

The Aesthetics of Online Privacy: Do We Communicate Context Through Interface Design?

J. Richard Stevens, Assistant Professor, University of Colorado at Boulder

Abstract:

Every year more legal codes and policy initiatives concerned with the regulation of consumer privacy are created throughout the world, yet the amount of personal information collected and stored continues to increase. Much of this data comes directly from individuals through small “trivial and incremental” interactions that “minimize its ultimate effect”¹

Privacy attitudes are neither static nor inflexible. When individuals perceive the potential benefits for information transactions outweigh potential risks, they voluntarily adjust their privacy decision-making to meet the demands of changing social contexts. Architecture itself creates social context and influences human behavior.

The current work examines the effect of certain aesthetics in “architectures of vulnerability” that lead individuals to provide personal information in exchange for security, comfort, a sense of belonging and the ability to perform surveillance. Through the communication of communal aesthetics, online storefronts, social networking sites and other online venues create an image of a contextual paradigm that does not conform to the behaviors of the underlying digital architecture.

In this manner, interface design is used to create false social contexts and illusions of voluntariness that cause individuals to disclose more personal information than they normally would.

Introduction

In recent years, the intersection between privacy and new technologies continues to be a critical area of controversy and debate in American political and cultural discussions. Thousands of books related to privacy are released every year. A March 2004 search on Amazon.com for books containing the word “privacy” yielded a results page containing 45,751 items, a repeat search in March 2008 yielded 184,398 books (a more than four-fold increase in as many years). Privacy literature would appear to be growing exponentially.

Privacy has many meanings. For some, privacy is a matter of restricting access to individuals within society.² For others, privacy is about personal autonomy and control of one’s body.³ And within each of these categories exist several sub-groupings of issues. Within the ranks of the access-based privacy advocates some argue for protection of one’s image, others for

¹ Julie E. Cohen, “Examined Lives: Informational Privacy and the Subject as Object,” *Stanford Law Review* 52 (2000), 1397.

² See Michael F. Mayer, *Rights of Privacy* (New York, Law-Arts Publishers, 1972); Edward Bloustein, “Privacy as an Aspect of Human Dignity: an answer to Dean Prosser,” *New York University Law Review* 39 (1964), 962-1007; Roland Garrett, “The Nature of Privacy,” *Philosophy Today* 89 (1974), 421-72; Ruth Gavison, “Privacy and the Limits of the Law,” *Yale Law Journal* 89 (1980), 421-71; William Parent, “Recent Work on the Concept of Privacy,” *American Philosophical Quarterly* 20 (1983), 341-54; Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Oxford and New York: Oxford University Press, 1984); and Anita Allen, *Uneasy Access: Privacy for Women in a Free Society*, (New Jersey: Rowman and Littlefield, 1988).

³ See Charles Fried, “Privacy,” *Yale Law Journal* 77 (1968), 475-493; Jeffrey Reiman, “Privacy, intimacy and Personhood,” *Philosophy and Public Affairs* 6 (1976), 26-44; James Rachels, “Why Privacy is Important,” *Philosophy and Public Affairs* 4 (1975), 232-33; Robert Gerstein, “Intimacy and Privacy,” *Ethics* 89 (1978), 86-91; and Richard Wasserstrom, “Privacy: Some Arguments and Assumptions,” in Richard Bronaugh, ed., *Philosophical Law* (Westport, CT: Greenwood Press, 1978), 148-66.

data protection and still others for the safeguarding of space. Within the ranks of the autonomy-based privacy advocates, some argue for abortion rights, some for medical rights and others for DNA genome protections.

This work is an attempt to demonstrate how interface design is often used to exploit confusion among data consumers about what constitutes privacy, leading many to disclose their valuable data for little, if any, compensation. In order to grasp how privacy norms are manipulated in online environments, it will be necessary to examine what role contextual clues play in the information disclosure decisions of Internet users.

