9 (Wash. Ct. App. Dec. 23, 2008) (holding that the transcript of an internet chat between a criminal defendant and a police officer, using a false identity, was properly admitted into evidence because the defendant's expectation of privacy was not reasonable).

[140] *See* RESTATEMENT (SECOND) OF TORTS § 652(e) (1977).

[141] *Id.* at § 652(e)(a).

[142] *See id.* at § 652(e)(b).

Second, absent a particularly telling set of facts, malice would seem difficult to prove as well.

4. Publication of Embarrassing Private Facts

An often overlooked tort is one that may most accurately portray both Coke and Brandeis's views of privacy providing repose from publicity. Within this tort, one is protected from having facts, even though they are true, published if a reasonable person would be offended at having such intimacies revealed.[143] But there is no protection if one is observed in a public place, or if the person or their activities are considered newsworthy.[144]

D. The Forgotten Tort: Breach of Confidentiality

One of the dilemmas posed by Prosser's four torts is that it left one behind. Between Brandeis & Warren's opus on privacy in 1890 and Prosser's clarification in 1960, a fifth tort—breach of confidentiality had emerged.[145] Cases had determined that it was improper for a hospital to leak a photo of a deformed child,[146] a photographer violated an implied contract in making extra copies of photos of dead babies,[147] and even finding that a doctor would likely be liable or prohibited from testifying about a patient's confidences in court.[148]

1. Traditional Roots

Similarly, one area in which citizens enjoyed widespread confidentiality involved their interactions with the government. For example, a promise of confidentiality within the mail service predates the birth of our nation and the formation of the U.S.

[143] *Id.* at § 652(d)(a).

[144] *See, e.g.,* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 492-93 (1975) (allowing no recovery for the disclosure of facts, such as the events of judicial proceedings, that are public record or of public concern). It is worth noting that if the revelation occurs through a news media outlet, it is virtually impossible to prevail in such an action. *See id.* at 492–93 ("The developing law surrounding the tort of invasion of privacy recognizes a privilege in the press to report the events of judicial proceedings.").

[145] Richards & Solove, *supra* note 95, at 146.

[146] *See* Bazemore v. Savannah Hosp.,155 S.E. 194, 196–97 (Ga. 1930) (holding that parents stated a cause of action for invasion of privacy against a hospital for publicizing photos of their malformed child).

[147] *See* Douglas v. Stokes, 149 S.W. 849, 849–50 (Ky. 1912).

[148] *See* Smith v. Driscoll, 162 P. 572, 573 (Wash. 1917).

Postal Service.[149] This confidentiality has survived throughout the nation's history[150] and has evolved to accommodate certain types of technology such as the telegraph.[151] Citizens also enjoy protection from disclosure of information collected by the government, most notably through information given to census takers,[152] as well as tax return information.[153] Most recently, the government has grappled with issues regarding access to confidential electronic passport records by state department employees to review the travels of celebrities.[154]

2. Transplantable to the Internet

In looking at the reality of the intersection of privacy and technology, it appears that a revival of the law of confidentiality may offer our best chance at creating measurable, enforceable,

149 *See* David J. Seipp, *The Right to Privacy In American History*, 7–8 (1978) (quoting 9 Ann., cap. X, § 40), *available at* http://pirp.harvard.edu/pubs_pdf/seipp%5Cseipp-p78-3.pdf ("The Post Office Act of that year [1710], reiterating a Proclamation of 1663, provided that 'No person or persons shall presume wittingly, willingly, or knowingly, to open, detain, or delay, or cause, procure, permit, or suffer or be opened, detained, or delayed, any latter or letters, packet or packets.'").

