Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 20 *Volume XX*
Number 3 *Volume XX Book 3*

Article 8

2010

Friending Privacy: Toward Self- Regulation of Second Generation Social Networks

Robert Terenzi, Jr.
Fordham University School of Law

Friending Privacy: Toward Self- Regulation of Second Generation Social Networks

Cover Page Footnote

I am very grateful to Yokum Taku and Glenn Luinenburg of Wilson Sonsini Goodrich & Rosati, and Professor Joel Reidenberg for helping me develop this article. I am particularly thankful for the advice, editing, and supervision of Professor Olivier Sylvain, who was both an advisor and mentor throughout the writing process.

Friending Privacy: Toward Self-Regulation of Second Generation Social Networks

Robert Terenzi, Jr.*

* J.D. Candidate, Fordham University School of Law, 2010; M.A. Candidate, International Political Economy and Development, Fordham Graduate School of Arts and Sciences, 2010. I am very grateful to Yokum Taku and Glenn Luinenburg of Wilson Sonsini Goodrich & Rosati, and Professor Joel Reidenberg for helping me develop this article. I am particularly thankful for the advice, editing, and supervision of Professor Olivier Sylvain, who was both an advisor and mentor throughout the writing process.

INTRODUCTION

The Internet is based on a layered, end-to-end model that allows people at each level of the network to innovate free of any central control. By placing intelligence at the edges rather than control in the middle of the network, the Internet has created a platform for innovation.

—Vinton Cerf[1]

Over the past five years, social networking sites such as Facebook,[2] Google,[3] and Twitter[4] have changed the way people use the Internet and interact with each other. These websites serve as a platform for people to connect with other users of the site and share information, pictures, and, increasingly, their real-time location. The explosive growth of sites such as Facebook and MySpace has spawned a second generation of social networks. Second generation social networks push the privacy envelope even further than initial experiments in information sharing by encouraging users to share a catalogue of their possessions, address books, and real-time purchases. Correspondingly, the ever-increasing amount of personal information divulged via these sites has had, and will continue to have, dramatic implications for the social networking sites, their users, and the law. Federal courts,

[1] Letter from Vinton G. Cerf, Vice President and Chief Internet Evangelist, Google, Inc., to Hon. Joe Barton, Chairman, House Comm. on Energy and Commerce, and Hon. John D. Dingell, Ranking Member, House Comm. on Energy and Commerce (Nov. 8, 2005), *available at* http://googleblog.blogspot.com/2005/11/vint-cerf-speaks-out-on-net-neutrality.html.

[2] Facebook, http://www.facebook.com (last visited Feb. 18, 2010).

[3] Google, http://www.google.com (last visited Apr. 1, 2010).

[4] Twitter, http://www.twitter.com (last visited Feb. 18, 2010).

Congress, and the industry itself will be making difficult and complicated decisions in the near term about how to protect users of social networking sites from the misuse of information that they have provided on a social network. Several recent controversies over a social network's use of personal information have the potential of spurring Congress to enact comprehensive privacy law reform, limiting the amount and use of information available to social networks.[5]

For decades, artists, politicians, and ordinary people alike have fretted over the United States government wiretapping their phones and tracking their movements by satellite and other "creepy" mechanisms of government surveillance.[6] Indeed, in George Orwell's classic, *1984*, government surveillance was central to creating the terrifying persona of Big Brother.[7] The recent revelation by author Matthew M. Aid that the National Security Agency ("NSA") is constructing a storage site to catalog quotidian email conversations between American citizens only serves to substantiate those anxieties.[8] Even in the private sector, these

---

[5] *See* discussion *infra* Part I.A.4.

[6] *See, e.g.*, Jeremy Redmon, *Cameras May Police City Street*s, ATLANTA J.-CONST., Oct. 26, 2009, at A1 ("'It's kind of creepy,' said Marc Rotenberg, Executive Director of the Washington-based Electronic Privacy Information Center. 'Mass surveillance is essentially directed toward everyone, so it doesn't matter if you are someone planning a crime or if you are a resident or tourist or someone who is walking into an office building to go to work. Everyone gets swept into these big databases.'").

[7] GEORGE ORWELL, 1984 (Thomas Pynchon ed., Penguin Books 2003) (1949).

[8] *See* MATTHEW M. AID, THE SECRET SENTRY: THE UNTOLD HISTORY OF THE NATIONAL SECURITY AGENCY 286–309 (2009); *see also* James Bamford, *Who's in Big Brother's Database?*, N.Y. REV. BOOKS, Nov. 5, 2009, http://www.nybooks.com/articles/23231 (describing the construction of a NSA facility that is designed to hold at least "a septillion pages of text").

> On a remote edge of Utah's dry and arid high desert, where temperatures often zoom past 100 degrees, hard-hatted construction workers with top-secret clearances are preparing to build what may become America's equivalent of Jorge Luis Borges's "Library of Babel," . . . .
>
> . . . It's being built by the ultra-secret National Security Agency—which is primarily responsible for "signals intelligence," the collection and analysis of various forms of communication—to house trillions of phone calls, e-mail messages, and data trails: Web searches, parking receipts, bookstore visits, and other digital "pocket litter."

Bamford, *supra*.

concerns have long been a focal point of anxiety in futuristic interpretations of our society. In *Minority Report*, for example, the character played by Tom Cruise receives advertisements projected onto his eyes based on where he is at the moment.[9] The eerie music and dark, ominous atmosphere suggest that if society ever reaches that point, doom is surely just around the corner.

Recent developments in location-based social networking applications[10] bring the American populace far closer to location-specific advertising than ever before and are forcing Americans, courts, and Congress to reimagine and redefine privacy rights and expectations. With applications like Loopt,[11] Foursquare,[12] and any of the thousands of applications available on the iPhone, the Internet community is ironically creating, using, and exploring the very surveillance and lack of privacy that the general population feared for so long. The potential for aggregating personally identifiable information ("PII") across a dizzying array of start-up social networks has the potential of completely erasing the idea of privacy and anonymity on the Internet. Second generation start-up social networks allow users to share a pattern of their locations with their "friends"[13] (Foursquare), a virtual catalogue of their possessions via YingYang.com,[14] and their real-time credit card purchases (Blippy).[15] As users of second generation social networking allow their "friends" to track their movements on a continual basis, and allow them access to increasing amounts of personal information, it will become increasingly important for the

---

9 MINORITY REPORT (Twentieth Century Fox Film Corp. 2002).

10 Location-based social networking refers to applications, websites, and online networks that use global positioning system ("GPS") technology to pinpoint the real-time location of the user and allow other users access to that information. GPS uses satellites and a hand-held device carried by the user to track the location of the user and then broadcast that location on the Internet. *See, e.g.*, *infra* text accompanying note 13.

11 About Loopt, http://www.loopt.com/about (last visited Feb. 18, 2010).

12 Foursquare, http://www.foursquare.com (last visited Feb. 18, 2010).

13 *Id.* A "friend" on Facebook or YingYang is a connection requested by one user and confirmed by another user, which allows both parties access to certain information each user has provided to the site. Usually, the "friending" process substantiates an existing real world connection, but not always. *See, e.g.*, William Lozito, *Facebook Linguistics: Changing the Definition of Friend/Unfriend*, NAME WIRE, Jan. 30, 2009, http://www.namedevelopment.com/blog/archives/2009/01/facebook_lingui.html.

14 YingYang, http://www.yingyang.com (last visited Feb. 18, 2010).

15 Blippy, http://www.blippy.com (last visited Feb. 18, 2010).

sites themselves to actively and cooperatively ensure the protection of their users' privacy.

We are at the dawning of a new age in terms of privacy, and the rapidly changing landscape of privacy rights and expectations will force hard decisions to be made regarding what aspects of a person's identity should be protected as private information as users of social networks willingly divulge more and more personal information. As social networks expand and share their application programming interfaces ("APIs"), information posted and shared by users will be updated across platforms. Likewise, when information is shared across and between social networks, the enforceability and predictability of which privacy policy governs that sharing of that information becomes complicated. This Note seeks to make sense of U.S. privacy law as it relates to social networking. With more and more social networks making use of location-based technology, and an increasing amount of information existing online about social networking users, the issues raised in this Note and how courts, legislatures, and the Internet community resolve them will undoubtedly shape the future of technology, communication, and Internet commerce.

Recent scholarship on legal issues relating to privacy policies and the enforceability of terms of use agreements has been written from the perspective of consumers,[16] alternatively warning users of "contracting away control over personal information,"[17] accusing social networks of "industrial-scale identity theft"[18] and seeking

[16] *See, e.g.*, Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1459 (2001) (arguing that the sale and commercial use of users' information is a violation of individual privacy rights); Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1878 (2003) (advocating greater consumer privacy rights through the gathering of personal information by Internet companies during bankruptcy proceedings); Andrew Hotaling, Comment, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 531 (2008) (arguing that consumers are "[i]nadequately protected against private actors by state and federal statutes").

[17] *See generally* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN. ST. L. REV. 587 (2007).

[18] Rohit Khare, *Privacy Theater: Why Social Networks Only Pretend to Protect You*, TECHCRUNCH, Dec. 27, 2009, http://www.techcrunch.com/2009/12/27/privacy-theater.

legal avenues, as strained as they may be, of holding websites liable for using personal information.[19] This Note takes an alternative perspective by advocating an approach that focuses on increased industry self-regulation, recognizing that overprotection of consumer privacy has the potential to stifle entrepreneurship and cripple Internet-based commerce and innovation. Despite concerns over users not reading or understanding the terms of use agreements that govern the use of personal information on a social network, a more flexible, reactive, and fluid approach to privacy[20] offers the benefit of being able to adapt to the incredibly rapid pace of change in privacy expectations due to the growth and use of social networks.[21] This approach does not suggest that social networks abdicate responsibility for their users' privacy. Rather, it encourages the social networking industry, which includes businesses as small as YingYang and those as dominant as Google, to take several steps to affirmatively protect their users' privacy and create an environment where users can feel comfortable sharing information. As comprehensive legislative overhauls of privacy law wind their way through the legislative process, this Note urges Congress to be aware of both the tradition of Internet self-regulation and the benefits of a laissez-faire approach to privacy before taking irreversibly misguided action.[22]

---

[19] Yasamine Hashemi, Note, *Facebook's Privacy Policy and Its Third Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 150–56 (2009) (exploring "whether Facebook's privacy policy could be used to bring a cause of action" and describing three potential claims users might pursue against Facebook).

[20] *See, e.g.*, Facebook's Privacy Policy, http://www.facebook.com/policy.php (last visited Feb. 18, 2010).

[21] Facebook, for example, as of this writing, is less than six years old and yet has over 350 million users. Facebook Factsheet, http://www.facebook.com/press/info.php?statistics (last visited Jan. 27, 2010).

[22] *See, e.g.*, Personal Data Privacy and Security Act, S. 1490, 111th Cong. (2009). Senator Leahy introduced the PDSA with the following goals:

- Increase criminal penalties for identity theft involving electronic personal data and make it a crime to intentionally or willfully conceal a security breach involving personal data;
- Give individuals access to, and the opportunity to correct, any personal information held by commercial data brokers;
- Require entities that maintain personal data to establish internal policies that protect the personal data of Americans;

Part I of this Note examines the existing laws and jurisprudence on privacy, terms of use agreements, and issues surrounding user-generated content. While courts, legislatures, and academics have put forth many potential resolutions to the privacy issues discussed in this piece, this Note will examine three: a common law approach, a comprehensive statutory approach, and a free-market approach. Part II of this Note analyzes two approaches to modifying privacy law and terms of use agreement law to respond to recent issues that have arisen as a result of location-based social networking applications and sites. One approach is the common law modification approach, whereby courts take it upon themselves to reshape terms of use agreements when the plaintiff alleges an infringement of privacy. The second approach is a legislative one, advocated and adopted by international communities and a number of legal academics, which would comprehensively overhaul privacy law in the United States. Part III offers an alternative approach to both of the approaches discussed in Part II; while recognizing a limited role for Congress, this approach relies on the free market and cooperative action by social networks to remedy and prevent breaches of privacy and use of personal information. Relying on recent events in the social networking industry and recognizing the complexity that APIs contribute to the enforceability of terms of use agreements, the approach offered by this Note encourages Congress to codify and courts to apply strict notice requirements to terms of use agreements. At the same time, this Note argues against legislative interference with social networks, which would be a radical reversal for United States privacy policy. As this Note will argue, the free market and industry self-regulation offer the most

- Require entities that maintain personal data to give notice to individuals and law enforcement when they experience a breach involving sensitive personal data; and
- Require the government to establish rules protecting privacy and security when it uses information from commercial data brokers, to conduct audits of government contracts with data brokers and impose penalties on government contractors that fail to meet data privacy and security requirements.

Press Release, U.S. Senator Patrick Leahy, Judiciary Committee Advances Leahy's Cybersecurity Bill (Nov. 5, 2009), *available at* http://leahy.senate.gov/press/press_releases/release/?id=bf6687fb-676b-4444-91bb-c66afec6cb9a.

practical, effective, and predictable approach for both consumers and companies in a rapidly changing landscape of privacy expectations in the social networking space.

I. THE EVOLUTION OF TERMS OF USE AGREEMENTS LAW IN THE UNITED STATES

Part I.A of this Note examines the history of privacy law in the United States. Recognizing the complexities of privacy law as a discrete sector of U.S. law, this Note focuses with particular emphasis on information privacy law. Legal protection for basic information privacy has deep roots in American and English jurisprudence, yet does not resemble the comprehensive and thoroughness of other legal systems. Part I.B analyzes the intersection of basic contract principles in terms of use agreements. Terms of use agreements, which are primarily a common law creation, fit untidily within traditional notions of contract law, thereby perpetuating an uneasy tension as courts seek to interpret their creation and content in the Internet age.

A. Privacy Law

Privacy law, as a discrete sector of American law, is a rather fragmented and incomplete body of law.[23] This Note looks specifically at information privacy law, which is distinguished from sexual privacy law or family planning privacy law.[24] Information privacy law derives from three primary sources: (1) the Constitution, (2) legislation, and, to a lesser extent, (3) academia.[25] Part I.A.1–3 of this Note will examine the development of information privacy law in chronological order. Accordingly, Part I.A of this Note will begin by looking at the

---

[23] *See, e.g.*, Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws*, MSNBC, Oct. 16, 2009, http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost.