Rosen described privacy in terms of context, as decisions concerning information disclosure depend heavily on the circumstances, audience and perceived implications of the disclosure.⁴ Palen and Dourish argue that privacy in networked contexts is a negotiated process conditioned by the expectations and experiences of the disclosing users.⁵

Dey, Abowd and Salber defined context as

any information that can be used to characterize the situation of entities (i.e., whether a person, place, or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves. Context is typically the location, identity, and state of the people, groups, and computational and physical objects”.⁶

Grudin presented an example of how changes in the context of information dissemination through aggregation of a search engine for a newsgroup called *Deja News* altered the experience of newsgroup readers, as one put it “we were discovering things about our colleagues that we didn’t want to know.”⁷

Privacy attitudes are neither static nor inflexible. When people see that the potential benefits for an information transaction outweigh the potential risks, they voluntarily adjust their privacy comfort levels.⁸ Stutzman surveyed 200 students and found that while students tend to

⁴ Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000).

⁵ Leysia Palen and Paul Dourish, “Unpacking ‘Privacy’ for a Networked World,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 2003), 129-136.

⁶ A.K. Dey, G.D. Abowd and D. Salber. “A Conceptual Framework and a toolkit for Supporting the Rapid Prototyping of Context-aware Applications.” *Human-Computer Interaction*, 16: 2-4 (2001), 106.

⁷ Jonathan Grudin, “Desituating Action: Digital Representation of Context,” *Human Computer Interaction*, 16:2-4 (2001), 269-281.

⁸ Batya Friedman, “Social Judgments and Technological Innovation: Adolescents’ Understanding of Property, Privacy, and Electronic Information,” *Computers in Human Behavior*, 13:3 (1997), 327-351; Robert F. Murphy, “Social Distance and the Veil,” *American Anthropologist* 66 (1964), 1257-1274.

view protecting their identity information online as important and cite concerns about the consequences of sharing information, they do not feel their online identity is well-protected nor do they plan to curb their future disclosure activities.⁹

McMillan and Morrison used qualitative analysis to show that college students increasingly rely on Internet technology in each of four primary domains (self, family, real communities and virtual communities).¹⁰ But the relationships maintained in each of these domains can be quite different, and the information disclosure decisions would hardly be consistent between domains. Context would appear to be rather important to how students manage personal information.

Interface design is defined by Steven Johnson as producing “software that shapes the interaction between user and computer. The interface serves as a kind of translator, mediating between the two parties making one sensible to the other.”¹¹ Manuel Castells describes the back-end of digital architecture as “unseen logic of the meta-network, where value is produced, cultural codes are created and power is decided.”¹² The purpose of this paper is to examine in what ways the back-end and the front-end experiences can communicate different contexts to users and therefore encourage different assumptions about what information disclosures are appropriate.

Privacy is about expectations. From its genesis in American culture, privacy advocates have tried to control the circumstances under which certain facts about themselves could be disclosed. However, a brief review of that genesis will demonstrate that the privacy of the early 20th century causes more confusion than clarification for Americans in the 21st century.

Considering the Roots of American Privacy

During the 1890s, America experienced a period of dramatic social and political development, forging the country into a unified nation. The political stagnation that had followed the Civil War soon began to yield to a new age of commerce, technological innovation and the

⁹ Fred Stutzman, “An Evaluation of Identity-sharing Behavior in Social Network Communities,” *International Digital Media and Arts Association Journal* 3:1 (2006).

¹⁰ Sally J. McMillan and Margaret Morrison, “Coming of Age in the E-Generation: A Qualitative Exploration of How the Internet has Become an Integral Part of Young People’s Lives.” *New Media & Society* 8:1 (2006), 73-95.

¹¹ Steven Johnson, *Interface Culture: How New Technology Transforms the Way We Create and Communicate*, (San Francisco: HarperEdge, 1997), 14.

¹² Manuel Castells, *The Rise of the Network Society*. (Cambridge, Mass.: Blackwell Publishers, 1996), 508.

industrialization.¹³ It is in the midst of the shift from the American Victorian era (sometimes referred to as the Gilded Age) to the progressive era that a need for legal privacy was born.