150 *See, e.g.,* Denis v. LeClerc, 1 Mart.(o.s.) 297, 1, 3, 9–10 (Orleans 1811) (punishing a defendant for disobeying an injunction against the publication of a letter intended, by its writer, to be private); *see also* Roberts v. McKee, 29 Ga. 161, 1–4 (Ga. 1859) (prohibiting publication of letter from one member of partnership to another after dissolution of the partnership); *see also* Eyre v. Higbee, 22 How.Pr. 198, 198 (N.Y. Gen. Term 1861) (holding that letters in the hands of an executor are not assets for sale).

151 Richards & Solove, *supra* note 95, at 144–45 (noting that by 1879, two-thirds of states had passed some type of statute protecting the confidentiality of a telegraph message).

152 Act of Mar. 1, 1889, ch. 319, § 8.

153 *See IRS Issues Regulations on Disclosure of Tax Return Information*, J. OF ACCT., Dec. 30, 2009, http://www.journalofaccountancy.com/Web/20092457.htm (last visited Mar. 27, 2010) (describing IRS regulation of the disclosure of taxpayer's information by tax return preparers). But the right to privacy with regard to tax returns depends on the circumstances as evidenced in the 2008 Democratic Presidential Primary, when now President Obama released his returns and demanded that his opponent, now Secretary of State Hillary Clinton, release hers—ostensibly accusing her of hiding something by not releasing them. Posting of David Wright to Political Radar ABCNews.com Blog, http://blogs.abcnews.com/politicalradar/2008/02/obama-to-clinto.html (Feb. 7, 2008, 17:24 EST). At this point, it is arguable that the citizenry has an expectation, if not a right, to see the tax returns of certain political candidates.

154 Grant Gross, *Fourth State Department Worker Pleads to Passport Snooping*, PC WORLD, July 10, 2009, http://www.pcworld.com/article/168233/fourth_state_department_worker_pleads_to_passport_snooping.html (last visited Mar. 27, 2010). Out of a control group of 150 celebrities, 127 had been accessed more than 4100 times. *Id*.

and comprehensible privacy standards. This also permits us to breathe new life into one of Prosser's more important goals with respect to the law: the establishment of clear rules.[155] Prosser also recognized that tort law, in particular, was a "'common sense' balancing of social interests rather than a series of universal principles."[156] Out of this, it could be assumed that the stagnation of privacy law was merely an unintended consequence and not the goal of Prosser's formulation of the four privacy torts. To that end, it may be time to revisit the law of confidentiality and its reliance on relationships to form a better approach to Internet and social networking privacy law.

IV. STRIKING THE APPROPRIATE BALANCE: WEIGHING SOLUTIONS

A. Catalyst Judges

As attorneys, one of our primary challenges is insuring that the Court understands exactly what it is that we are discussing. This can be particularly troublesome within the online environment because a quick look at the statistics shows that judges are likely not within the target audience of social networking sites, for example.[157] This means that when presented with a case involving these issues, attorneys should assess the need to acquaint the Court with the technology underlying the suit.[158] Similarly, the Court's experiences with technology will be influential and assist in cultivating an understanding of the significance of the issues raised.

When looking at the apparent success plaintiffs had in *Lane* and *Harris* with regard to challenging Facebook's Beacon service,

155 *See* Richards & Solove, *supra* note 95, at 149.

156 *Id*.

157 *See* Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online,* 11 VAND. J. ENT. & TECH. L. 1001, 1017 (2009) (citing Press Release, More than Half of MySpace Visitors are Now Age 35 or Older, as the Site's Demographic Composition Continues to Shift (Oct. 5, 2006), *available at* http://www.comscore.com/Press_Events/Press_Releases/2006/10/More_than_Half_MySpace_Visitors_Age_35/(language)/eng-US) (noting that, within online social networks, "only 10% of users are older than 55 and close to 50% are younger than 35.").