[24] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1094 (2002) [hereinafter Solove, *Conceptualizing Privacy*] (identifying six classifications of privacy rights, one being "control over personal information").

[25] *See* Hotaling, *supra* note 16, at 541 (explaining the sources of information privacy law); *see also* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 855–56 (3d ed. 2006).

colonial era, followed by the nineteenth century and into the twentieth century, when privacy law became institutionalized. Finally, Part I.A.4 will look at twenty-first century developments in information privacy law. By exploring the roots of information privacy law, this subsection will seek to provide a working definition of information privacy rights and explore the complexities posed by social networking sites to those rights.

1. Colonial Era Foundations of Information Privacy Law

This section of this Note will examine the roots of information privacy law. Although understandings, definitions, and implications of information privacy law have morphed considerably since the eighteen and nineteenth century, shaping the future of information privacy law requires an understanding of its roots.[26] Despite the low population density of America at its founding, early American laws demonstrate that privacy was not taken for granted.[27] The relatively few number of people in these early settlements meant, "everybody knew each other's business."[28] Accordingly, laws existed to protect personal privacy. Professor Solove identifies laws against eavesdropping[29] and against being a "common scold," which applied only to women as early examples of privacy focused laws.[30] Importantly, both of these examples of colonial privacy protection law assume a lack of consent by the invadee. In other words, presumably, should those who are speaking grant permission to the "eavesdropper" to "listen under walls or windows," the action would no longer be a crime,

---

[26] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 2 (2d ed. 2009) ("Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law. Information privacy law is relatively new, although its roots reach far back.").

[27] DAVID FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 133 (1972).

[28] Daniel J. Solove, *The Origins and Growth of Information Privacy Law*, 828 PLI/Pat 23, 27 (2005) [hereinafter Solove, *Origins*].

[29] *Id.* at 27 (citing 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 168 (1769)) (defining eavesdropping as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales").

[30] *See* DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 7 (1978).

even if the eavesdropper heard more than the invadee originally intended.

Nonetheless, early American privacy laws focus primarily on intrusions of the government on privacy.[31] Of particular concern to prominent early Americans was the government's use of general warrants and writs of assistance.[32] Noted as "the worst instrument of arbitrary power . . . that ever was found in the English law book,"[33] writs of assistance allowed officials to enter a house and conduct "sweeping searches and seizures without any evidentiary basis."[34] General warrants authorized similarly intrusive searches and seizures, often resulting in the ransacking and arbitrary seizure of the papers and writings of political dissenters.[35] Again, it is important to note that the Framers were principally concerned with the one-sided, powerful central government conducting unauthorized searches of the house.

The Framers formalized their concerns with privacy in the Bill of Rights, with privacy being a central component of the Third, Fourth, and Fifth Amendments. The Third Amendment protects the privacy of the home by barring the government from requiring the quartering of soldiers in a private home, "without the consent of the Owner."[36] The Fourth Amendment "provides broad limitations on the government's power to search and seize"[37] and

---

[31] *See* Solove, *Origins*, *supra* note 28, at 28 ("At the time of the Revolutionary War, the central privacy issue was freedom from government intrusion.").

[32] *See id.* (citing LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 8 (1994)).

[33] James Otis, Against Writs of Assistance, Boston, Mass. (Feb. 1761) (transcript available at The National Humanities Institute).

[34] Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1998).

[35] *See* DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 38 (1979); *see also* William Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 405–07 (1995).

[36] U.S. CONST. amend. III. For a more fulsome analysis of laws protecting the privacy of one's home, see Solove, *Origins*, *supra* note 28, at 27–28 (citing Semayne's Case, (1604) 77 Eng. Rep. 194 (K.B.); BLACKSTONE, *supra* note 29, at 168; Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1894 (1981)). Professor Solove identifies protection of one's home as fundamental to the idea of privacy law in America. *See id.*

[37] Solove, *Origins*, *supra* note 28, at 28.

prevents the practice of general warrants or overly broad searches conducted by the government.[38] Finally, the Fifth Amendment gives individuals the right not to be compelled to testify against themselves.[39] The government cannot compel an individual to speak against his own interests during a criminal proceeding.[40] A detailed examination of these amendments is beyond the scope of this Note, however, it is nonetheless important for courts, legislatures and start-up companies alike to recognize that America's earliest attempts to protect its citizens from privacy intrusions focused on arbitrary searches in which one party did not give consent to the other party for such an intrusion.

2. The Nineteenth and Twentieth Century in Information Privacy Law

During the nineteenth century, American law began to mature as more discrete privacy concerns began to arise. The practice of collecting information for the census became controversial when the number of personal questions asked by the federal government boomed from four for the first census in 1790 to 142 in 1860.[41] A public outcry erupted in 1890 when the census asked about family diseases and finances, leading to legislation in the early twentieth century limiting the scope of information included in and produced by the census.[42] Additionally, the security and confidentiality of the mail system were major issues during the nineteenth century.[43]

---

[38] *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[39] U.S. CONST. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.").

[40] *Id.*

[41] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 46 (1995).

[42] *Id.* at 47.

[43] Solove, *Origins*, *supra* note 28, at 30.

Benjamin Franklin, George Washington, Thomas Jefferson, Alexander Hamilton, and even Ralph Waldo Emerson expressed concerns over their ability to transmit correspondence safely and privately.[44] Concerns with the security of the mail system led Congress to pass several laws criminalizing the unauthorized opening of mail.[45] The Supreme Court provided constitutional protection to privacy of correspondence when it held, in *Ex parte Jackson*,[46] that the Fourth Amendment required government officials to obtain a permit before opening letters.[47]

Mirroring the privacy concerns that have arisen as a result of the expansion of the Internet, the development of a new technology, telegraphs, raised red flags over privacy of correspondence and control of personal information.[48] During the Civil War, the Union and Confederate armies tapped each other's telegraph lines and rival news organizations attempted to "scoop" each other by intercepting telegrams.[49] *The New York Times* called the practice "an outrage upon the liberties of the citizen."[50] While a bill introduced in Congress to protect telegraphs ultimately failed, several courts secured the privacy of telegraphs by analogizing them to letters and more than half of the states enacted

---

44 *Id.*; *see also* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 49–50 (2000) (explaining that Benjamin Franklin required his employees to swear not to open his mail and describing Emerson's frustrations with the mail system).

45 SMITH, *supra* note 44, at 50–52. A statute passed in 1825 provided:

> Whoever takes any letter, postal card, or package out of any post office or any unauthorized depository for mail matter, or from any letter or mail carrier, . . . before it has been delivered to the person to whom it was directed, with design to obstruct the correspondence, or to pry into the business or secrets of another, or opens, secretes, embezzles, or destroys the same, shall be fined . . . or imprisoned.

Id. at 52.

46 96 U.S. 727 (1877).

47 *Id.* at 733.

48 *See* Solove, *Origins*, *supra* note 28, at 31–32.

49 *Id.* at 31; *see also* REGAN, *supra* note 41, at 111.

50 SEIPP, *supra* note 30, at 31.

laws prohibiting the disclosure of telegraph messages by company employees.[51]

Commentators also point to the Supreme Court's decision in *Boyd v. United States*[52] as an important development in information privacy law.[53] In *Boyd*, the government sought to compel a merchant to produce personal and business documents in a civil forfeiture proceeding.[54] The Court relied on both the Fourth and Fifth Amendments in striking down the government's request.[55] In its most articulate definition of privacy to that point, the Court stated that allowing such a request would be an "invasion of [the merchant's] indefeasible right to personal security, personal liberty and private property."[56] Accordingly, *Boyd* and its progeny established a powerful legal recognition of personal privacy.[57]

In 1890, Samuel Warren and Louis Brandeis published *The Right to Privacy*,[58] an article that would define and shape close to a century of privacy law.[59] Warren and Brandeis argued that common law could and should develop greater protections for privacy rights.[60] Warren and Brandeis's article is particularly

---

[51] *See, e.g.*, *Ex parte* Brown, 72 Mo. 83, 95 (Mo. 1880) (holding that a subpoena for telegrams must fail because "such an inquisition . . . would destroy the usefulness" of telegrams); *see also* SEIPP, *supra* note 30, at 65.

[52] 116 U.S. 616 (1886).

[53] *See, e.g.*, SEIPP, *supra* note 30, at 70; Solove, *Origins*, *supra* note 28, at 32; William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1054–55 (1995).

[54] *Boyd*, 116 U.S. at 619.

[55] *See id.* at 634–38.

[56] *Id.* at 630.

[57] Stuntz, *supra* note 53, at 1050.

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

[59] *See, e.g.*, ALPHEUS MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946) (noting that the article "add[ed] a chapter to our law"); Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (calling the Warren and Brandeis article the "most influential law review article of all"); Solove, *Origins*, *supra* note 28, at 34 (describing the publication of Warren and Brandeis's article as "the most profound development in privacy law").

[60] Warren & Brandeis, *supra* note 58, at 198 ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."); *see also* Solove, *Origins*, *supra* note 28, at 35 ("Warren and Brandeis argued that the common law could readily develop a remedy for protecting privacy.").

relevant to this Note because it argued that the development of technology, most notably "instantaneous photography,"[61] and an increase in the availability and prevalence of newspapers would lead to widespread privacy abuses.[62] Warren and Brandeis argued that these threats required a remedy and recognized that existing tort law, such as defamation and libel, protected against the spread of false information but not true private information.[63] They acknowledged however, that traditional common law concepts such as contract and property were not adequate for the mode of protection they envisioned and, instead, urged courts to develop a discrete common law action and remedy for protecting privacy based on a more general right of "the individual to be let alone."[64] Arguably, privacy rights and protections reached an apex towards the end of the nineteenth century.[65] Congress and courts retreated significantly from such an inclusive definition of privacy as the twentieth century progressed and the government's need for personal information increased with the rise of the powerful "fourth branch," administrative agencies.[66]

Warren and Brandeis's article had tremendous influence over courts and legislatures in the beginning of the twentieth century.[67] In 1902, the New York Court of Appeals, New York state's highest court, heard the case of *Roberson v. Rochester Folding Box Co*.[68] The court held that the plaintiff, who sued because an advertisement used a picture of her without her consent, failed to

---

61 Warren & Brandeis, *supra* note 58, at 195 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").

62 *Id.* at 196 ("The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.").

63 *See id.* at 214–18.

64 *Id.* at 205, 214–18.

65 *See* Stuntz, *supra* note 53, at 1052 ("As it happened, the cases did not continue along Boyd's path. Beginning in the first decade of this [twentieth] century, Boyd was effectively cabined . . . .").

66 *See* Martin Flaherty, *The Most Dangerous Branch*, 105 YALE L.J. 1725, 1819 (1996).

67 *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388–89 (1960) (recording over 300 privacy cases spawned by the Warren and Brandeis article).

68 64 N.E. 442 (N.Y. 1902).

state a cause of action because "no precedent for such an action [can] be found in the decisions of this court."[69] A significant debate ensued from the court's decision, as *New York Times* editorials and law review articles extolled the need to create a tort for breaches of privacy.[70] In 1903, New York did indeed enact such a statute.[71] In the years following the *Roberson* decision, state courts and legislatures continued to develop privacy law and expand the remedies available to plaintiffs who suffered invasions of that right.[72] By 1960, the Restatement of Torts enshrined much of what Warren and Brandeis had argued for in their landmark article.[73] The Restatement included four privacy torts: (1) Intrusion Upon Seclusion, (2) Public Disclosure of Private Facts, (3) False Light, and (4) Appropriation.[74]

Wiretapping and the power of the federal government to conduct surveillance on American citizens became the central front of the battle for increased privacy rights in the middle of the twentieth century. First, in 1928, the Supreme Court held in *Olmstead v. United States*[75] that the Fourth Amendment did not require the government to obtain a search warrant before wiretapping a telephone.[76] Congress subsequently enacted section 605 of the Federal Communications Act, which prohibited the

---

69 *Id.* at 443.

70 Denis O'Brien, *The Right to Privacy*, 2 COLUM. L. REV. 437, 437 (1902) (providing examples of *New York Times* editorials).

71 For a current version of this law, see N.Y. CIV. RIGHTS §§ 50, 51 (McKinney 2009).

72 *See, e.g.*, Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 70 (Ga. 1905) (holding that the "right of privacy in matters purely private is therefore derived from natural law").

73 The Restatement of Torts is a non-binding but persuasive and ostensibly objective attempt by a committee of experienced practitioners and legal academics to articulate a consensus on the current state of tort law.

74 RESTATEMENT (SECOND) OF TORTS § 652A(2). A detailed discussion of the case law that led to each of these torts is beyond the scope of this Note; see Solove, *Origins*, *supra* note 28, at 37–40, for more discussion and history.

75 277 U.S. 438 (1928).

76 *Id.* at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses of offices of the defendants."). *But see id.* at 473 (Brandeis, J., dissenting) ("Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

interception and disclosure of intercepted communications by federal, but not state, officials.[77] In subsequent Supreme Court decisions,[78] the court limited the reach of § 605, holding that the law restricted officials "only from disclosing intercepted communications in court proceedings," not from wiretapping in the first place.[79] Throughout the twentieth century, wiretapping became widespread and increased exponentially as a result of these rulings.[80]

In the 1960s and 1970s, the Supreme Court substantially developed privacy law in a series of decisions.[81] Ultimately, the Court recognized a "zone of privacy" as a constitutional right insulated from interference by federal and state actors, but stopped short of recognizing such a right as enforceable against private actors.[82] In *Griswold v. Connecticut*,[83] the Court held that the right to privacy against state and federal actors is a "penumbra" of rights "created by several fundamental constitutional guarantees" found in the Third, Fourth, and Fifth Amendments.[84] In *United States v. Miller*,[85] on the other hand, the Court held that personal financial records in possession of third parties are not within the "zone of privacy" recognized in *Griswold*.[86] Congress acted quickly to provide the protection to privacy that the Court refused to recognize in *Miller*.[87]

---

77 Federal Communications Act of 1934, Pub. L. No. 73-416, ch. 652, § 605, 48 Stat. 1064, 1103–04 (codified as amended at 47 U.S.C. § 605 (2006)).