In particular, the introduction of several key communication technologies changed the way individual Americans thought about themselves and their relationship to society. The telegraph, the telephone, improvements to mass printing processes and the development of snap photography would forever change American cultural boundaries. These innovations would serve to provide a previously unknown degree of access to information by members of society from all ranks and social classes.

Due to of the industrialization of the American economy, a rising middle class was formed as money markets tied together previously unrelated occupations and the professional workplace brought people together despite differences in background. Urban America was populated by communities of strangers, most of whom had been born or raised in other places.¹⁴

As the urbanization trends continued, social status began to be measured not by who one's parents were, but by what clothing one wore and what products one consumed. The resulting increase in the importance of money and consumer expression increased the tensions between classes. As the links of paternalism were broken, the elite class was increasingly seen as separate from the working man. As the distance between social classes increased, the poor began to portray the upper classes as crafty thieves who tried justified their wealth through manipulation and dishonesty.

The growing inequalities between the haves and the have-nots led to rioting over labor and work conditions.¹⁵ The result of these generalized attitudes led to the blending of society into economic classes: no longer were the boundaries for social interaction formed primarily upon the old loyalties to bloodlines or family standing. But increasingly, those of similar economic status began to identify with others with similar means. Within the emerging urban identity of the modern American came the distrust of members of other classes, igniting class warfare. The convergence of so many different groups into increasingly crowded spaces led to an increased level of surveillance between the social castes, and particularly on the part of the lower classes toward the increasingly mistrusted upper classes.

¹³ Robert W. Cherny, *American Politics in the Gilded Age: 1868-1900*. (Wheeling, Ill.: Harlan Davidson, Inc., 1997).

¹⁴ David Nashaw, *Children of the City: At Work and At Play* (New York: Oxford University Press, 1985), 195.

¹⁵ Gunther Barth, *City People: The Rise of Modern City Culture in 19th Century America* (New York: Oxford University Press, 1980), 21.

Forum on Public Policy

As in most societies, the elites of the upper classes generally possessed more economic and political power in early American history than did the lower classes. However, as the urbanization of the late 19th century drove people of similar class values together, two new forces began to redistribute power to the lower classes: the mass appeal of journalism and technological innovation.

Into this environment, one major technological innovation led directly to the establishment of a privacy protection for upper class members: flash photography. With the introduction of flash powder to the process, the exposure time was only limited by the limitations of the mechanical hardware, and photographs could be taken in less than a single second. As a result, “snap shots” let a photographer take photographs without the permission or even without the knowledge of the subject.

The ability of photographs to capture action led to a novel interest in the activities of other people. As newspapers began to run photographs of prominent people in compromising positions, the public’s desire for this style of content increased, and newspapers began to serve the entertainment appetite by emphasizing scandal with renewed vigor.

In 1890, two young lawyers from Boston decided to challenge the photographers’ newly acquired abilities with the law. The construct of American privacy as a legal right first appeared in an 1890 *Harvard Law Review* article written by Samuel D. Warren and Louis D. Brandeis titled, “The Right to Privacy.” This article did not attempt to establish a right of privacy from either a constitutional justification or an argument of privacy’s intrinsic value to all societies. Instead, its argument was that as American society had evolved, a “certain level of sophistication” in society has made it increasingly difficult for a person to retreat from external scrutiny:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual, what Judge Cooley calls the right ‘to be left alone.’ 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 housetops.”¹⁶

Warren and Brandeis cited the development of instant flash photography and numerous other mechanical devices as threats to personal space that required a legal restriction for their use. This

¹⁶ Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy” *Harvard Law Review* 4 (1890), 195.

argument led to their definition of the right to privacy simply as the “right to be left alone,” a reference to Judge Thomas Cooley’s statement concerning “personal immunity”¹⁷ two years earlier. While elegant in its simplicity, this phrase was of little help in the legal arena, as determining to what extent someone should be left alone has varied almost as often as the circumstances under which the right is challenged by a competing right of access.