158 For example, if the suit involves a Facebook page, or an opt-out policy, an attorney should be prepared to introduce and display those pages on computers within the Courtroom. The best approach is likely to show these concepts on the computer, as one would access them, and then navigate through these pages.

the Video Privacy Protection Act was the primary means of challenge.[159] This act prohibits the distribution of personally identifiable information to third parties with regard to video renting or buying habits without written consent.[160] The genesis for this law was the 1987 confirmation proceedings of Judge Robert Bork. In the course of his confirmation, a list of 146 videos that he had rented was released during the proceedings and published by a newspaper.[161] In response to this publication, Congress enacted the Video Privacy Protection Act to expressly prohibit future releases.[162]

Similarly, Ninth Circuit Judge Kozinski recently more narrowly defined the procedures and safeguards federal courts should observe in the issuance of search warrants and subpoenas for electronic information.[163] The catalyst in this case may have been the revelation of a large number of eye-raising photographs and videos which were found on a website,[164] which he thought was private.[165] Notably, *Comprehensive Drug Testing* expressly attempts to "strike a proper balance between the government's legitimate interest in law enforcement and the people's right to privacy and property in their papers and effects . . . ."[166] *Comprehensive Drug Testing* recognizes that privacy necessarily includes one's ability to control personal information and with whom to share it.[167]

Paramount within this need for balance is a concern that

159 Harris v. Blockbuster, Inc., 622 F. Supp. 2d 396, 397 (N.D. Tex. 2009); Lane v. Facebook, Inc., No. C 08-3845 RS, 2009 WL 3458198, at *1 (N.D. Cal. Oct. 23, 2009); *see also* Jacqui Cheng, *Suit Accuses Blockbuster*, *Facebook of Privacy Law Violations*, http://arstechnica.com/tech-policy/news/2008/04/suit-accuses-blockbuster-facebook-of-privacy-law-violations.ars (last visited Mar. 27, 2010) (describing the Harris lawsuit in which the plaintiff claimed that Blockbuster's actions violated the Video Privacy Protection Act).

160 18 U.S.C. § 2710 (2010).

161 *See* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 238 (D.N.J. 1996).

162 *See id*.

163 United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004 (9th Cir. 2009).

164 *See* Scott Glover, *9th Circuit Chief Judge Posted Sexually Explicit Matter On His Website*, L.A. TIMES, June 11, 2008, *available at* http://www.latimes.com/news/local/la-me-kozinski12-2008jun12,0,6220192.story (noting that the content at the time was accessed by typing in the name of a subdirectory.).

165 *See id.*

166 *Comprehensive Drug Testing Inc.*, 579 F.3d at 994.

167 *See id*. at 1005–07 (recognizing that the scattered landscape of information storage re-affirms a need to protect individual privacy when balancing against government searches); *see also* Levin & Abril, note 157, at 1008.

Government would be able to justify all of its searches in relation to technology making the seizure of more rather than less a powerful incentive.[168] The means by which materials are aggregated within computer storage media make it too easy to conduct limitless searches.[169] The ease with which this aggregation and searching occurs is what triggers the greatest of our privacy concerns[170]—a concern that sometimes cannot not be neutralized through any series of affirmative steps.[171] It is precisely this balance that lies at the heart of the future of privacy within the socially networked world.

B. The Illusory Opt-Out

Although it has been shuttered, Facebook's Beacon represents just how illusory the reliance on opt-outs can be on the Internet. Remembering that the notification was a pop-up window in a corner of your computer screen, which also disappeared within about ten seconds, the pop-up included a button to prevent the pop-up from appearing in the future.[172] But to actually opt-out required a user to, within the ten seconds the window was visible, click on "See More," then know to click on "Edit Settings."[173] Finally, this opt-out would only opt a user out of Beacon services for the site that you had clicked in from.[174] For example, if you figured out the opt-out on Overstock.com, then you were only opted out of the Beacon service on Overstock.com—you would have to go through the above process on Blockbuster.com all over again, and so on.[175]

The opt-out as a defense was also used in *Boring v. Google*.[176]

---

168 *See Comprehensive Drug Testing Inc.*, 579 F.3d at 998.