78 *See, e.g.*, Nardone v. United States, 308 U.S. 338, 341 (1939) (finding evidence obtained as the fruit of illegal wiretapping could not be used in court); Nardone v. United States, 302 U.S. 379, 384 (1937) (excluding evidence directly obtained by wiretapping).

79 Solove, *Origins*, *supra* note 28, at 43; *see also* WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, CRIMINAL PROCEDURE 260 (3d ed. 2000).

80 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1128–33 (2002) [hereinafter Solove, *Digital Dossiers*].

81 *See, e.g.*, Whalen v. Roe, 433 U.S. 425 (1977); United States v. Miller, 425 U.S. 435 (1976); United States v. Nixon, 418 U.S. 683 (1974); Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965).

82 *See* Hotaling, *supra* note 16, at 542–43.

83 381 U.S. 479 (1965).

84 *Id.* at 485.

85 425 U.S. 435 (1976).

86 *Id.* at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

87 *See* Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended in scattered sections of the U.S.C.).

While Congress enacted a number of privacy laws in the 1970s,[88] the focus of this Note is on the expectation of privacy and privacy rights between private parties. Congress's first attempt to regulate such commercial behavior came in 1978 with the Right to Financial Privacy Act ("RFPA").[89] In a nod to Justice Brennan's dissent in *Miller*,[90] the RFPA prohibited banks and other financial institutions from disclosing personal financial information about their customers without a subpoena or search warrant.[91] The statute is limited in scope, providing evidence of Congress's hesitation to interfere with the market.

The blossoming of federal legislation protecting privacy in the 1970s would continue in the 1980s with several new statutes, the most significant of which was the Electronic Communications Privacy Act ("ECPA").[92] Title I, the Wiretap Act,[93] and Title II, the Stored Communications Act,[94] of the ECPA dramatically strengthened both the civil and criminal penalties private actors faced for violations of privacy and unauthorized disclosure of

---

88 *See, e.g.*, Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C (2006)); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(a)); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (codified as amended in scattered sections of 20 U.S.C.); Foreign Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1118 (codified as amended in scattered sections of the U.S.C.); Fair Credit Reporting Act of 1970, Pub. L. No. 90-321, 84 Stat. 1128 (codified as amended in scattered sections of 15 U.S.C.); Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 1002).

89 Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended in scattered sections of the U.S.C.).

90 *See Miller*, 425 U.S. at 447–54 (Brennan, J., dissenting); *see also* Hotaling, *supra* note 16, at 543 ("[T]he reasoning behind [Justice Brennan's] dissenting opinion became highly influential in Congress's efforts to protect an individual's reasonable expectation of privacy in various forms of personally identifiable information.").

91 12 U.S.C. § 3407.

92 18 U.S.C. § 2510; *see also* Katherine A. Oyama, *E-Mail Privacy After* United States v. Councilman: *Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 503 (2006) (explaining that the ECPA provides constitutional protection due to the unclear gap in the Fourth Amendment's application to cyberspace); Paul Taylor, *The Scope of Government Access to Copies of Electronic Communications Stored with Internet Service Providers: A Review of Legal Standards*, 6 J. TECH. L. & POL'Y 109, 117 (2001) (noting the enactment of the ECPA as Congress's response to the emergence of electronic communication and the digital era).

93 18 U.S.C. §§ 2510–22.

94 *Id.* §§ 2701–11.

personal information. Reflecting a consistent congressional desire to avoid overly burdening market transactions, the ECPA exempted intentional interceptions of communications if one party to the transaction consented.[95] Further, the Stored Communications Act allows for a defense based on consent.[96] The extent to which a clicked-through terms of agreement amounts to consent for the purposes of avoiding liability under the ECPA and other federal privacy laws is the subject of much debate and, partially, the focus of this Note.[97] Nonetheless, it is clear that Congress intended to allow private parties a means of contracting around the restrictions embodied in the ECPA.[98]

3. Recent Developments in the Law of Information Privacy

The computer came into the public consciousness during the 1960s and sparked an immediate concern with privacy disclosures made through the computer.[99] The interests and concerns first expressed at the dawn of the computer age have become more acute as personal computing has grown and the data collected by Internet-based companies has become more comprehensive. Congress has reacted by passing a number of privacy protection statutes.[100] The most important mechanism in enforcing privacy protection has been the Federal Trade Commission's ("FTC") efforts to make companies accountable when they violate their own privacy policies.

---

95 *Id.* § 2511(2)(d).

96 *Id.* § 2702(b)(3).

97 *See* discussion *infra* Part II.

98 *See* Hotaling, *supra* note 16, at 545.

99 *See* Solove, *Origins*, *supra* note 28, at 48 & n.162 (citing MYRON BRENTON, THE PRIVACY INVADERS (1964); ARTHUR MILLER, THE ASSAULT ON PRIVACY (1971); NOMOS XII: PRIVACY (J. Ronald Pennock & J.W. Chapman eds., 1971); VANCE PACKARD, THE NAKED SOCIETY (1964); ALAN WESTIN, PRIVACY AND FREEDOM (1967); ALAN WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY (1972); Clark C. Havighurst, Foreword: Symposium, *Privacy*, 31 LAW & CONTEMP. PROBS. 251 (1966); Kenneth L. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342 (1966); Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968)).

100 *See* Acts cited *supra* note 88.

One statute that merits consideration is the Gramm-Leach-Bliley Act ("GLBA") of 1999.[101] The law allowed financial institutions with different branches to share "nonpublic personal information" between affiliates.[102] The law included a requirement for affiliates to notify customers that their information would be shared, but it did not allow consumers to stop the sharing.[103] The law is important because it demonstrates Congress's lack of consistency on the issue of privacy, as this law lacks even the consent requirement most other laws contained. Most financial institutions did include an opt-out provision, but few customers opted-out, complaining that the privacy policies were confusing or misleading.[104] The arguments against the opt-out provisions financial institutions used to comply with the GLBA are similar to those being advanced presently by courts, legislators, and consumer advocates against the click-through terms of use used by most websites today—they complain that the agreements are vague, cumbersome, and difficult to understand.[105]

Over the past ten years, the FTC has been responsible for the largest amount of work with respect to protecting personal information on the Internet.[106] The FTC can bring enforcement actions against companies who fail to abide by their own privacy policies.[107] Enforcement actions for violations of privacy policies are generally resolved between the company and the FTC in a settlement, resulting in a dearth of case-law on the subject.[108] However, it seems clear that as long as the company abides by its

---

101 Gramm-Leach-Bliley Act of 1999, Pub L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. §§ 6801–09).

102 15 U.S.C. § 6802(a)–(b).

103 *Id.*

104 Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230–31 (2002).

105 *See* Hotaling, *supra* note 16, at 552.

106 *See* Haynes, *supra* note 17, at 603, 613–14; Hashemi, *supra* note 19, at 155.

107 Federal Trade Commission Act, 15 U.S.C. § 45(a)(1)–(2).

108 Hashemi, *supra* note 19, at 155–56; *cf.* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004) (highlighting that only a few cases explain how the Stored Communications Act works).

own privacy policy, regardless of how broad it may be, the company will likely not be subject to FTC enforcement.[109]

While the events of September 11, 2001, certainly reshaped privacy as a body of law, most of those shifts have occurred within the government-citizen relationship. The focus of this Note concerns privacy law between private parties in the commercial context, and accordingly, this Note will not focus on the USA PATRIOT Act[110] or related wiretapping issues raised in the wake of the terrorist attacks of 9/11. More important to this discussion is the extent to which terms of use agreements and contracts validly transfer rights of control over personal information freely given by users to companies on the Internet.

4. Recent Controversies

Lately, there has been increasing attention paid to the information that users of social networking sites disseminate on the Internet and to the control social networking sites exercise over that information.[111] Of particular concern is the extent to which social networking websites should be allowed to sell, distribute, or otherwise transmit information to third party application developers.[112] Once a user submits information about his or her birthday for example, the social network can then give that

[109] *See* Hashemi, *supra* note 19, at 156; *cf.* Haynes, *supra* note 17, at 588 ("[I]f the website complies with its own promises, there is little else to prevent the site from doing with the information whatever it wants—sharing, selling or otherwise making use of the information—besides the website company's own interest in attracting and maintaining customers.").

[110] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered titles of the U.S.C.).

[111] *See* Jason Kincaid, *Massive Facebook and MySpace Flash Vulnerability Exposes User Data*, TECHCRUNCH, Nov. 5, 2009, http://www.techcrunch.com/2009/11/05/massive-facebook-and-myspace-flash-vulnerability-exposes-user-data; *see also* Jason Kincaid, *Facebook Rewrites Privacy Policy, Foreshadows Location Services*, TECHCRUNCH, Oct. 29, 2009, http://www.techcrunch.com/2009/10/29/facebook-rewrites-privacy-policy-foreshadows-location-based-services; Posting of Alistair Croll to GigaOm, *Big Internet Is Web 2.0's OS—So Who Owns the Apps?*, http://gigaom.com (Oct. 18, 2007, 21:00 EST).

[112] *See* ANDREW BESMER ET AL., SOCIAL APPLICATION: EXPLORING A MORE SECURE FRAMEWORK 1 (2009), *available at* http://cups.cs.cmu.edu/soups/2009/proceedings/a2-besmer.pdf.

information to an external developer.[113] The external developer can then plug that information into an algorithm, which then becomes permanently part of the third party's program or application.[114] Even if the user abandons the social network, the user's information is not only no longer within the user's control, it is also no longer within the social network's control.[115] This situation raises significant issues about privacy as the relationship, as is, creates a nearly irrevocable level of access to the user's information once the user agrees to the terms of use agreement.

In November of 2007, Facebook launched its now infamous Beacon program with forty-four partner websites.[116] Beacon essentially tracked a Facebook user's movements around the Internet and broadcast certain activities on the user's wall as part of his or her news feed.[117] Even if a Facebook user was not signed into Facebook at the time, information between Facebook and the partner site was exchanged and then disseminated via Facebook.[118] Lacking an obvious opt-out mechanism and instituted automatically, Beacon soon became a focal point of user ire, prompting a string of critical blog posts on technology blogs and a number of Facebook user groups devoted to its termination.[119] Sure enough, in early 2009, Facebook abandoned the program and apologized to its users for abusing their trust and personal

---

113 *Id.*

114 *Id.*

115 *See, e.g.*, Facebook's Privacy Policy, *supra* note 20.

116 Press Release, Facebook, Leading Websites Offer Facebook Beacon for Social Distribution (Nov. 6, 2007), http://www.facebook.com/press/releases.php?p=9166 ("Additional websites and companies participating in Beacon at launch include AllPosters.com, Blockbuster, Bluefly.com, CBS Interactive (CBSSports.com & Dotspotter), ExpoTV, Gamefly, Hotwire, Joost, Kiva, Kongregate, LiveJournal, Live Nation, Mercantila, National Basketball Association, NYTimes.com, Overstock.com, (RED), Redlight, SeamlessWeb, Sony Online Entertainment LLC, Sony Pictures, STA Travel, The Knot, TripAdvisor, Travel Ticker, TypePad, viagogo, Vox, Yelp, WeddingChannel.com and Zappos.com.").

117 *Id.*

118 *Id.*

119 *See, e.g.*, The Idea Shower, *Block Facebook Beacon*, http://www.ideashower.com/blog/block-facebook-beacon (Nov. 7, 2007).

information.[120] During the Beacon program, Facebook faced the defection of thousands of users.[121]

Facebook caused another controversy with its changes in terms of use and privacy policy in December 2009. On December 5, 2009, Facebook alerted all of its members when they signed on to the site that their privacy settings had been changed and were now set for automatic indexing on public search engines. Previously, the information on Facebook was not accessible via a standard search engine. The "blogosphere" erupted in outrage over Facebook's change in policy.[122] As of the writing of this article, Facebook has not responded to the controversy. Facebook's two privacy controversies attract attention to a difficult and complicated issue, thereby strengthening calls for Congress to pass laws making Facebook's abuse of privacy illegal.

Second generation social networks have contributed to recent worries regarding privacy as well. RockYou, a social networking site, had accumulated 32,603,388 users and their personal identification since its launch in 2006.[123] On December 14, 2009, the company came under a firestorm of criticism when Imperva, a security firm, discovered that RockYou stored the passwords of all of its users in an easily accessible, plaintext format online.[124] By storing the websites in such an obvious manner and by not protecting the information from discovery, RockYou demonstrated

---

120 *Facebook to Terminate the Beacon Program*, FINANCIAL, Aug. 12, 2009, http://www.finchannel.com/Main_News/Tech/53576_Facebook_to_terminate_the_Beacon_program.

121 On December 3, 2009, Facebook settled a set of claims concerning its Beacon program and notified users of the settlement. *See* Posting of Nick O'Neil to All Facebook, *Facebook Users Receive Notice of Pending Class Action Settlement*, http://www.allfacebook.com/2009/12/facebook-users-receive-notice-of-pending-facebook-settlement/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+allfacebook+%28Facebook+Blog%29 (Dec. 3, 2009, 18:45 EST).

122 *See, e.g.*, Jason Kincaid, *The Facebook Privacy Fiasco Begins*, TECHCRUNCH, Dec. 9, 2009, http://www.techcrunch.com/2009/12/09/facebook-privacy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch&29; Brennon Slattery, *Why Privacy Concerns Are Ruining Facebook*, PCWORLD, Dec. 2, 2009, http://www.pcworld.com/article/183530/why_privacy_concerns_are_ruining_facebook.html.

123 *See* Khare, *supra* note 18.

124 *Serious SQL Flaw Could Have Compromised Millions of Rockyou.com Users*, TECHCRUNCH, Dec. 14, 2009, http://www.net-security.org/secworld.php?id=8612.

the vulnerabilities of an industry that lacks statutory protection. RockYou violated its own terms of use agreement by not protecting the information and passwords of its users, yet lawsuits brought in reaction to the security breach are unlikely to yield favorable results.[125]

Despite the existence of privacy laws in Colonial America, in recent decades, information privacy law in the U.S. has been constructed on an ad hoc basis, resulting in a set of rights that depend on private enforcement instead of enforcement through the courts.[126] While courts have certainly been instrumental in initiating and recognizing a set of information privacy rights, most of those rights have been either protected against government intrusion or left to the market to protect in the private sector.[127] Importantly, despite various attempts by Congress to define and protect privacy rights,[128] the rapidly changing landscape of technology and social networks have left current protections and laws in place out of date and ineffective. Social networking sites are effectively being called to ensure online privacy protection by Congress's repeated failures to do so lest users abandon this otherwise beneficial commercial activity.