In essence, Warren and Brandeis formed their argument by stitching together English Common law and existing copyright law to form a right to withhold personal information from publication, which gave them the foundation for a right to privacy.

The authors claimed that a right of privacy is due a person out of respect for his or her standing, and claimed that the unauthorized disclosure of private facts (the only form of violation mentioned in their article) can corrupt a society by encouraging the nation to divert its attention away from important political and economic issues. The article also argued that each person possesses an “inviolable personality,” an abstract collection of images, texts and facts that when assembled, form a person’s identity.

This construct allowed the authors to argue that this “inviolable personality” should be controlled by the possessor, because 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.”¹⁸ In effect, they argued from the precedent of copyright law to make a person the owner of his or her image, with the implied control and disposal rights granted private property.

Eventually, this link between privacy and copyright law also implied that a citizen had the right to sell his or her image as a commodity. “Inviolable personality” is an abstract self made up of images, texts and facts, the collection of which can be sold as a commodity. In essence, Warren and Brandeis seem to have been arguing that people have copyright rights to themselves, which allowed the person to have their potential marketability of their “inviolable personality” damaged or “assaulted” (and thus in need of protection under tort law) when someone exposed them to public scrutiny without permission. Thus, this abstract self soon became a commodity in its own right.

¹⁷ Thomas McIntyre Cooley, *A Treatise on the Law of Torts*. 2 (Chicago: Callaghan & Co., 1888), 29.

¹⁸ Warren and Brandeis, 198.

Forum on Public Policy

For Warren and Brandeis, this protection of the abstract self was based on their desire to provide a response mechanism for upper class individuals trying to protect the sanctity of their family names and reputations. As technology increasingly empowered the lower classes in democratic fashion, the upper classes turned to law to reinforce the existing social boundaries. Brook Thomas framed “The Right to Privacy” as a representation of “elitist, bourgeois ideology”¹⁹ and Dean Prosser called it an attempt by the Boston elite to make law out of failing social custom.²⁰

In other words, Warren and Brandeis had front row seats for the cultural changes America experienced in the transition between the Victorian era, when social pressure and self-restraint governed behavior, and the progressive era, when law began to become an increasingly utilized control.

Because this right is not constitutionally supported, the right of privacy was first defined under tort law, and the cases that it is applied to have been exclusively cases of defending the privacy of one person or group against another person or group of persons. Tort law can vary from state to state and only advances as individual cases are brought before the U.S. Supreme Court for judgment.

Though the foundation of the privacy tort was effectively created in 1890, it was not until the 1960s that it became a useful tool, when legal scholar William Prosser argued that the previous privacy cases could be categorized into four distinct torts: intrusion, private facts, false light and appropriation. These distinctions made it easier for a citizen to bring civil suit against another, and made the legal discourse surrounding privacy easier to navigate. Despite this contribution, it is difficult to overemphasize how influential Warren and Brandeis’ article, born of class conflict, shaped the way Americans today think about privacy, publicity and intellectual property. Thousands (if not millions) of articles and books about access-based privacy have been written in the ensuing years, and many different frameworks and arguments have been presented in response to new technological challenges (and it is beyond the scope of this work to present an organized taxonomy). However, inherent in most access-based privacy arguments is the foundational argument that people have a right to preserve their reputation and that the public disclosure of private facts is the root concern of privacy law.

¹⁹ Brook Thomas, “The Construction of Privacy in and Around The Bostonians,” *American Literature*, 64:4 (December 1992), 723.

²⁰ William L. Prosser, “Privacy,” *California Law Review* 48 (1960), 403.

This foundation, born in an environment of class warfare and analog technology, does not always clearly translate to the contemporary challenges presented by the introduction of digital technologies and platforms, making the application of privacy law to questions of data usage somewhat problematic.