169 As the Court noted, the case agent in *Comprehensive Drug Testing* found information related to all of the baseball players within the program (as opposed to the 10 players who were the targets of the search warrants), and prepared additional search warrants based on this information. *Id.* at 999.

170 *See id.* at 1003 (noting the effects on baseball players David Ortiz, Manny Ramirez, Sammy Sosa, and Alex Rodriguez.).

171 *See id.* at 1004 (recognizing the steps law-abiding citizens may take to protect data and the harm they may suffer from the disclosure of that data if large quantities of data are permitted to be scooped and sifted). *See also id.* at 1005–06 (noting that often information is stored in ways in which individuals have not made a choice, but rather some other entity has made that choice for them. This does not mean that the individual has sacrificed their privacy).

172 My Heart's in Accra, *supra* note 51.

173 *Id.*

174 *Id.*; *see also* Grimmelmann, *supra* note 5.

175 My Heart's in Accra, *supra* note 51.

176 598 F. Supp.2d 695, 698–700 (W.D. Pa. 2009), *reconsideration denied*, No.

In *Boring,* plaintiffs brought an action against the search engine Google for infringements of the privacy torts with regard to Google's taking and publishing pictures of the Boring's property even though those pictures could not have been obtained from the public street.[177] According to the Borings, the pictures could only be obtained by driving up their unpaved drive, past two no trespassing/ private property signs.[178] Notably within the course of the opinion granting summary judgment for Google, the judge chastised the plaintiffs for bringing more publicity to their plight by filing the lawsuit.[179] But the Court did not end its admonishment of plaintiffs with its observations on publicity, but continued with an admonishment of the plaintiffs for bringing suit instead of following the opt-out procedures with regard to Google's street view feature.[180]

But the problem with the opt-out as a defense is, as explained with regard to the process to opt out of Facebook's Beacon above, the same when applied to Google's street view. The opt-out process from Google's street view is illusory at best. For example, a member of the Electronic Freedom Foundation, Kevin Bankston sought to have a picture of him walking down the street removed from street view.[181] In response, Google initially sought a sworn statement (under penalty of perjury) and a photocopy of a valid driver's license among other pieces of information to have the image removed.[182] After publication of Google's demand with regard to its informational requirements to opt-out, Google relented, and permitted Bankston to opt-out, and removed his picture upon the provision of his name and the location of the image within their street view service.[183]

This scenario illustrates two things. First, content providers

Civ.A 08-694, 2009 WL 931181 (W.D. Pa. Apr. 6, 2009).

[177] *Id*. at 698–99.

[178] *Id*. at 699.

[179] *Id*. at 700, 704.

[180] *Id*. at 700.

[181] Kevin Poulsen, *Want off Street View? Google Wants Your ID and a Sworn Statement—Update: Google Gives*, WIRED.COM June, 15, 2007, http://www.wired.com/threatlevel/2007/06/want_off_street/.

[182] *Id*.

[183] *Id*. Bankston observed that when confronted with the choice of having his unidentified picture on Google or sending Google a copy of his driver's license without any clear indication of what they needed the information for, or what they would do with that information, the choice was a no-brainer to leave the unidentified picture up to avoid having to sacrifice more of his personal information. *Id*.

should be more accommodating to requests to take information down, particularly information that they have not received any consent to publish. Second, if content providers and courts are going to rely on opt-out procedures as a means of preventing litigation and protecting privacy, then they must ensure that the procedures work. As mentioned above, this is likely an area where an attorney should be prepared to show the Court why the opt-out is or is not a valid option.[184] Google's initial policy reads as if it is intended to dissuade all but the most dedicated and savvy of users from pursuing an opt-out to its conclusion. If opt-outs are relied upon, it is predictable that much of the determinative power will reside in those most interested in the aggregation of information while too little rests in those whose privacy interests may be harmed.