B. Terms of Use and Basic Contract Principles

Courts have struggled recently to determine the extent to which traditional contract principles apply to terms of use agreements in the electronic commerce context.[129] The resolution of this turmoil will have dramatic consequences for Internet companies, especially

---

[125] *See* Khare, *supra* note 18; *see also* Nik Cubrilovic, *RockYou Hack: From Bad to Worse*, TECHCRUNCH, Dec. 14, 2009, http://www.techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[126] *See* Joel R. Reidenberg, *Enforcing Privacy Rights: Agency Enforcement and Private Rights of Action*, 54 HASTINGS L.J. 877, 877 (2003).

[127] *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868 (7th Cir. 2002) (indicating that plaintiff asserted privacy rights for stored electronic communications).

[128] *See, e.g.*, Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. § 2000aa (2006)); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[129] *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (using ordinary contract principles, a shrinkwrap license is a valid and enforceable contract); Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 596 (S.D.N.Y. 2001) (holding software license agreements are binding contractual agreements).

social networking websites. In order to understand the trouble courts and legislators have with applying traditional contract concepts to click-through terms of use agreements, it is necessary to define different forms of terms of use agreements and how contract law has been applied to them over the past twenty years. The first section of this Part will briefly examine basic contract law and principles. Contract law is, for the most part, a creation of common law, meaning that the rules regulating the construction, interpretation, and enforcement of contracts have been crafted by court decisions on the topic and modified by legislation. Next, this section looks at different forms of terms of use agreements and how the form of a terms of use agreement affects its enforceability in court.

1. Basic Contract Law

A contract is a legally enforceable promise or set of promises.[130] While on its face, this definition seems simple enough, in fact, whether a contract exists at all is often a painstaking and fact-intensive inquiry.[131] Contracts require an agreement; that is, there must be an offer and an acceptance of the terms of a contract in order to create a legally enforceable duty between the two parties to a contract.[132] Additionally, contracts must contain consideration, which is "something (such as an act, a forbearance, or a return promise) bargained for and received by a promisor from a promisee."[133] Again, as used in everyday language, these requirements seem plain and straightforward enough, but decades of case law and competing interpretations

[130] RESTATEMENT (SECOND) OF CONTRACTS § 1 (1981); 1 WILLISTON ON CONTRACTS § 1:1 (4th ed. 1990); JOSEPH M. PERILLO, CALAMARI AND PERILLO ON CONTRACTS 1 (5th ed. 2003).

[131] PERILLO, *supra* note 130, at 1 ("No entirely satisfactory definition of the term 'contract' has ever been devised.").

[132] *Id.* at 2 ("'[A]greement' is at the core of the law of contracts . . . .").

[133] BLACK'S LAW DICTIONARY (8th ed. 2004) (defining consideration as an essential element to a contract "necessary for an agreement to be enforceable" (citing RESTATEMENT (SECOND) OF CONTRACTS § 81 (1979))); *see also* THOMAS E. HOLLAND, THE ELEMENTS OF JURISPRUDENCE 286 (13th ed. 1924) ("'[C]onsideration' has been explained to be 'any act of the plaintiff from which the defendant, or a stranger, derives a benefit or advantage . . . .'").

demonstrate that finding and defining a contract is an endeavor riddled with complications.[134]

A legally enforceable contract requires the assent of the parties it binds.[135] Typically, establishing an agreement requires the process of offer and acceptance.[136] As contract law has developed, there has been disagreement over what standard to use in determining the existence of assent, objective or subjective.[137] Advocates of a subjective approach to determining the existence and meaning of contracts argue that a "meeting of the minds" is required to substantiate the agreement between the parties.[138] The subjective approach to contracts gives respect to party autonomy by recognizing the parties' intentions primarily, instead of the literal meaning of the words in the contract.[139] Strict subjective approaches to contract law would look "solely to the intention of the party" who created the contract or to whom the contract was directed.[140] This approach is impractical because it would essentially allow any party the opportunity to escape its obligations to a contract by pleading that it intended something different than what is written.[141] A more palatable subjective standard "would

---

134 *See* PERILLO, *supra* note 130, at 1–3.

135 *Id.* at 26 ("Usually an essential prerequisite to the formation of a contract is an agreement: a mutual manifestation of assent to the same terms." (citing Russell v. Union Oil, 86 Cal. Rptr. 424 (Cal. Ct. App. 1970); Quality Sheet Metal v. Woods, 627 P.2d 1128 (Haw. Ct. App. 1981); Brown v. Considine, 310 N.W.2d 441 (Mich. Ct. App. 1981); Christenson v. Billings Livestock Comm'n, 653 P.2d 492 (Mont. 1982))).

136 *See id.* at 26 (citing Dura-Wood Treating v. Century Forest Indus., 675 F.2d 745 (5th Cir. 1982); Hahnemann Med. Coll. & Hosp. v. Hubbard, 406 A.2d 1120 (Pa. Super. Ct. 1979); Eisenberg v. Cont'l Cas., 180 N.W.2d 726 (Wis. 1970)).

137 *See* PERILLO, *supra* note 130, at 26–28. *Compare* Samuel Williston, *Mutual Assent in the Formation of Contracts*, *in* SELECTED READINGS ON THE LAW OF CONTRACTS 119, 126 (1931) (advocating a subjective standard for determining the existence of assent), *with* RESTATEMENT (SECOND) OF CONTRACTS § 20 (1980) (requiring objective manifestation of agreement).

138 Joseph M. Perillo, *The Origins of the Objective Theory of Contract Formation and Interpretation*, 69 FORDHAM L. REV. 427, 429 (2000).

139 *Id.*

140 *Id.*

141 *Cf. id.* at 429 ("It is improbable that any economically developed society would fully adopt either of these vantage points. One party's intentions would be subordinated to the idiosyncratic meanings of the other. More importantly, if the legal system permits parties to testify as to their understandings or intentions, perjury as to their subjective states of mind would be extremely difficult to detect.").

allow only such meanings as conform to an intention common to both or all the parties, and would attach this meaning although it violates the usage of all other persons."[142] The subjective approach is popular today in France, though in America, the objective approach holds sway.[143]

The objective approach to contract law has dominated the common law of contracts in America for at least the past century.[144] Like subjective approaches, there is no single "objective approach."[145] One objective approach to contract law is the "general usage" test, which dictates that the terms of the contract are enforceable as written, even if it is clear from other evidence that they are not the terms that either party intended.[146] This approach exhibits less respect for party autonomy than the subjective approach by subordinating the parties' intent to the need for regular application of language; however, it does allow the courts interpreting contracts more ability to maintain consistency and predictability.[147] More moderately, the objective test emphasizes the perspective of "the reasonable person in the position of the addressee" of the terms.[148] This approach allows some room for differing understandings of language in the contract.

---

[142] RESTATEMENT OF CONTRACTS § 227(3) (1932). The first Restatement stated this as a possible standard, but did not adopt it, and instead favored an objective standard.

[143] *See, e.g.*, 2 FORMATION OF CONTRACTS: A STUDY OF THE COMMON CORE OF LEGAL SYSTEMS 1316–19 (R. Schlesinger ed., 1968); BARRY NICHOLAS, THE FRENCH LAW OF CONTRACT 35, 47–49 (2d ed. 1992); *cf.* Perillo, *supra* note 138, at 430 ("Although some observers indicate that in practice there is little difference in result in the application of the French subjective approach and the common law's objective approach, the difference in theory explains, among other things, why in France there is no definitive rule on whether an acceptance is effective on dispatch or on receipt.").

[144] Perillo, *supra* note 138, at 431–32 ("Consequently, contract law, when viewed together with the law of evidence, was a mixture of subjective and objective elements with the objective elements dominating the decisions of almost all concrete cases.").

[145] *See id.* at 431 ("Objective tests also vary.").

[146] *See, e.g.*, Nicholson Air Servs., Inc. v. Bd. of County Comm'rs, 706 A.2d 124, 132 (Md. Ct. Spec. App. 1998) ("When the language of the contract is clear, the court will presume that the parties intended what they expressed, even if the expression differs from the parties' intentions at the time they created the contract."); *see also* Perillo, *supra* note 138, at 431.

[147] *See* Perillo, *supra* note 138, at 431.

[148] *Id.*

Courts generally interpret contracts in modern America using the objective standard.[149] Accordingly, an offer and acceptance by at least two parties creates a set of legally enforceable duties between the parties as specified by the terms of the contract. However, terms of use agreements have recently become problematic for courts. Due to the standardized form of terms of use agreements and the one-sided nature of the offer and acceptance process, courts have begun to look at the terms of use agreements offered by Internet companies as potentially outside the ambit of traditional contract interpretation. Some courts have gone so far as to void terms of use agreements even though those agreements objectively meet the requirements for a valid contract.

2. Terms of Use Agreements

This section seeks to provide a working definition of different terms of use agreements and then discusses which contract doctrines and principles are most directly implicated by the proliferation of terms of use agreements. This Note examines terms of use agreements because they typically govern both the privacy policy and control over the information provided by the user to the Internet company.[150] This is particularly important in the context of social networking websites because users provide vast amounts of data about themselves to these websites.[151] The extent of control that users retain over that information and the right to sell, use, and transmit that personal information is typically addressed in the terms to which users agree before accessing the website and handing over their information to the social network.[152]

---

[149] 2 THEOPHILUS PARSONS, THE LAW OF CONTRACTS 6 (1st ed. 1855) ("Therefore, modern courts interpret contracts according to an 'objective' theory by first looking to the explicit words the parties used, and then by 'giv[ing] to the contract the construction which will bring it as near to the actual meaning of the parties as the words they saw fit to employ . . . will permit.'").

[150] *See generally* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006) [hereinafter Lemley, *Terms of Use*].

[151] *See, e.g.*, Facebook, *supra* note 2.

[152] *See, e.g.*, Facebook's Privacy Policy, *supra* note 20.

a) What is a Terms of Use Agreement?

For the purposes of this Note, a terms of use agreement is a set of promises proposed by a website and agreed to by the user of the website. For example, YingYang.com is a social networking website that bases its concept of "friends" on users who have similar interests in material possessions, such as watch collections, sneakers, and more.[153] When a user visits YingYang.com, he or she is required to accept YingYang, Inc.'s terms of use in order to become a user (i.e., get a handle, create a profile, post and tag pictures, etc.) on YingYang.com.[154] The terms of use agreement henceforth governs the legal duties and liabilities between YingYang, Inc. and the users of YingYang.com. Accordingly, the terms of use agreement delineates the legal responsibilities of both parties and what each party is allowed to do with the information of the other party. Crafting a comprehensive terms of use agreement, therefore, is a crucial aspect of beginning a social networking website as courts will refer to the terms of use agreement to determine any claims that may arise between the two parties.

Terms of use agreements come in three principal forms: shrinkwrap agreements, browsewrap agreements, and clickwrap agreements.[155] Shrinkwrap agreements are licenses included with physical copies of software, purchased by a consumer.[156] The contract theory behind these licenses is that "by breaking the shrinkwrap or running the program" the user consents to the terms of agreement; the user thereby creates a mutually binding contract based on his or her acceptance of the offer of terms of use by the producer of the software.[157] A one-sided bargain offer such as this shrinkwrap agreement is a unilateral contract, and though examples of such contracts are rather scarce in non-electronic scenarios, they do exist.[158]

---

153 About YingYang, http://www.yingyang.com/about (last visited Feb. 18, 2010).

154 YingYang Terms of Use, http://www.yingyang.com/terms (last visited Feb. 18, 2010).

155 *See* Lemley, *Terms of Use*, *supra* note 150, at 459–60.

156 *Id.* at 467.

157 *Id.*; *see also* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1239 (1995) [hereinafter Lemley, *Intellectual Property*].

158 *See* Mark Pettit, Jr., *Modern Unilateral Contracts*, 63 B.U. L. REV. 551, 551 (1983).

Until 1996, every court confronted by shrinkwrap licenses held them unenforceable.[159] Among other reasons, courts noted the lack of an opportunity for the consumer to review the terms before being bound by them,[160] the lack of options for a user if he did not assent to the terms,[161] and the lack of clear evidence of consent on the user's part[162] as reasons to hold shrinkwrap licenses unenforceable. In 1996, Judge Easterbrook wrote an influential opinion upholding the terms of a shrinkwrap terms of use in *ProCD, Inc. v. Zeidenberg*.[163] Judge Easterbrook relied on the Uniform Commercial Code section 2-204, which states that a contract may be formed in any manner to which the parties agree.[164] Accordingly, Judge Easterbrook held that by installing the software, the user consented to the terms of use agreement included in the packaging.[165] While not universally followed,[166] federal courts have, more often than not, held shrinkwrap agreements enforceable since 1996.[167]

---

159 Lemley, *Terms of Use*, *supra* note 150, at 459 (citing Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 102–03 (3d Cir. 1991); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268–70 (5th Cir. 1988); Ariz. Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 763–66 (D. Ariz. 1993); Foresight Res. Corp. v. Pfortmiller, 719 F. Supp. 1006, 1009–10 (D. Kan. 1989)).

160 *See, e.g.*, *Step-Saver*, 939 F.2d at 104.

161 *See, e.g.*, *Vault Corp.*, 847 F.2d at 270.

162 *See, e.g.*, *Ariz. Retail Sys.*, 831 F. Supp. at 766.

163 86 F.3d 1447, 1455 (7th Cir. 1996).

164 U.C.C. § 2-204 (2004) ("Formation in General. (1) A contract for sale of goods may be made in any manner sufficient to show agreement, including . . . conduct by both parties which recognizes the existence of a contract. . . . (2) An agreement sufficient to constitute a contract for sale may be found even though the moment of its making is undetermined. (3) Even if one or more terms are left open, a contract for sale does not fail for indefiniteness if the parties have intended to make a contract and there is a reasonably certain basis for giving an appropriate remedy."); *ProCD*, 86 F.3d at 1452 ("A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.").