Considering Contemporary Privacy Trends

America has changed much since the early 20th Century. As the beginning of that century saw the conclusion of the transition from agrarian economy to industrial economy, the beginning of the 21st century saw America struggling with the transition from an industrial society to an information economy.

In 1962, Fritz Machlup measured information production, becoming one of the first to see information and knowledge as an economic resource.²¹ These observations led to discussions about the coming “Information society” and how business would change.

Society also changed. After the end of World War II, the decline in family size and the decreasing age of independence led to the creation of a greater number of single dwellings. This increase in privacy led to a greater need for surveillance for the purposes of social control. As the embedded familial networks began to lose their influence, reputations ceased to be an effective measure of a person’s trustworthiness, and Americans began to measure trust by requiring credentials and data about individuals.²² Rather than the strength of one’s standing in a community of known connections, trustworthiness began to be measured by degrees, credit scores and government records.

In this environment, the importance of data management was born. Gandy persuasively argued that access to one’s data places allows individuals to be categorized by others in ways in which few would be comfortable.²³ Because these categories can be used to predict market behavior, consumer information has become a commodity in the information economy.

Much of the recent privacy research has focused on invasions of secret spaces in the forms of surveillance cameras, telemarketing calls and identity theft. These topics sell books

²¹ Fritz Machlup, *The Production and Distribution of Knowledge in the United States* (Princeton, N.J.: Princeton University Press, 1962).

²² Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*. (New York: A. De Gruyter, 1993).

²³ Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*. (Boulder, Colo.: Westview, 1993).

because of their sensational nature, but ignore many of the structural changes occurring in society that make personal data vulnerable.

Information is routinely collected through networks for modification and analysis.²⁴ Modern Americans leave data trails with almost every interaction in which we engage: secrecy simply is not possible in a world in which credit cards, cell phones, biometric cameras and even toll roads are all used to track the movements of individuals.²⁵

It is increasingly difficult for most of us to know what information is being collected, what it is being connected to, and who has access to it. When one considers the number of privacy disclosure agreements one signs in a given year (just a few common examples: medical disclosure forms, mortgage agreements, software agreements, credit card agreements, online bank access agreements, loans, cable and television service, etc.), it quickly becomes apparent that little about our behavior is not known by someone.

Americans are not wholly ignorant of these issues, but seem ill equipped to act in meaningful ways to protect their data. A recent study conducted by Jupiter Research revealed that while 70 percent of U.S. consumers worry that their privacy is at risk, they report doing little to protect their data.²⁶ Of particular interest, the study found that only 40 percent of those polled read privacy statements before handing over personal information to Web sites (and only 30 percent of online consumers find Web site privacy statements easy to understand).

It is within interactions such as these that individuals and corporations establish surveillance. Lyon demonstrated how modern surveillance works through solicitations and seductions, encouraging individuals to “trigger” own inclusion in systems of surveillance.²⁷

Leathern argued that consumers should learn how to manage their data in ways that allowed them to capitalize on its exchange and get value from its use.²⁸

“Data” is the plural form of “datum,” which means “something given.” If data is a commodity in the information economy, why are so many giving away their inherent value for so little in return?

²⁴ Castells, 32.

²⁵ Colin Bennett, Charles Raab and Priscilla Regan “People and Place: Patterns of Individual Identification within Intelligent Transportation Systems,” in David Lyon (Ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London: Routledge, 2003), 153-175.

²⁶ Robert Leathern, “Online Privacy: Managing Complexity to Realize Marketing Benefits.” *Jupiter Research*, 17 May 2002.

²⁷ David Lyon, *The Electronic Eye: The Rise of Surveillance Society*. (Cambridge, UK: Polity Press, 1994), 52.

²⁸ Leathern.

One of the chief causes of the disparity between attitudes of concern and seemingly irresponsible behavior is the influence of online interface design. By seeming to create a particular aesthetic of intimacy, information architects can encourage individuals to disclose data in ways they might not choose were the implications of the actual network context in which they operated within were disclosed in a meaningful way.