C. Outside the Box . . . Perhaps Even Reality

Some have argued that in order to protect our privacy, we should embrace the emerging trend towards omniveillance.[185] In sum, the argument is that society will largely enjoy informational privacy because everyone's personal information will be available to everyone else.[186] As a way to ensure fair play within the realm of data collectors and information harvesting, the balance is to ensure that the same information that is being collected from the public at large is also collected and made available for the employees and executives of the company doing the collecting.[187]

Intriguingly, advocates of transparency do not argue for a completely transparent system, but rather transparency with caveats.[188] Advocates acknowledge the need for some respite from omniveillance, such as within the walls of one's home as Coke famously asserted in the *Semayne's Case*.[189] Revealingly, many of the exceptions that would be acknowledged within a

184 *See supra* note 158.

185 *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 80–83 (1998); *see also* Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 996 (2004).

186 BRIN, *supra* note 185, at 182–84.

187 *See* Zarsky, *supra* note 185, at 996 (discussing Brin's approach).

188 *Id*. at 1001.

189 *Id*.; Semayne's Case, 77 Eng. Rep. 194, 199 (1604)*; see also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (prohibiting use of thermal imaging devices without a warrant to search interiors of homes).

transparent society are relationship based, and would therefore likely be protected under the law of confidentiality.[190] But as this solution is offered, when viewed with its attendant caveats, it is not clear in how much it differs from the system now in existence. Finally, its greatest flaw may be in that it treats all information as if it were worth the same.[191]

D. Anonymity or Pipe Dream?

Regulation of information privacy is piecemeal at best within the United States.[192] Although financial data,[193] medical data,[194] and children's data[195] are protected, much of this data can still be shared provided the subject of the data cannot be identified.[196] Generally, the belief is that provided the information cannot be used to identify a particular person, then there is a lesser need to regulate the collection of that data.[197] However, anonymized data has been mined, analyzed, and traced back to identify specific users.[198]

Surprisingly, anonymous data continues to avoid regulation even when confronted with repeated successes at distilling the anonymous information into identifying information. More than

190 *See* Zarsky, *supra* note 185, at 1001–02 (recognizing lawyer-client, physician-patient, employer-employee, and bank-client as protected, as well as communications between two people (prohibiting any interception)).

191 *See id*. at 1006–08 (criticizing the argument of transparency protagonists that equality in the accessibility of personal information will deter misuse).

192 Compare the treatment of data protection in the United States to the European Union's 1998 Directive on the Privacy of Personal Data. Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 461–62 (2000).

193 *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338, 1436–37 (1999) (codified as amended at 15 U.S.C. § 1843 (2006) (providing for regulation of entities engaged in financial activities including restrictions on cross-marketing).

194 *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936, 2021–26 (1996) (codified as amended at 42 U.S.C. §§ 1320d-1-1320d-2 (1996) (providing for regulation of the transmission of health information including the adoption of standards for ensuring the confidentiality of such information)).

195 *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2010) (providing for regulation of the collection and release of personal information from children on the internet).

196 Benjamin Charkow, *The Control Over the De-identification of Data*, 21 CARDOZO ARTS & ENT. L.J. 195, 196 (2003); *see also* C. Christine Porter, *De-identified Data and Third Party Data Mining: The Risk of Re-identification of Personal Information*, 5 SHIDLER J.L. COM. & TECH. 3 (2008).

197 Porter, *supra* note 196.

198 *Id*.

10 years ago, scientists were able to simply cross-reference medical information with an open voter database.[199] More recently, in 2006, the New York Times was able to take searches performed by anonymous users and then re-identify the user based on the searches.[200] In 2007, supposed anonymous data was again distilled to re-identify users who had ranked movies on Netflix.com as part of a promotional prize offering.[201]

Although individuals have repeatedly enjoyed success with re-identifying anonymized data, courts have been reticent to affirm the need to protect individuals from the collection of anonymized data.[202]

E. A Forgotten Tort Remembered

Regulation of privacy on social networking sites may be best addressed through an evolution of one or a combination of the above-mentioned torts. Likely the best tort for a foundation is that of confidentiality. The tort of confidentiality resets the privacy field appropriately because its critical analysis point is the relationship between the person about whom information is being shared and the person sharing the information. Confidentiality also allows American privacy law to evolve from the flawed starting point[203] within its foundation—privacy equals complete secrecy.[204]

Based on the way that information is collected and shared on the Internet, the most likely starting point is a relationship-based tort. Also, accepting that complete or perfect privacy is

---

[199] Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L. MED. & ETHICS 98, 100 (1997).