165 *ProCD*, 86 F.3d at 1452–53.

166 *See* Lemley, *Terms of Use*, *supra* note 150, at 469 (citing Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1339 (D. Kan. 2000); Morgan Labs., Inc. v. Micro Data Base Sys., Inc., No. C96-3998TEH, 1997 WL 258886, at *2–4 (N.D. Cal. Jan. 22, 1997); Novell v. Network Trade Ctr., Inc., 25 F. Supp. 2d 1218, 1224 (D. Utah 1997), *vacated in part*, 187 F.R.D. 657 (D. Utah 1999); Rogers v. Dell Computer Corp., 127 P.3d 560, 562 (Okla. 2005), *republished in* 138 P.3d 826, 827 (Okla. 2005)).

167 *Id.* (citing Davidson & Assocs. v. Jung, 422 F.3d 630, 632 (8th Cir. 2005); Bowers v. Baystate Techs., 320 F.3d 1317, 1320 (Fed. Cir. 2003); Adobe Sys., Inc. v. One Stop

Browsewrap agreements are terms of use agreements the user may not read at all; the user, however, consents to the terms of use by using the website.[168] Browsewrap agreements are typically included on a website and accessed by clicking a link which often appears on the bottom of the page.[169] Even in the context of electronic contracting, there is a "dearth of settled law" regarding browsewrap agreements.[170] Underlying the dispute over the enforceability of browsewrap agreements and their validity as contracts is the lack of notice given to users of the actual terms contained within the agreements.[171] The hyperlink at the bottom of a webpage directing users to the terms of use is often insufficient to give the consumers actual notice of the terms of use they are accepting through use of the webpage.[172] Because of the weakness of notice in browsewrap agreements, courts have devised means of protecting consumers but are generally unwilling to extend the same protection to businesses that repeatedly access a website.[173]

Courts generally find that browsewrap agreements are unenforceable when a consumer sues a website to avoid liability under the terms of the browsewrap agreement.[174] However, most often, browsewrap litigation surrounds a company's misuse of a competitor's website,[175] and in these cases, courts will generally

Micro, Inc., 84 F. Supp. 2d 1086, 1086 (N.D. Cal. 2000); Info. Handling Servs., Inc. v. LRP Publ'ns, Inc., No. Civ. A. 00-1859, 2000 WL 1468535, at *1–2 (E.D. Pa. Sept. 20, 2000); Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519 (W.D. Pa. 2000); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305, 307 (Wash. 2000)).

168 Ian A. Rambarran, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?* 2–3 (Bepress Legal Series, Working Paper No. 1885, 2006), *available at* http://law.bepress.com/expresso/eps/1885.

169 *Id.* at 5.

170 *Id.* at 3 (citing Christina Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279, 289 (2003)).

171 *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 20 (2d Cir. 2002).

172 Rambarran, *supra* note 168, at 5 (noting that "browse agreements do not have the same notice guarantees" as other forms of electronic contracting because the terms of the agreement are "incorporated by reference").

173 *See, e.g.*, Lemley, *Terms of Use*, *supra* note 150, at 459, 472–73.

174 *Id.* at 462 (citing Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 556–57 (1st Cir. 2005); Waters v. Earthlink, Inc., 91 F. App'x 697, 698 (1st Cir. 2003); *Specht*, 306 F.3d at 35–38).

175 *Id.* at 472–73.

enforce a browsewrap agreement against the defendant company.[176] This tends to happen when a company exploits another company's user's information for its benefit, either to collect contact information for potential customers or to directly contact users, in violation of the terms of use agreement. The federal courts likely treat these agreements with greater deference to the agreement itself because of an underlying presumption that businesses are more sophisticated parties than the average consumers, and if they are seeking to profit from a given website, they should be aware of the terms of engaging the website.

Clickwrap agreements are the most widely used type of electronic terms of use agreements and the most consistently upheld as enforceable by courts.[177] Clickwrap agreements are terms of use agreements that require the user to click a link that says "I Agree" or otherwise give affirmative consent to the terms of use before accessing the website's content.[178] By forcing the user to scroll through the agreement, or at least presenting him or her with the agreement and requiring action on his or her part, the clickwrap agreements avoid the notice issues present with the browsewrap agreements.[179]

In 2007, the American Bar Association promulgated a series of recommendations to avoid legal issues with electronic contracting. Its "legal best practices for electronic contracting" identified four "bottom line" steps for forming legally binding online contracts:[180]

1. The user must have adequate notice that the proposed terms exist;

---

[176] *Id.* at 460 (citing Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 428–30 (2d Cir. 2004); Cairo, Inc. v. Crossmedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610, at *5 (N.D. Cal. Apr. 1, 2005); Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *1–2 (C.D. Cal. Mar. 7, 2003); Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 982 (E.D. Cal. 2000)).

[177] *See* Lemley, *Terms of Use*, *supra* note 150, at 459.

[178] *Id.*; *see also* Rambarran, *supra* note 168, at 7 ("Click-through agreements require users to assent affirmatively to terms before downloading or using a service or product.").

[179] *See* Rambarran, *supra* note 168, at 7–8.

[180] ThinkingOpen, *How Do I Build an Enforceable Online Agreement?—Not (Always) the Way SalesForce.com or Google Would*, http://thinkingopen.wordpress.com/2008/03/08/how-do-i-build-an-enforceable-online-contract-not-always-what-salesforcecom-or-google-would-do (Mar. 8, 2008).

2. The user must have a meaningful opportunity to review the terms;
3. The user must have adequate notice that taking a specified, optional action manifests assent to the terms; and
4. The user must, in fact, take that action.[181]

Clickwrap agreements generally satisfy these requirements by presenting the user with the terms of use before allowing him or her to access content on or interact with the website. Indeed, until recently, nearly every time a court faced a clickwrap agreement, it found it enforceable and binding upon the parties.[182] However, recently there has been tension and disagreement between federal courts and circuits on the issue of enforceability.

b) Contract Doctrines Implicated by Online Contracting

There are several important doctrines of contract law that are implicated by the use of online contracting. First, the doctrine of third party beneficiary is particularly important with regards to social networking websites and user-generated content. Second, a contract voidable for unconscionable terms is also pertinent to this discussion. Finally, contracts voidable for unfair bargaining power are also at issue in this discussion.

The third party beneficiary doctrine is a contract doctrine that allows third parties to a contract to sue and enforce promises or duties intended to protect them even though they are not a party to

---

[181] *Id.*

[182] *See* Lemley, *Terms of Use*, *supra* note 150, at 459 ("Every court to consider the issue has found 'clickwrap' licenses, in which an online user clicks 'I agree' to standard form terms, enforceable." (citing Davidson & Assocs. v. Jung, 422 F.3d 630, 638–39 (8th Cir. 2005); Salco Distribs., L.L.C. v. iCode, Inc., No. 8:05-CV-642-T-27TGW, 2006 WL 449156, at *2 (M.D. Fla. Feb. 22, 2006); Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756, 781–83 (N.D. Tex. 2006); Mortgage Plus, Inc. v. DocMagic, Inc., No. 03-2592, 2004 WL 2331918, at *4–5 (D. Kan. Aug. 23, 2004); i-Sys., Inc. v. Softwares, Inc., No. Civ. 02-1951(JRT/FLN), 2004 WL 742082, at *6 (D. Minn. Mar. 29, 2004); Novak v. Overture Servs., Inc., 309 F. Supp. 2d 446, 451–52 (E.D.N.Y. 2004); i.LAN Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 330–31 (D. Mass. 2002); Hotmail Corp. v. Van$ Money Pie, Inc., No. C-98-20064JW, 1998 WL 388389, at *3–9 (N.D. Cal. Apr. 16, 1998) (granting a preliminary injunction assuming such an agreement was enforceable without reviewing the merits); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 532–33 (N.J. Super. Ct. App. Div. 1999))).

the contract.[183] One requirement is that the contract must have been made for their benefit, thereby largely limiting the doctrine's availability to third parties.[184] Despite several attempts by litigants, the third party beneficiary doctrine has yet to succeed in court to enforce rights based on a terms of use agreement.[185]

Some courts have found certain clauses of the terms of use agreements unenforceable because they were unconscionable or ambiguous. Courts will occasionally invoke "unconscionability" as a reason to "refuse to enforce oppressive bargains on grounds of substantive unconscionability."[186] Ambiguous terms are terms that lack a sufficiently clear definition or context within the contract to be enforceable by courts.[187] As will be discussed later, courts struggle to apply traditional contract principles to electronic contracts as the contemporary form of contract and methods of assent used by the parties clash sharply with older notions of contract law.[188]

Social networking websites exist in a strange tension with their users. Networks like Facebook.com, Loopt.com, and YingYang.com require users to contribute to their websites in order to be a "value added" service. The term "value added" means that as more users contribute to the site with pictures, information, and applications used exclusively by the site and its users, the site becomes more valuable, and, in turn, more used, visited, and profitable. The concept is referred to as "sticky" content because content generated by social networking users that is exclusive to that site sticks to the site and is what draws more

---

183 *See generally* PERILLO, *supra* note 130, at 663–67.

184 *Id.*

185 *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004); Kremen v. Network Solutions, Inc., 337 F.3d 1024 (9th Cir. 2003); Jackson v. Am. Plaza Corp., No. 08 Civ. 8980(PKC), 2009 WL 1158829 (S.D.N.Y. Apr. 28, 2009); Dluhos v. Strasberg, No. Civ.A. 00-3163(JCL), 2005 WL 1683696 (D.N.J. June 24, 2005); Morrison v. Am. Online, Inc., 153 F. Supp. 2d 930 (N.D. Ind. 2001); *see also* Posting of Thomas O'Toole to E-Commerce and Tech Law Blog, *Online, Third-Party Beneficiary Claims Are Likely Losers*, http://pblog.bna.com/techlaw/2009/05/online-thirdparty-beneficiary-claims-are-likely-losers.html (May 1, 2009).

186 PERILLO, *supra* note 130, at 382.

187 *See id.* at 382–87.

188 *See* discussion *infra* Part II.A.

users to use the site.[189] Social networking websites challenge traditional notions of ownership and consumer-owner relationships.[190]

The United States legal system has had a long tradition of defining property and ownership based on the efficient allocation of resources. The Lockean Proviso is a famous edict by one of the seventeenth century's greatest political philosophers, John Locke, and is a fairly traditional view on what creates ownership.[191] The Lockean Proviso argues that the fruits of one's labor are one's own possession.[192] In other words, a person who works on something can claim at least partial ownership of it.

Social networks challenge this understanding of ownership because users are constantly creating, adding to, and producing content on social networking websites, yet they do not own the material or a portion of the site. Rather, the site, by the terms of agreement, co-opts the information and declares ownership of it. Accordingly, users add value to the website; indeed, user-generated content on sites such as Facebook is what makes the site attractive for other users and yet, users never own anything they add to the site.[193]

Ultimately, understanding privacy rights and a social networking site's freedom to use personal information posted or shared by users requires an understanding of both the history of United States privacy law and contract law.[194] Congress has in only rare instances enacted laws codifying privacy rights and only

---

[189] NetLingo, Sticky Content, http://www.netlingo.com/word/sticky-content.php (last visited Feb. 18, 2010) (defining "sticky content" as "[i]nformation or features on a Web site that gives users a compelling reason to revisit it frequently").

[190] *See* Croll, *supra* note 111.

[191] *See generally* JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT (Thomas P. Peardon ed., 1952).

[192] *Id.* at ch. 5 § 27.

[193] In fact, in a recent case, *Finkel v. Facebook*, No. 102578/09, 2009 WL 3240365 (N.Y. Sup. Ct. Sept. 15, 2009), it appears the plaintiffs alleged for the first time anywhere that immunity should not attach when the social networking defendant (in this case, Facebook) actually gains from value-added of user contributions. *Id.* While the case was dismissed, *id.*, this line of reasoning could have important consequences for the future of immunity litigation under 47 U.S.C. § 230 (2006), which generally gives immunity to social networking sites.

[194] *See* discussion *supra* Part I.

on very specific issues, such as the ECPA. Yet, courts continue to reinterpret privacy rights, beginning with *Griswold* and continuing through today. Courts have been attempting to use traditional common law principles to provide greater protection for privacy than legislatively afforded. The use of personal information by social networks gives rise to a host of new privacy considerations. The next Part of this Note will examine two proposals to address the host of issues raised by social networks and location-based technology.

II. THE COMMON LAW AND STATUTORY APPROACHES

Concerns for the privacy of users of social networking sites have led both courts and legislatures to begin to adopt and apply a set of ad hoc rules to provide greater protection for users. There are two principal ways that courts and commentators have approached the issue of increasing privacy protections for social networking site users. First, courts have begun using a common law approach to strike down terms of use agreements as unenforceable when the site has not demonstrated sufficient notice procedures or when the terms of use agreement has been drafted too broadly.[195] Alternatively, commentators have taken cues from Canada and the European Union to suggest adopting a legislative approach to enhancing privacy controls in cyberspace.[196] Advocates of a legislative overhaul tend to suggest amending the ECPA as a legal mechanism to provide consumers with greater protection and control over the content they post on social networking sites.[197]

This Part first looks at several recent court cases that have struck down terms of use agreements as unenforceable. Parsing these decisions is crucial for social networking websites in order to understand what is acceptable in drafting terms of use agreements.

---

[195] *See* discussion *infra* Part II.A (describing recent federal courts' holdings that relied on common law doctrines to strike down terms of use agreements as unenforceable and void).

[196] *See infra* notes 292–306 and accompanying text (explaining recent international edicts on privacy and arguments for amending the ECPA).

[197] *See infra* notes 266–79 and accompanying text.

Additionally, this Part looks at arguments by commentators pushing for a myriad of common law solutions to privacy concerns. Next, this Part collects various academic articles and privacy directives issued by other countries and attempts to distill the essence of what is being proposed as potential changes to the privacy law landscape regarding terms of use agreements.