Interface as Social Control

Interface design can be a form of social control. Wood defines social control as the “the use of power with the intention of influencing the behavior of others.”²⁹ Berndt argued that social control covered “all the processes and procedures which regulate behavior, in that they exert pressure on persons and groups to conform to the norms.”³⁰ When describing media exposure, Mathiesen described social control as exerted by “disciplining our consciousness.”³¹

In physical space, architecture creates psychological and social effects³² including changing individual conduct.³³ In the classical example of contextually driven attitudes, a sense of crowdedness can depend on intentionality and environment, such as whether one is at a rock concert or ball room dancing.³⁴ Architecture frames intentions by connecting schema with opportunities for action, though not always consciously. Benjamin explained that architecture is experienced habitually and in a state of distraction, but nonetheless perceived.³⁵

It is not a stretch to imagine the effects digital architecture can have on online behavior. After all, Mok wrote that “[i]nformation design makes information understandable by giving it a context. Information design builds new relationships between thoughts and places.”³⁶

In order to use the World-Wide Web, almost every user must participate in the consensual hallucination: users believe they “visit” sites when in fact they are having online content delivered to their computer. The context of Web surfing in that metaphor is not the setting of one’s computer, but rather the setting on the screen.

²⁹ Arthur L. Wood, *Deviant Behavior and Control Strategies*. (Lexington, MA: D.C Health, 1974), 53.

³⁰ Ronald M. Berndt, *Excess and Restraint* (Chicago: University of Chicago Press, 1962), 11.

³¹ Thomas Mathiesen, “The Viewer Society: Michel Foucault’s ‘Panopticon’ Revisited.” *Theoretical Criminology* 1:2 (1997), 215–234.

³² Yi-fu Tuan, *Space and Place: The Perspective of Experience* (Minneapolis: University of Minnesota Press, 1977).

³³ Neil Katyal, “Architecture as Crime Control,” *Yale Law Journal* 111 (2002), 1039-1139.

³⁴ Tuan, 61.

³⁵ Walter Benjamin, “The Work of Art in the Age of Mechanical Reproduction,” *Illuminations: Essays and Reflections* (New York: Schochen Books, 1969), 217-252.

³⁶ Clement Mok, *Designing Business*. (San Jose: Adobe Press, 1996), 46.

Humans interface with the people and institutions of the world through the mental schema they develop. We constantly filter stimuli (tuning out noise, ignoring visuals) by directing attention towards specific elements. Too much sensory input can cause stress and inhibit functionality.³⁷

To some degree, we all interpret the world through mental representation. Gibson described this interpretation as the reading of affordances, the practice of interpreting the world as an offering of possible actions, communicated through structural design.³⁸ According to Gibson, one's perception is influenced by environment, embodiment and perceived possible action.

Taking these perspectives into consideration, it becomes apparent that changes in context don't necessarily control actions so much as shape schema by directing attention towards particular features or visual cues. Contextual cues can cause cognition to be directed in a particular way, which can either encourage or discourage certain patterns behavior. Users are often not aware of the differences between interface design and back-end architecture. As Raskin observes, "As far as the customer is concerned, the interface is the product."³⁹

In his treatise on the aggregation of personal data through online databases, Solove explained that current practices create "architectures of vulnerability,"⁴⁰ insecure structures that create opportunities for significant harm. Such architectures encourage individuals to expose themselves to those who have greater access to online structures and thus more power. Currently, most of those who collect personal data do so out of the user's view. Most users do not know when their information is gathered, where it is stored or how it is used. Furthermore, most companies that gather information are often not accountable to consumers.

How companies utilize user data and how consumers react on the rare occasions they witness such use can be illustrated by tracking several recent controversies surrounding the social networking platform *Facebook*.

³⁷ John Seely Brown and Mark Weisner. "The Coming Age of Calm Technology," *Beyond Calculation: The Next Fifty Years* (New York: Copernicus, 1997), 75-85.