[200] Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000.

[201] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[202] *See, e.g.,* IMS Health Corp. v. Rowe, 532 F. Supp. 2d 153, 157 (D.Me. 2008).

[203] A fundamental demonstration of this flaw is reflected in the inconsistencies of Courts analyzing the point at which a privacy claim is defeated through disclosure. For example, in *Duran v. Detroit News, Inc.*, the Court held that telling a few people eliminated the claim. 504 N.W.2d 715, 718–20 (Mich Ct. App. 1993). But in *Times Mirror Co. v. Superior Court*, the Court held that sharing with a few people does not convert private information into public information. 244 Cal. Rptr. 556, 561 (Cal. Ct. App. 1988).

[204] Richards & Solove, *supra* note 91, at 497.

impossible in today's society,[205] the tort of confidentiality recognizes that privacy will be breached[206] and properly focuses on the obligations owed within the chain of the breach.[207] Put simpler, a duty of confidence arises when a party subject to the duty is in a situation where it is known or should be known that other person can reasonably expect a protection of privacy.[208] From this straightforward assignment of situational duties, a hierarchy of privacy relationships on the Internet emerges.

1. Relationships Establish Themselves

For example, the highest duty of privacy is likely due to users who enter a site to make a financial transaction or purchase of a product. Thus, there is a direct relationship between a site such as Amazon and a customer who must input their personal financial information to complete the transaction. Amazon's duty to a customer would likely be considered among the highest, similar to the relationship enjoyed between a bank and its customer based on the financial information required of Amazon to complete a transaction.[209]

But courts have been reluctant to apply these types of duties. In *Dwyer v. American Express*,[210] cardholders' purchase information was offered to merchants.[211] The Court rejected a claim for intrusion into seclusion because cardholders voluntarily provided their information to American Express.[212] Appropriation was similarly rejected because the Court did not recognize the independent value of American Express's lists.[213]

[205] Gavison, *supra* note 66, at 428.

[206] Professor Gavison astutely notes that privacy is not an all or nothing concept, one cannot enjoy perfect privacy just as one cannot lose all privacy. Privacy should then be analyzed through the degrees associated with losses of privacy. *Id*. at 428–29.

[207] An example of this duty is evident within the criminal context with the law of blackmail. The law emerged as the laws of Victorian society required citizens to always appear respectable irrespective of private vices. Richards & Solove, *supra* note 96, at 139*; see also* Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1102 (2002) (noting that the Victorian compromise was to protect the reputations of respectable men).

[208] A v. B, (2003) Q.B. 195, 207; *see also* Richards & Solove, *supra* note 95, at 170–71 (quoting A v. B, (2003) Q.B. at 207).

[209] *Cf.* Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961).

[210] Dwyer v. Am. Express, 652 N.E.2d 1351 (Ill. App. Ct. 1995).

[211] *Id*. at 1353.

[212] *Id*. at 1354.

[213] *Id*. at 1356.

In dismissing the value of the lists, the Court fails to recognize the inherent value of information. A good example of this inherent value is found in free fantasy football sites.[214] The data collected through these sites for free has an enormous value to marketers.[215] This aggregated information even takes on a value of its own, and can become independently alienable.[216] This is the precise scenario where a breach of confidentiality claim would become applicable because the court would not focus on the information released, but rather the relationship between American Express, a bank, and the cardholders, its clients.[217] Focusing on this relationship, American Express's duty to protect the information of its clients reveals itself.