A. The Common Law Approach to Increasing Online Privacy Protection

Courts have taken the issue of terms of use agreements as they relate to privacy protections rather seriously and have begun to hold terms of use agreements unenforceable, especially when the alleged harm is a privacy infringement. Part I.A will use three cases as examples of the types of limits courts impose on terms of use agreements—*Harris v. Blockbuster, Inc.*,[198] *Specht v. Netscape*,[199] and *Hines v. Overstock.com*.[200] Read together, these cases demonstrate a shift by the federal judiciary towards increasing consumer protection at the expense of web-businesses when privacy concerns are implicated. Courts tend to be more aggressive in interpreting terms of use agreements to the benefit of the user when the user alleges a breach of privacy. Terms of use agreements that precedent suggests should be binding are scrutinized more carefully when privacy concerns are involved. The holding of these cases suggests a shift towards a more interventionist approach to terms of use agreements, transforming the Internet into an area increasingly regulated by the courts.

1. Specht v. Netscape

Specht v. Netscape was the first decision by a court to invalidate a browsewrap agreement, and it involved allegations of privacy infringement.[201] That the court chose this case to invalidate a browsewrap agreement suggests that, as in *Harris*,[202] the court had identified a void in privacy protection and stretched

198 622 F. Supp. 2d 396 (N.D. Tex. 2009).
199 306 F.3d 17 (2d Cir. 2002).
200 No. 09 CV 991(SJ), 2009 WL 2876667 (E.D.N.Y. Sept. 8, 2009).
201 *Specht*, 306 F.3d at 17.
202 *Harris*, 622 F. Supp. 2d at 399.

contract principles to remedy that legislative inadequacy. *Specht* is particularly noteworthy because although the controlling precedent in the Second Circuit would have pushed the court to enforce the terms of use agreement at issue, allegations of breach of privacy seem to have forced the court to ignore precedent and invalidate the agreement.[203] In other words, the court attempted to afford special protection to the privacy rights of the plaintiff, despite precedent.

In *Specht*, the plaintiffs claimed that software downloaded from the defendant's website "invaded plaintiffs' privacy by clandestinely transmitting personal information to the software provider."[204] As in both *Harris* and *Overstock*, the court limited its holding to the enforceability of the arbitration provision, ultimately invalidating it and establishing strong precedent for future terms of use agreement litigation where privacy interests might be at stake. Then-Judge Sotomayor wrote the opinion of the court, holding that the user "did not unambiguously manifest assent to the arbitration provision contained in the license terms."[205]

The plaintiffs claimed that the defendants violated the ECPA by transmitting private information about their use of the defendant's software.[206] The plaintiffs claimed that when they installed the software, they also installed a cookie, "an identification tag for future communications," which allowed the defendants to illegally eavesdrop on their Internet and computer usage.[207] Essentially, the plaintiffs claimed that by installing a cookie on their computer, defendants profited by being able to track a user of the defendants' program's page visits beyond what could have been expected.

The court took particular issue with the lack of notice of terms of use.[208] The court noted that "no clickwrap presentation

---

[203] *See Specht*, 306 F.3d at 36–37.

[204] *Id.* at 17.

[205] *Id.* at 20.

[206] *Id.* at 21.

[207] *Id.* ("These processes, plaintiffs claim, constituted unlawful 'eavesdropping' on users of Netscape's software products as well as on Internet websites from which users employing SmartDownload downloaded files.").

[208] *Id.* at 22.

accompanied" the downloading of the challenged program, SmartDownload.[209] Describing the advantages of a clickwrap agreement, the court noted the differences between a typical clickwrap agreement and the notice described by the plaintiffs in SmartDownload's terms of use agreement.[210] After downloading the program, "these plaintiffs encountered no further information about the plug-in program or the existence of license terms governing its use."[211] Noting that "the sole reference" to the terms of use agreement was a text box on the following page, the court condemned the lack of notice by concluding that the software did not require the plaintiffs "to express unambiguous assent to that program's license agreement nor even to view the license terms or become aware of their existence before proceeding with the invited download of the free plug-in program."[212]

The court proceeded with a lengthy discussion of controlling precedent, noting that all the cases cited by the defendants "were distinguishable on the facts" because they involved "paper contracting."[213] The court noted that the "world of paper contracting" was different, separate, and essentially required different common law principles than "online transactions."[214] Indeed, the court devoted an entire section to explaining why the cases the defendants relied on were not, in its view, applicable to online transactions.[215] Yet, the court used the term "eavesdropping," a word with deep colonial roots,[216] to describe the placing of a cookie on a computer, thereby cognitively linking in-person eavesdropping and online eavesdropping. In essence, the court allowed framing-era privacy language to have the same meaning in both online and in-person scenarios, but required applicable standards for contract interpretation to depend on

---

209 *Id.* at 23.
210 *Id.* at 22–24.
211 *Id.* at 23.
212 *Id.*
213 *Id.* at 33.
214 *See id.* at 31–33.
215 *See id.* at 33–35.
216 *Id.* at 21, 37, 38 (appearing four times in the court's decision, the word "eavesdropping" received positive recognition by the court); *see supra* note 29 and accompanying text.

whether the contract had been agreed to online or in-person.[217] The refusal of the court to allow paper contracting cases to be used by the defense along with its willingness to allow the plaintiffs to freely interchange concepts typically associated with corporeal privacy infringements[218] suggests that the court was making allowances in the interest of providing enhanced protection for online privacy. This case is important for online companies because it shows that courts will occasionally use inconsistent reasoning as a means of ensuring protection of a user's privacy.

2. Harris v. Blockbuster

In *Harris v. Blockbuster, Inc.*, the federal court for the Northern District of Texas held that the terms of use agreement in that case was "illusory and unenforceable" and denied Blockbuster's motion to compel arbitration as stipulated in the terms of use agreement.[219] The plaintiff alleged violations by Blockbuster, Inc. of the Video Privacy Protection Act ("VPPA")[220] resulting from Blockbuster's participation in the Facebook Beacon Program.[221] Ultimately, the court held that the terms of use agreement written by Blockbuster and agreed to by the plaintiff was unenforceable because of a lack of adequate consideration and unconscionable terms.[222]

The Facebook Beacon program generated a lot of controversy.[223] As discussed earlier, it was a program initiated by Facebook through which other websites could create a relationship with Facebook; a Facebook user's activity on another website therefore would be broadcast as a news story on Facebook and appear in a public feed on the site.[224] Users could opt out of the program, but essentially, the privacy concerns expressed by Facebook users ended up scuttling the program.[225] However,

217 *See id.* at 37–38.
218 *See id.* at 31–33.
219 622 F. Supp. 2d 396, 400 (2009).
220 18 U.S.C. § 2710 (2006).
221 *Harris*, 622 F. Supp. 2d at 397.
222 *Id.* at 399.
223 *See supra* notes 116–21 and accompanying text.
224 *See supra* notes 116–21 and accompanying text.
225 *See supra* notes 116–21 and accompanying text.

Harris serves as an example of the concerns many social networking websites have as a result of Facebook's Beacon program.

The plaintiff in *Harris* alleged that Blockbuster's agreement with Facebook, which would allow movie rental choices to be disseminated publicly on Facebook, violated the VPPA.[226] The *Harris* decision did not reach the merits of the claim as it only ruled on the defendant's motion to compel arbitration.[227] The plaintiff, a woman named Cathryn Elaine Harris, brought suit against Blockbuster initially as a class action suit, seeking the maximum allowed $2,500 per infringement as stipulated in the VPPA.[228] Blockbuster sought to compel arbitration and thereby avoid a messy public battle over its role in the privacy debacle created, in part, by the Beacon program.[229]

Blockbuster argued that its terms of use agreement, a clickwrap agreement that Harris had clicked through, specifically authorized the company to use the information in the ways the plaintiff challenged.[230] Blockbuster's terms of use agreement included the following language:

> Blockbuster may at any time, and at its sole discretion, modify these Terms and Conditions of Use, including without limitation the Privacy Policy, with or without notice. Such modifications will be effective immediately upon posting. You agree to review these Terms and Conditions of Use periodically and your continued use of this Site following such modifications will indicate your

---

226 *Harris*, 622 F. Supp. 2d at 397.

227 *Id.*

228 *See* 18 U.S.C. § 2710(c)(2)(A) (2006); Caroline McCarthy, *Blockbuster Sued over Role in Facebook's Beacon Ad Program*, CNET NEWS, Apr. 17, 2008, http://news.cnet.com/8301-13577_3-9921496-36.html.

229 *Harris*, 622 F. Supp. 2d at 398.

230 *Id.* at 397 ("As a precondition to joining Blockbuster Online, customers were required to click on a box certifying that they had read and agreed to the Terms and Conditions."); *see also* Posting of Thomas O'Toole to E-Commerce and Tech Law Blog, *'Illusory' Contract Looks Awfully Familiar*, http://pblog.bna.com/techlaw/2009/04/illusory-contract-looks-awfully-familiar-.html (Apr. 20, 2009) (describing Blockbuster's terms of agreement as "terms that were assented to via a mouse-click").

> acceptance of these modified Terms and Conditions of Use. If you do not agree to any modification of these Terms and Conditions of Use, you must immediately stop using this Site.[231]

The court relied on precedent to rule that the language in the above clause was too broad, one-sided, and unfair to be enforceable.[232] Specifically, the court highlighted the terms "at its sole discretion" and "at any time" to hold that Blockbuster had gone both too far in its reservations of rights to unilaterally amend the contract and not far enough in granting the plaintiff notice of the changes.[233]

The court relied heavily on the Fifth Circuit case *Morrison v. Amway Corporation*[234] to reach its decision in *Harris*. In *Morrison*, the Fifth Circuit invalidated an arbitration provision similar to the one at issue in *Harris*.[235] *Morrison* involved a defendant company, a seller of home goods, that was sued by several plaintiffs for various torts, and sought to enforce an arbitration clause against the plaintiffs.[236] The plaintiffs agreed to the arbitration clause in their contracts with the defendant.[237] The agreement, similar to Blockbuster's, included a clause allowing the defendant to unilaterally alter the contract; "the only express limitation on that unilateral right [was] published notice."[238] This led the court to suggest that the amendments made by the defendant could be applicable to events occurring before the amendments were even published.[239] The *Morrison* court distinguished the amendment clause from a similar one in *In re Halliburton Co.*,[240] which "specifically limited the defendant's ability to apply changes to the agreement."[241]

---

231 *Harris*, 622 F. Supp. 2d at 398–99.
232 *Id.* at 399.
233 *Id.* at 398–99.
234 517 F.3d 248 (5th Cir. 2008).
235 *Id.* at 257; *Harris*, 622 F. Supp. 2d at 397–98.
236 *Morrison*, 517 F.3d at 252–53.
237 *Id.* at 253.
238 *Id.* at 254.
239 *Id.*
240 80 S.W.3d 566, 569–70 (Tex. 2002).
241 *Harris*, 622 F. Supp. 2d at 398 (citing *In re Halliburton Co.*, 80 S.W.3d at 569–70).

Indeed, the lack of limitations on Blockbuster's terms of agreement was determinative in the *Harris* case.[242] The fact that Blockbuster could change the contract at any time and apply those changes to events that occurred before the changes were made created an illusory contract, according to the court.[243] The court then extended the *Morrison* rule by saying that the contract is illusory "even when no retroactive modification has been attempted."[244] In denying the defendant's motion to compel individual arbitration based on the terms of use agreement that the plaintiff had accepted,[245] the court broadened the scope of the *Morrison* ruling and left the enforceability of similar agreements in jeopardy.

The *Harris* decision reverberated throughout the Internet and legal community. It is far too early to tell if *Harris* will have any long-term effect on terms of use agreement drafting or on privacy litigation, but it seems like it may have such an impact, based on the court's reasoning that the real concern here was privacy. The court used an attack on the terms of agreement contract to address an underlying concern with privacy. *Harris* is a warning sign for social networking websites to draft their terms of agreement carefully and attempt to tailor them narrowly to avoid the kinds of problems faced by Blockbuster.

---

[242] *See id.* at 399 ("The Court concludes that the Blockbuster arbitration provision is illusory for the same reasons as that in *Morrison*. Here, as in *Morrison*, there is nothing in the Terms and Conditions that prevents Blockbuster from unilaterally changing any part of the contract other than providing that such changes will not take effect until posted on the website. There are likewise no '*Halliburton* type savings clauses,' as there is 'nothing to suggest that once published the amendment would be inapplicable to disputes arising, or arising out of events occurring, before such publication.' The Fifth Circuit in *Morrison* noted the lack of an 'express exemption' of the ability to unilaterally modify all rules, which the Blockbuster agreement also does not contain. The Blockbuster contract only states that modifications 'will be effective immediately upon posting,' and the natural reading of that clause does not limit application of the modifications to earlier disputes.").

[243] *Id.*

[244] *Id.* at 400.

[245] *Id.*

3. Hines v. Overstock.com

In *Hines v. Overstock.com*, the federal court for the Eastern District for New York denied the defendant's motion to dismiss Cynthia Hines's claims for breach of contract against Overstock.com because it found the terms of use agreement invalid and unenforceable.[246] As in *Harris*, the arbitration clause of Overstock.com's terms of use agreement was the focal point of the court's analysis.[247] However, the case differs from *Harris* because rather than holding that the contract was illusory, the court held that the plaintiff did not receive notice of the terms within the contract sufficient to create a meeting of the minds or actual assent.[248]

Ms. Hines commenced a class action suit against Overstock.com for breach of contract, fraud, and violations of New York General Business Law sections 349 and 350.[249] The claims originated from a thirty dollar "restocking fee" the defendant charged Ms. Hines when she tried to return a vacuum she purchased from Overstock.com.[250] She claimed that she had never been notified or warned of the potential charge.[251] Overstock.com, Inc. responded with a motion to dismiss or stay for arbitration or transfer to the venue stipulated in the terms of use agreement.[252] The relevant portion of the terms of use agreement is as follows: "All retail purchases from Overstock are conducted through Overstock's Internet website. When an individual accesses the website, he or she accepts Overstock's terms, conditions and policies, which govern all of Overstock's customer purchases."[253] Plaintiff alleged that the placement of the terms of use agreement,

246 No. 09 CV 991(SJ), 2009 WL 2876667, at *3 (E.D.N.Y. Sept. 8, 2009).

247 *Id.* at *1–2.

248 *Id.* at *3 ("In the instant case, it is clear that Plaintiff had no actual notice of the Terms and Conditions of Use.").

249 *Id.* at *1.