³⁸ J.J. Gibson, *The Ecological Approach to Visual Perception*. (Boston: Houghton Mifflin, 1979).

³⁹ Jef Raskin, *The Human Interface: New Directions For Designing Interactive Systems* (Reading: Addison Wesley, 2000), 5.

⁴⁰ Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004), 99.

Considering *Facebook*

Facebook is an online social networking platform used primarily by university students to coordinate offline social relationships as well as learn more about the members of their community. Like most social networking sites, *Facebook* allows its users to frame and present their identities in the form of authored profiles. These profiles are then linked together as members add “friends” to their network, write messages to each other, join topical groups, share images and post content to weblogs and online bulletin boards. Users typically spend about 20 minutes each day on the site and two-thirds of users log in at least once per day.⁴¹

Facebook was introduced in early 2004 by Mark Zuckerberg, a Harvard University student. A month later, the site expanded to 10 other schools. By June of 2004, Zuckerberg left school to run the site full-time.⁴²

A series of controversies involving the use and access to member data have demonstrated to users the potential for abuse when disclosing personal data online. These controversies, while frustrating for many involved, actually shed light on the abilities of many firms dealing in personal information who choose not to disclose their privacy practices.

In September 2006, *Facebook* members awoke to find their social network filtered through an aggregating tool that reported the latest actions of members to a member’s personal network. Immediately, tens of thousands of users voiced their anger over the changes, claiming that the aggregation of information was invasive.⁴³ How members reacted to this change in the environment provides insight into how users perceive access and privacy within their social networks.

Facebook responded by posting a blog entry by Zuckerberg, explaining that none of the information portrayed in the feeds was unavailable before the aggregation. “Nothing you do is being broadcast; rather, it is being shared with people who care about what you do – your friends.”⁴⁴

A survey of 180 undergraduate students conducted by the author soon after the controversy erupted reported that while more than 90% of respondents considered online data

⁴¹ John Cassidy “Me media,” *New Yorker* 15 May 2006, 50-59.

⁴² Kevin Alexander, “Fast times at make-believe high,” *Boston Magazine*, 4 February 2007, http://www.bostonmagazine.com/articles/fast_times_at_make_believe_high.

⁴³ Michael Calore, “Privacy fears shock Facebook,” *Wired*, 6 September 2006, <http://www.wired.com/news/culture/0,71739-0.html>

⁴⁴ Mark Zuckerberg, “Calm down. Breathe. We hear you.” *Facebook Blog*, 5 September 2006, <http://blog.facebook.com/blog.php?post=2208197130>.

management to be important and more than 2/3 did not agree that *Facebook* protected their personal data, only one student reported leaving *Facebook* because of privacy concerns, and even that one reported logging in via a friend's account to keep up with the content of her friend's pages.⁴⁵

Another controversy erupted in November 2007, when *Facebook* launched Beacon, an aggregating advertisement utility that published users' activities on partner Web sites like *eBay*, *Fandango*, *Travelocity*, *Overstock* and *Blockbuster*.⁴⁶ In protest, more than 50,000 *Facebook* users signed an online protest organized by *MoveOn.org*.⁴⁷

Finally, in February of 2008 a controversy erupted when many users discovered that should they ever decide to delete their *Facebook* account, their information would continue to be a permanent part of the network.⁴⁸ An analysis of the site's policy agreement suggested that its use of data was legal in the U.S., though not in the European Union.⁴⁹

In each of these controversies, users expressed surprise and outrage at how their data was distributed to other users. Though they had personally supplied the data, the general lack of understanding of underlying database structures displayed by the more vocal critics indicated many users do not understand the implications of the distribution of data across networked environments.

What sets *Facebook* apart from the millions of online venues that collect personal data is not its information collection techniques. Presumably, most sites that collect data are equally capable of combining together information strings and the contextual threads that connect them together. What makes *Facebook* controversial is the transparency with which it operates. By allowing users to see their data reconfigured and redistributed into multiple contexts, the site causes distress by demonstrating information aggregation techniques that have been enacted behind a veil of technology for years.