2. Current Privacy Exceptions Apply

Within the context of social networks and information sharing, the duties are assigned across a broader spectrum but still no less predictable. Generally, under the tort of confidentiality, a

[214] *See* Paul R. La Monica, *Fantasy Football . . . Real Money*, CNN MONEY, Aug. 11, 2006, http://money.cnn.com/2006/08/11/news/companies/fantasy football/ (last visited Mar. 1, 2010).

[215] A marketer observed that the average fantasy football player is "predominately male, married, in a high income bracket" and highly likely to make purchases online. *Id*.

[216] For example the recent bankruptcies of Toysmart and Egghead.com involved efforts to sell the marketing lists by these entities. Each of these efforts was met by the Federal Trade Commission seeking to enjoin the sale of these lists because the respective privacy policies made promise to "never sell" personal information. *See* Objection of States to the Public Sale of the Debtor's Customer List, *In re* Toysmart.com, L.L.C., No. 00-13995-CJK (Bankr. Mass. July 20, 2000) (arguing Toysmart's attempted sale of its customer list was "inconsistent with [their stated privacy] policy, misleading to consumers who read the policy, and is unfair or deceptive pursuant to the Consumer Protection Acts."); Fed. Trade Comm'n v. Toysmart, No. 00-11341-RGS, 2000 WL 34016434, at *2 (D. Mass. July 21, 2000) (stating that defendants must "delete or destroy all Customer Information"); *In re* Egghead.com, Inc., No. 01-32125-SFC-11, 2001 WL 35671549, at *3–5 (Bankr. N.D. Cal. Sept. 21, 2001) (discussing the court's order which included the transfer of User Data from the Debtor to the Buyer); *see also* Warren E. Agin, *The New Regime for Treatment of Customer Data in Bankruptcy Cases*, 10 J. Bankr. L. & Prac. 365, 375–76. (2001) (discussing that in many cases of bankruptcy, the companies have attempted to sell/auction their client lists).

[217] Oddly, the Court expressly rejected application of a bank standard within the *Dwyer* case and instead noted that the compilation of this information was akin to the construction of magazine subscription lists. Dwyer v. Am. Express, 652 N.E.2d 1351, 1354–55 (Ill. App. Ct. 1995). One would have to wonder if the recent revelations, bailout, and related issues with the banking industry would dictate a similar conclusion by this same court?

third person cannot be liable for a disclosure provided it was not learned from a confidant.[218] Information is shared in two primary ways within Social Networks, among users, and then through aggregation by the hosting platform. Distilling the information sharing into these two broad categories makes the assignment of duties relatively simple.

3. Relationship Responsibility

Among users, the general rule of confidences should apply. In other words, if a user would not know of the information but for the relationship they have with the other user, but then disclose that confidence, the disclosure could be addressed under the tort of confidentiality. Thus, a former girlfriend who posted intimate information on dontdatehimgirl.com[219] should be liable for that disclosure through the tort of confidentiality because the basis for her information is an intimate relationship in which one would not expect all of the details to be publicized.

As a data miner and aggregator, the social networking platform owes a duty of confidentiality to its users. But the threshold of confidentiality will be much lower within this relationship because users are often inputting information to share and connect with other users. This means the platform owes this duty in two ways. First, the platform should inform users of what the privacy settings within the site mean.[220] For example, within Facebook's privacy settings page, there are a series of drop down menus that allow a user a tremendous amount of control over the privacy of their profile,[221] but there is no explanation of what each of these settings means to the user.

---

[218] Richards & Solove, *supra* note 95, at 178.