250 *Id.* ("After receiving the vacuum, Plaintiff returned it to Defendant and was reimbursed the full amount she had paid for it, minus a $30.00 restocking fee.").

251 *Id.*

252 *Id.*

253 *Id.*

on the bottom of the webpage, did not constitute actual notice of the terms she agreed to by entering the website.[254]

The court essentially agreed, taking particular issue with the way in which Overstock.com presented its terms of use agreement to customers.[255] Referring to decades of case law, the court maintained that a contract required "a 'meeting of the minds' and 'a manifestation of mutual assent.'"[256] The court distinguished clickwrap agreements from browsewrap agreements,[257] providing that "courts consider primarily 'whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site.'"[258] The court then cited several other Second Circuit decisions finding browsewrap agreements non-binding when the user "respond[ed] to an offer that did not carry an immediately visible notice of the existence of license terms or required unambiguous manifestation of assent to those terms."[259]

---

[254] *Id.* ("Plaintiff affirms, however, that she 'never had any notice that disputes with Overstock.com require mandatory arbitration in Salt Lake City, Utah.' Plaintiff affirms that when she accessed Overstock's website to purchase the vacuum, she was never made aware of the Terms and Conditions; specifically, Plaintiff avers that: 'Because of this lawsuit, I later learned that if you scroll down to the end of the website page or pages, there is in smaller print placed between 'privacy policy' and Overstock.com's registered trademark, the words 'site user terms and conditions.' I did not scroll down to the end of the page(s) because it was not necessary to do so, as I was directed each step of the way to click on to a bar to take me to the next step to complete the purchase.'").

[255] *See id.* at *3 ("Hines therefore lacked notice of the Terms and Conditions because the website did not prompt her to review the Terms and Conditions and because the link to the Terms and Conditions was not prominently displayed so as to provide reasonable notice of the Terms and Conditions.").

[256] *Id.* at *2 (citing Express Indus. & Terminal Corp. v. N.Y. Dep't Transp., 715 N.E.2d 1050, 1050 (N.Y. 1999); 1-800 Contacts, Inc. v. Weigner, 127 P.3d 1241, 1242–43 (Utah Ct. App. 2005); R.J. Daum Const. Co. v. Child, 247 P.2d 817, 819–20 (Utah 1952)).

[257] *Id.* ("Unlike a clickwrap agreement, a browsewrap agreement 'does not require the user to manifest assent to the terms and conditions expressly . . . [a] party instead gives his assent simply by using the website.'" (quoting Sw. Airlines Co. v. Boardfirst, L.L.C., No. 06-CV-0891-B, 2007 WL 483761, at *4 (N.D. Tex. Sept. 12, 2007))).

[258] *Id.* (quoting Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 20 (2d Cir. 2002)).

[259] *Id.* at *3 (quoting *Specht*, 306 F.3d at 23); *see also* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 402–03 (2d Cir. 2004) (finding browsewrap agreement enforceable because the user conceded actual notice of the terms of use agreement); Motise v. Am. Online, Inc., 346 F. Supp. 2d 563, 564–65 (S.D.N.Y. 2004) (refusing to find notice where the terms of service were not presented to the plaintiff as an ISP user).

Perhaps most interestingly, the court recognized that "very little is required to form a contract nowadays—but this alone does not suffice," referring to the statement within the terms of use agreement that users would be bound by the terms and conditions of use via their use of the website alone.[260] First, the court distinguished this case from other browsewrap agreements in which the notice that users would be bound by the terms of use agreement merely by using the site was more prominently displayed.[261] The fact that the court admitted that very little was required to form a contract, however, was a backdoor victory for website owners and terms of use agreements.

Taken together, these cases stand for the proposition that courts will look at terms of use agreements across a spectrum of accessibility and look at them potentially more restrictively when privacy concerns are implicated by the plaintiff's claims. On the least-likely-to-be-upheld end of the spectrum are terms of use agreements that are not prominently displayed on the website and which bind users of the website without notice.[262] On the other end of the spectrum are prominently displayed clickwrap agreements that require the user to scroll through the agreement and do not reserve the right to unilaterally alter the agreement.[263] *Harris* is the first decision to declare that an online terms of use clickwrap agreement is unenforceable, and in fact, several decisions from other circuits seem inconsistent with the court's analysis in *Harris*.[264] The court allowed the plaintiff to pursue a claim that required an expansion of its contract doctrine because the injury alleged was an infringement of the plaintiff's privacy rights.[265] Accordingly, the *Harris* decision could breathe life into the widely backed argument in academia for courts and legislatures to expand privacy protection with a modified common law approach.

---

260 *Hines*, 2009 WL 2876667, at *3.

261 *Id.* (citing Hubbert v. Dell Corp., 835 N.E.2d 113, 121–22 (Ill. App. Ct. 2005) (finding sufficient notice where three pages completed by the plaintiff had statements advising users that they would be bound by the use of the site)).

262 *See id.*

263 *See, e.g.*, Harris v. Blockbuster, Inc., 622 F. Supp. 2d 396, 398 (N.D. Tex. 2009).

264 *Id.*; *see supra* note 182 and accompanying text.

265 *Harris*, 622 F. Supp. 2d at 397, 399.

B. Increase Privacy Online by Amending the ECPA

Advocates of increasing Internet privacy protections legislatively argue that the federal government should amend the ECPA or otherwise expand legislation to protect a user's basic expectation of privacy.[266] Pressure on Congress to codify and protect a user's rights to privacy on social networking websites has found widespread support from academic circles and Canada and the European Union,[267] both of which have stronger codified protections for Internet users. Proponents of a legislative overhaul of privacy law in the United States argue that existing legal loopholes and immunities provide protection to only a very select subset of Internet users, which often does not include those who are most vulnerable to infringements of their privacy rights.[268] Ultimately, those on this side of the debate claim that the free market is not an effective safeguard of people's privacy and that it is the government's responsibility to provide a uniform and effective legal framework to both protect the consumer and restrain the company from exploiting outdated assumptions of privacy in the United States.[269]

Recently, there has been an increasing amount of attention paid to the ECPA as a growing number of academics suggest that Congress should use this law as a baseline from which to update privacy protection online.[270] Professor Joel R. Reidenberg has written about the lack of a coherent privacy framework in the United States, calling privacy rights "a fractured and incomplete right in American law"[271] and calling out the "sophistry of U.S.

---

[266] *See, e.g.*, Oyama, *supra* note 92; Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999) [hereinafter Reidenberg, *Restoring Americans' Privacy*].

[267] *See, e.g.*, Carly Brandenburg, *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*, 60 FED. COMM. L.J. 597, 614 (2008) ("The solution to this privacy threat can best be resolved by the courts and the legislature."). For a discussion on Canada and European Union Initiatives on Privacy, see *infra* notes 279–92.

[268] *See* Oyama, *supra* note 92, at 523.

[269] *Id.*

[270] *See, e.g.*, Kerr, *supra* note 108, at 1208; Oyama, *supra* note 92, at 501; Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 879 (2003) [hereinafter Reidenberg, *Privacy Wrongs*].

[271] Reidenberg, *Privacy Wrongs*, *supra* note 270, at 879.

privacy policy."[272] Reidenberg argues that the current patchwork American legislative scheme to protect privacy is insufficient.[273] At issue is the fact that expectations of privacy and privacy rights take various forms and require various degrees of protection against infringement, a point the current legislative framework completely ignores.[274]

For the purposes of this Note, Professor Reidenberg's discussion of "personal or private" wrongs is particularly relevant.[275] Reidenberg argues that there are at least three personal privacy wrongs requiring legislative attention: (1) "intrusive information practices," (2) "misuse of personal information," and (3) "outrageous and noxious data disclosures."[276] Relying on "shifting expectations" and increased public concern for privacy, Reidenberg argues that the time is ripe for the U.S. federal government to address privacy expectations on the Internet and provide legislative avenues for redress of privacy right infringements.[277]

Central to the argument for government intervention on Internet privacy is a lack of faith in the free market's ability to account for the void in formal privacy protections. Despite a tradition of Internet company self-regulation, advocates of increased government in the social networking space argue that without full disclosure of the use, acquisition, and transmission of personal information, the Internet is in the midst of "a classic case of market failure."[278] Echoes of this argument resonate internationally. In the past several years, the European Union and

---

[272] Reidenberg, *Restoring Americans' Privacy*, *supra* note 266, at 773.

[273] *Id.* at 772 ("For years, the United States has relied on narrow, ad hoc legal rights enacted in response to particular scandals involving abusive information practices. The approach has led to incoherence and significant gaps in the protection of citizens' privacy.").

[274] Reidenberg, *Privacy Wrongs*, *supra* note 270, at 878.

[275] *Id.* at 881.

[276] *Id.* at 881–82.

[277] *Id.* at 879; *see* Reidenberg, *Restoring Americans' Privacy*, *supra* note 266, at 771–72 ("During the last few years, an overwhelming majority of Americans report that they have lost control of their personal information and that current laws are not strong enough to protect their privacy.").

[278] Reidenberg, *Restoring Americans' Privacy*, *supra* note 266, at 775.

Canada have tightened privacy laws and are pressuring the United States to do the same.[279]

Notably, in August of 2009, the Canadian government effectively forced Facebook to rewrite its privacy policy to bring it in line with Canadian privacy laws.[280] Following a complaint from the Canadian Internet Policy and Public Interest Clinic, the Privacy Commissioner's Office investigated Facebook's privacy policies and found them lacking in conformity with Canada's primary privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act ("PIPEDA").[281] The PIPEDA governs how private sector organizations collect,[282] use, and disclose personal information while the Privacy Act focuses on government-user data collection on the Internet.[283]

Four issues were of particular concern to the Privacy Commissioner. First, as discussed earlier,[284] control over third party application developers and their access to personal information was severely lacking on Facebook, according to the Privacy Commissioner.[285] Secondly, Facebook was unclear about the difference between deactivating an account, whereupon Facebook continues to hold the user's information in its servers, and deleting an account, where the user effectively erases his or her data from Facebook's servers.[286] Third, the Privacy Commissioner claimed that Facebook did not sufficiently guarantee the privacy of non-users' information, which is posted as

---

279 *See, e.g.*, Press Release, Facebook, Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner (Aug. 27, 2009), *available at* http://www.facebook.com/press/releases.php?p=118816 [hereinafter Facebook, Privacy Improvements].

280 *Id.*

281 *Facebook Agrees to Address Canadian Privacy Commissioner's Concerns*, NET NEWS PUBLISHER, Aug. 27, 2009, http://www.netnewspublisher.com/facebook-agrees-to-address-canadian-privacy-commissioners-concerns/ [hereinafter *Facebook Agrees*].

282 The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000 S.C., ch. 5 (Can.).

283 Privacy Act, R.S.C., ch. P-21 (1985); Office of the Privacy Commissioner of Canada, Mandate and Mission, http://www.priv.gc.ca/aboutUs/mm_e.cfm#contenttop (last visited Apr. 15, 2010).

284 *See supra* notes 111–15 and accompanying text.

285 *See Facebook Agrees*, *supra* note 281.

286 *Id.*

a result of an associate's use of the site.[287] Finally, Facebook was unclear in its privacy policy as to how it would handle the death of a user and how friends could continue to use the user's profile as a memorial.[288] In reaction to the Privacy Commissioner's report, Facebook agreed to rewrite its privacy policy and "retrofit" its site to conform to the Privacy Commissioner's suggestions.[289] Importantly, Facebook's changes affected its site no matter where the user was located.[290] Therefore, Facebook's improvements to its privacy policy, enacted at the behest of the Canadian government, improved the privacy policy for users throughout the world.[291]

The establishment of Canada's Privacy Commissioner Office is part of an international movement intended to strengthen privacy rights for Internet users via government legislation and intervention.[292] In Europe, privacy is a fundamental human right, based on a concept of dignity, beginning with the European Union's Directive on Data Protection of 1995, which required that each country that was part of the European Union pass a national privacy law and create a Data Protection Authority to protect its citizens' privacy.[293] Indeed, as some have suggested, compared to the United States privacy law regime, the European Union's efforts and legislative scheme is an aggressive, comprehensive attempt to both reign in social networking sites' use of their users' personal information and protect the European citizenry.[294]

Comparing the amalgam of federal and state laws that represent the body of United States privacy law with other

---

287 *Id.*

288 *Id.*

289 *Id.*

290 *Id.*

291 *Id.*

292 *See, e.g.*, Wayne Madsen, David L. Sobel, Marc Rotenberg & David Banisar, *Cryptography and Liberty: An International Survey of Encryption Policy*, 16 J. MARSHALL J. COMPUTER & INFO. L. 475 (1998).

293 Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 35 (EC); Sullivan, *supra* note 23.

294 *See* Sullivan, *supra* note 23 (titling one section of the article "piecemeal approach vs. comprehensive law" and expounding upon the differences between U.S. and E.U. privacy law).

international systems does indeed make both European and Canadian efforts appear more substantial and more cohesive.[295] Nonetheless, even advocates of an internationalist approach to United States privacy law admit that assessing the impact of Europe's increased privacy protections is hard to measure.[296] However, that limitation does not tend to deter proponents, such as Marc Rotenberg of the Electronic Privacy Information Center, who call for a similarly encompassing United States privacy regime.[297] The European Union looks at privacy as a "fundamental human right," and has a strict enforcement procedure whereby each country is required to maintain a federal office called the Data Protection Authority to enforce the 1995 directive.[298] Further, the European Union goes to great pains to ensure that all databases are registered and that consumers have the right to periodically review the information collected about them by private actors.[299] Notably, however, the European Union does not have a system set up to ensure citizens equal protection from government infringements, making private data collection and use of that data the European Union's primary focus of concern.[300]

Pointing to divergent court decisions, the promulgation of conflicting state laws dealing with privacy, and pressure from international sources, advocates of a legislative fix to privacy concerns argue for a wholesale accounting and top-down approach to privacy protection law.[301] As social networking sites mine terabytes of personal information concerning their users, advocates

---

295 *See id.*

296 *Id.* ("'How do you assess whether there is a greater privacy protection or not (in Europe) . . . . To what extent do people have rights? It's hard to measure.'" (quoting Daniel J. Solove)).