[219] Dontdatehimgirl.com is a website, where users share photos and warnings of people that others should not date. Often the tales include details of sexual preferences, STDs, and other intimate details. Dontdatehimgirl.com, About DDHG, http://dontdatehimgirl.com/about/ (last visited Mar. 1, 2010). The site truly brings to life the famous quote from *The Mourning Bride,* "Heav'n has no rage like love to hatred turn'd, [n]or hell a fury like a women scorn'd." WILLIAM CONGREVE, THE MOURNING BRIDE, *reprinted in* BELL'S BRITISH THEATER 63 (Vol. XIX 1797).

[220] *See* Grant Gross, *Online Privacy Policies Don't Do Their Job, Critics Say*, PC WORLD, Nov. 4, 2007, http://www.pcworld.com/article/id,139238-c,online privacy/article.html (stating that website privacy policies should be standardized. This would lessen the learning curve as users manipulate their privacy settings).

[221] Facebook, Privacy on Facebook, http://www.facebook.com/privacy/ explanation.php?ref=pf, (last visited Mar. 2, 2010).

One solution is for the platform to provide "hover boxes" that appear when an option is selected to inform the user of what will be visible to who and when.

The second duty owed to users by the platform requires users to be informed with regard to data collection and aggregation. Related to this information is permitting a user the means to make friends lists private. For example on Facebook, often the most private settings still have a users list of Friends available.[222] When this list of friends is coupled with an application such as the M.I.T. sexual preference application, it creates a possibility that a company may be able to "guess" a prospective employee's sexual orientation as it considers a hiring decision.[223] Platforms should not only enable users to block their profiles from these types of information, but also inform users as to how their information will be accessible to others. As mentioned previously, hover boxes could assist users as they refine their privacy settings. Probably most significantly, platforms could ask for users to prepare their privacy profiles at the same time the sites are harvesting sign-up information instead of relying on default settings.

V. CONCLUSION

The rise of the Internet[224] and social networking[225] occurred in defiance of conventional business norms.[226] This defiance of norms has extended into the legal and regulatory systems as governments and courts have struggled to address the dynamic

[222] *See* Facebook, *supra* note 221; Facebook's Privacy Policy, *supra* note 7.

[223] *See* Carolyn Y. Johnson, *Project Gaydar,* THE BOSTON GLOBE, Sept. 20, 2009, *available at* http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

[224] Marc Andreessen is credited with writing the computer software that created the browser when he was 23 and at the University of Illinois. Melanie Warner, *Inside the Silicon Valley Money Machine,* FORTUNE, Oct. 26, 1998, *available at* http://money.cnn.com/magazines/fortune/fortune_archive/1998/10/26/250008/index.htm.

[225] *See* Elinore Longobardi, *Who Invented Facebook?*, COLUMBIA JOURNALISM REV., June 26, 2008*, available at* http://www.cjr.org/the_audit/am_credit_to_rolling_stone_625.php (noting that Facebook Founder Mark Zuckerberg started working on the site while drunk).

[226] Amazon.com is a perfect example of this defiance. Prior to its ever turning a profit, the stock soared high above $100 a share, with many doubtful that it would ever turn a profit. *See* James B. Kelleher, *Dueling Analysts Amazon Plan Sparks Debate On Stock Value*, THE N.Y. POST, Dec. 20, 1998, at 84. Few would argue with Amazon.com's success at this point.

environment of the Internet and social networks. Existing legal procedures, laws, and decision-making are designed to address conventional and predictable legal issues. But social networking and all of its evolutions do not follow the rules of convention. The advent of the Internet challenges existing legal structures because technology is not restricted by precedent, statutes, or in many situations any codified regulation. The Internet and social media's rapid evolutionary capacity further defy legal tradition.

As outlined within this article, the legal system must become more nimble. One of the strategies that may be most effective is one that the existent privacy torts have resisted—focusing on the relationship between parties when information is disclosed, rather than the content. Another may be an expansion of the forgotten tort of confidentiality by looking back to the roots of our legal system in England, and applying it prospectively to the relationships technology creates between its users and providers. The Internet has launched society into this next century. The law must similarly evolve.