297 *See, e.g.*, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 [hereinafter Rotenberg, *What Larry Doesn't Get*]; Marc Rotenberg, *Privacy vs. Security? Privacy*, HUFFINGTON POST, Nov. 9, 2007, http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-priva_b_71806.html [hereinafter Rotenberg, *Privacy vs. Security*].

298 Sullivan, *supra* note 23 (comparing, in a chart, how E.U. and U.S. laws differ on privacy protection).

299 *Id.*

300 *See id.*

301 *See supra* notes 268–69 and accompanying text; *see also* Reidenberg, *Restoring Americans' Privacy*, *supra* note 266, at 788.

of a strong federal approach to regulating these entities declare that the current immunities provided to Internet companies are too great to make any of the existing laws effective.[302] The primary source of immunity for Internet hosts is § 230 immunity, which provides operators of an interactive website immunity from liability for content published on their site.[303] Codified at 47 U.S.C. § 230, the immunity provision essentially jettisons all potential claims a user of a social network might have against an operator of the site.[304] Advocates of this approach argue that as social networking websites become more international in nature, the United States should be the guardian of its citizens' data and privacy rights.[305] By lacking a strong infrastructure, the United States is forcing its citizens to seek protection abroad and essentially feeding them to the interests that dominate the legislative process, computer companies with strong lobbies in Washington, D.C.[306]

III. URGING SOCIAL NETWORKS TO REGULATE THEMSELVES

The Internet has a strong tradition of self-regulation and letting consumer preferences correct perceived deficiencies in security.[307] As second generation social networks grow, the extent to which

---

[302] *See, e.g.*, Blumenthal v. Drudge, 992 F. Supp. 44, 52–53 (D.C. Cir. 1998) (immunizing The Drudge Report for comments made by a gossip columnist); Zeran v. Am. Online, 129 F.3d 327, 332 (4th Cir. 1997) (immunizing America Online for a defamatory post by a customer); Paul Festa, *Decision Bolsters Online-Publisher Immunity*, CNET NEWS, June 23, 2004, http://news.cnet.com/Decision-bolsters-online-publisher-immunity/2100-1024_3-5245395.html.

[303] 47 U.S.C. § 230(c)(2) (2006).

[304] *See id. But see* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1165 (9th Cir. 2008) (refusing to immunize Roommates.com from an online posting that violated Federal Housing Authority and state laws).

[305] *See* Reidenberg, *Privacy Wrongs*, *supra* note 270, at 898; Reidenberg, *Restoring Americans' Privacy*, *supra* note 266, at 771–72; *see also* Madsen et al., *supra* note 292; Rotenberg, *Privacy v. Security*, *supra* note 297; Rotenberg, *What Larry Doesn't Get*, *supra* note 297.

[306] *See Facebook Agrees*, *supra* note 281; Facebook, Privacy Improvements, *supra* note 279.

[307] Reidenberg, *Privacy Wrongs*, *supra* note 270, at 877 ("The American legal system has generally rejected legal rights for data privacy and relies instead on market self-regulation and the litigation process to establish norms of appropriate behavior in society.").

companies control and use information should be determined by what their users require and demand. Terms of use agreements require the notice and assent of their users in order to be effective and enforceable. Courts should apply strict notice requirements for terms of use agreements but they should not innovate beyond traditional applications of privacy and contract law. Privacy law has been devised and applied in a somewhat patchwork manner.[308] Rather than a comprehensive legislative approach to remedying consumer privacy concerns, the best course of action to prevent future breaches of privacy would be to foster a flexible market-driven approach, based on the industry's capacity to self-regulate.

Social networking applications that abuse personal information for their own benefit (i.e., Facebook's Beacon Program and RockYou's password security) will fail while those that have a strong reputation for protecting privacy will attract customers and thrive. Social networks that cooperate with each other and encourage self-regulation will benefit by earning a reputation for respecting user privacy. Industry self-regulation does not mean that companies should simply protect the privacy of their own users. Industry self-regulation requires second generation social networking sites (such as YingYang and Blippy), Facebook, and Google, among others, to take steps that actively foster an online environment where users can feel safe and secure by clearly defining their privacy policies, publicizing privacy breaches that occur on other sites, and banning information-sharing with sites that violate generally accepted privacy standards.

Social networks need to take several actions to sufficiently safeguard their users' information. First, privacy policies need to be explicit and understandable to the layperson in order to create a clear and definable legal relationship between the user and the site. There have been sufficient changes within the last several years to standard privacy policies and terms of use agreements to anticipate that second generation social networks will protect PII according to users' expectations.[309] Start-up companies, such as YingYang

[308] *Id.* ("Information privacy is protected through an amalgam of narrowly targeted rules.").

[309] *Compare* YingYang's Privacy Policy, http://www.yingyang.com/privacy/ (last visited Feb. 3, 2010) (easily accessible and clearly articulated), *with* Facebook's Privacy

and Friend Feed, have made their privacy policies easy to read and understand. Bullet points highlighting the most important privacy provisions ensure informed consent by the user. Further, limitations on what the company anticipates doing and is legally allowed to do with the user-supplied PII avoid the overly broad wording previously ruled invalid in *Overstock*.[310]

Second, terms of use agreements need to be not only clearly written, but also need to specify how the social network interacts with APIs. Terms of use agreements defining API use will be increasingly important as social networks begin to distribute and share information as sensitive as real-time locations and credit card purchases. API's, in particular, represent a fundamental challenge to traditional contract models, such as privity of contract and informed consent. APIs, which distribute information across platforms and enable third party application developers to access information on a social network, have their own terms of use agreements, which are most often agreed to as an addendum to the primary network's terms of use agreement. Although complicated, the user should be presented with this terms of use agreement, and agreeing to the API's terms of use should require more notice than is customarily presently.

Third, in the wake of privacy violations, such as RockYou's password debacle,[311] the industry as a whole should respond by isolating the guilty site and ending cooperation with the site until the privacy breach has been remedied. This should be standard industry practice.[312] If a third-party developer is caught spamming or irresponsibly distributing information, all social networks should immediately cut them off, alert their users, and suspend communication with the site until the privacy problem not only has been addressed, but remedied.

One example of a company that has embraced self-regulation successfully is Google. Google has an understanding of its users'

Policy, *supra* note 20 (confusing to a layperson because it is littered with legalese and industry jargon).

310 *See supra* note 246 and accompanying text.

311 *See supra* notes 123–25 and accompanying text.

312 *See* Khare, *supra* note 18.

hopes and needs for transparency of use of their information.[313] First of all, Google anonymizes all of the information it collects about its users, so that in sharing the information across APIs, the information is not traceable to any specific or individual user.[314] Further, in November of 2009, Google launched a "Privacy Dashboard," which contains a list of all of a user's applications and allows the user to set his or her privacy preferences accordingly for each application.[315] By allowing the user to control the flow of information, Google is attempting to assuage the fears of its users and earn the trust of the Internet community.[316] By encrypting and anonymizing the information of its users, Google shields its users from intrusive and invasive use of their PII.

Industry self-regulation has proven remarkably effective in remedying, clarifying and preventing privacy breaches. In February 2010, Google launched Google Buzz, a new social networking tool integrated into its users' email interface.[317] Within one day of the launch, technology-focused blogs identified several features that jeopardized user privacy.[318] Specifically, Google Buzz automatically found followers for users based on their contact lists. These lists were, by default, made public, so other users could find out who their friends were emailing.[319] Theoretically, this feature endangered journalists with confidential sources and businesses with customer lists, as well as any other relationships that were intended to be private.[320] Within four days,

---

313 *See generally* Google Privacy Center, http://www.google.com/privacy.html (last visited Feb. 3, 2010).

314 *Id.*

315 Erick Schonfeld, *Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You*, TECHCRUNCH, Nov. 5, 2009, http://www.techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you.

316 *See id.*

317 Matt McGee, *Liveblogging the Google Buzz Launch*, SEARCH ENGINE LAND, Feb. 9, 2010, http://searchengineland.com/liveblogging-the-google-social-event-35702.

318 *See, e.g.*, Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, BUS. INSIDER, Feb. 10, 2010, http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2; Kashmir Hill, *The Huge Privacy Flaw in Google Buzz (and How to Fix It)*, TRUESLANT, Feb. 10, 2010, http://trueslant.com/KashmirHill/2010/02/10/the-huge-privacy-flaw-in-google-buzz-and-how-to-fix-it.

319 *See* Carlson, *supra* note 318.

320 *See, e.g.*, Robin Wauters, *Google Buzz Privacy Issues Have Real Life Implications*, TECHCRUNCH, Feb. 12, 2010, http://techcrunch.com/2010/02/12/google-buzz-privacy/

Google responded to the online furor by issuing an apology[321] and modifying the problematic features.[322] While critics will point to this situation as a failure of privacy law in America, it would have been nearly impossible to conceptualize and design anticipatory legislation for the innovation behind Google Buzz.

The benefits of relying on self-regulation are consistent with both the Internet's tradition and its future. Second generation social networking start-ups, such as YingYang, Blippy, and Foursquare, grow, benefit, and thrive from the free exchange of information. Collectors and traders of rare sneakers achieve a higher level of satisfaction when they can freely exchange price and availability information via a social network platform. Transparency is perhaps the key benefit of the Internet, and social networking sites enable and achieve a maximum flow of knowledge. People benefit by giving YingYang their information, and YingYang benefits too by increasing advertising revenue. However, the amount and type of information the networks collect and their users divulge is becoming increasingly specialized, requiring a more clear and complete understanding of the extent of control the social network exercises over the information.

As discussed above, in cases such as *Harris*[323] and *Specht*,[324] courts have gone out of their way to provide users who regret giving up control of their personal information with relief. These cases should be read as a common law approach to provide a

?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29.

321 Posting of Todd Jackson to The Official Gmail Blog, *A New Buzz Start-up Experience Based on Your Feedback*, http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html (Feb. 13, 2010, 15:53 PST) ("We've heard your feedback loud and clear, and since we launched Google Buzz four days ago, we've been working around the clock to address the concerns you've raised."); *see also* Thomas Claburn, *Google Sorry About Buzz Privacy*, INFO. WK., Feb. 16, 2010, http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=222900563&subSection=Securityc.

322 Jason Kincaid, *Google Buzz Abandons Auto-Following Amid Privacy Concerns*, TECHCRUNCH, Feb. 13, 2010, http://techcrunch.com/2010/02/13/google-buzz-privacy-update/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29 (noting that Google "isn't wasting any time in responding to user criticism" by modifying Google Buzz features).

323 *See* discussion *supra* Part II.A.2.

324 *See* discussion *supra* Part II.A.1.

remedy for violations of privacy expectations in the absence of a legislative remedy. Advocates of supplying such a legislative remedy ignore the rapid pace of social networking technology development. Facebook is less than six years old and Twitter is less than three years old. It would have been nearly impossible to expect that within a year or two of the iPhone 3G launch,[325] there would be several hundred thousand people making use of location-based social networking applications. It is easier to envision a blanket prohibition on the misuse of personal information by social networks than it would be to implement such a regime. Congress lacks the mechanisms to keep up with the pace of innovation online and the constantly developing methods of information-sharing available to social networks.

Rather than attempting to win an arms race against social networks, Congress should focus on codifying current common law regarding notice requirements of terms of use agreements. Providing a set of uniform procedures would enable greater predictability of the enforceability of terms of use agreements for both users and operators of social networks. The industry should make common sense language standard for terms of use agreements, but this requirement should be instituted organically, not via a law. Legal requirements for terms of use agreements should include posting the site's privacy policy clearly. There should be a requirement that the user scroll through the entire set of terms of use and affirmatively click-through the agreement or be required to type "I understand and I agree." By focusing on the procedures governing the establishment of the user-site operator relationship, Congress can ensure an informed decision-making process, while leaving the substance of the user-operator relationship subject to the terms of use agreement. In defining a baseline set of procedures, Congress can effectively ensure notice for the user of the terms of use, while allowing companies themselves to battle for customers based upon the amount of privacy protection they provide.

---

[325] Brandon Griggs, *iPhone 3Gs Launch Has App Developers Seeing Gold*, CNN.COM, June 19, 2009, http://www.cnn.com/2009/TECH/06/19/iphone.3gs.launch/index.html.

The social networking industry is capable of resolving privacy concerns, but it needs to take certain steps quickly. Second generation social networks need to act aggressively before Congress attempts to limit the kind or amount of information that users are allowed to share via social networks and to mitigate the uneven administration of justice by courts providing ad hoc remedies for vague privacy injuries. The resolution of this debate will have dramatic consequences for the Internet, our domestic economy, and federal courts. We are now in the infancy of social networking, proved by the limited duration of most networks and their accompanying sky-high valuations. The time is ripe for the United States to determine its participation in social networking. Neither a strictly common-law approach nor a comprehensive legislative overhaul of privacy law sufficiently addresses the concerns of social network users. Legislation should focus on fine-tuning the notice requirements of terms of use agreements. Any complete overhaul of privacy law will constantly lag behind the Internet community, and it will force traditional concepts of privacy rights to never completely square with the issues raised by social networking, particularly those that utilize location-based technology or other niche second generation social networks. Instead, the United States should provide a set of strict notice requirements for terms of use agreements, which will strengthen the world of online contracting and enable, rather than hinder, its citizenry the freedom to contract, use, and enjoy social networking.

CONCLUSION

Social networking, the ability for users to connect and share personal information over a privately owned Internet-based platform, raises a number of information privacy rights issues. Terms of use agreements dictate the amount of control users of social networks retain over the personal information they share with a social network. Over the past several years, as social networking has taken a more central role in people's lives, courts and legislatures have been attempting to regulate and remedy the privacy concerns and issues raised by the widespread use of networks such as Facebook and Twitter on their own, without clearly defined limits. While privacy law has never been very

comprehensive in the United States, especially when compared to Europe, recent attempts to govern privacy on social networks have been particularly patchwork and confusing. Social networks need to proactively effectuate industry self-regulation to both avoid user anxiety and overreaching congressional legislation. Rather than attempt to reverse centuries of tradition in the privacy realm, Congress should provide social networks with a set of requirements for their terms of use agreements, including strict notice requirements, and encourage courts to apply these notice requirements rigorously, leaving the extent of ownership of personal information to contractual bargaining between the network and its users.