⁴⁵ J. Richard Stevens, "Facing Change: The Role of Context and Privacy Expectations in Facebook Disclosure Decisions." Paper presented at the midwinter meeting for the Association for Education in Journalism and Mass Communication, February 23-24, 2007, in Reno, NV.

⁴⁶ Louise Story, "The Evolution of Facebook's Beacon." *The New York Times BITS blog*. 29 November 2007, <http://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/>.

⁴⁷ Louise Story and Brad Stone, "Facebook Retreats on Online Tracking." *The New York Times BITS blog*. 30 November 2007, <http://www.nytimes.com/2007/11/30/technology/30face.html>.

⁴⁸ Maria Aspan, "How Sticky Is Membership on Facebook? Just Try Breaking Free." *The New York Times*. 11 February 11, 2008, <http://www.nytimes.com/2008/02/11/technology/11facebook.html>.

⁴⁹ Anita Ramasastry, "On Facebook Forever? Why the Networking Site was Right to Change its Deletion Policies, And Why Its Current Policies Still Pose Privacy Risks." *FindLaw.com*. 29 February 2008, <http://writ.news.findlaw.com/ramasastry/20080229.html>.

Facebook appears to offer one set of expectations (drawn from the interface aesthetic) for its users, while the output of the collected data demonstrates a radically different relationship between the user and the architecture. In most data transactions, users are not privy to the output of their data collection.

The ignorance displayed by *Facebook* users is particularly disturbing considering that each of the controversies in question were specifically addressed within the official privacy policies of the site (the site emails users when significant changes to the policies are enacted or when changes to core services are introduced).

When registering, every user is required to confirm that he or she has read and understands the policies of the site (including the privacy policies, which in its most recent incarnation is 3,730 words in length) before being granted access to the site. However, users are only required to check a box declaring they've read the policies, a common step in technology installation that few users appear to actually follow.

Privacy Presentation Through Interface Design

The design of a technical interface is implicitly political. Green (2001) explains that technological manifestations are symbols of “socially bound knowledge,” a phrase that she uses to illustrate how each manifestation represents a particular perspective of how a society believes a technology should be created and how its utility should be determined.⁵⁰

Because of the aesthetics used to construct most sites that collect personal information, most users have little or no awareness about how their data is treated within online databases. Many interfaces do not make the access provided between software and personal information explicit.

Privacy decisions depend heavily upon perceived context, and yet it appears that many (if not most) users have not developed a sense of spatial literacy necessary to make responsible decisions regarding their personal data. The interface that unlocks our ability to use digital technology keeps us from seeing what the technology actually is:

Put simply, the importance of interface design revolves around this apparent paradox: we live in a society that is increasingly shaped by events in cyberspace, and yet cyberspace remains, for all practical purposes, invisible, outside our perceptual grasp. Our only access to this parallel universe of zeros and ones runs through the conduit of the

⁵⁰ Lelia Green, *Communication, Technology and Society* (London: Sage, 2001), 6.

computer interface, which means that the most dynamic and innovative region of the modern world reveals itself through the anonymous middlemen of interface design.⁵¹

Understanding the context of interaction as a sense of place instead of a tool set is important. Dourish pointed out that where we are located (or perceive we are located) determines what is considered appropriate, rather than the tool. One example he presented was the different behavior people engage in with a cell phone, depending on the setting of its use.⁵²

Online site aesthetics also create a sense of environment: how one drafts and email to a bank representative will likely be different than the text comprising a message to friends. Dourish used Suchman's attempt to use ethnomethodology⁵³ to bring a sociological understanding of interaction, ultimately arguing that "interaction is intimately connected with the settings in which it occurs."⁵⁴

Dourish encapsulated this view in his term embodiment, which recognized that:

[t]he technical infrastructures that deliver information into our homes and work environments create barriers that separate one stream of information from another and make coordination difficult. Humans respect barriers, too, but they are barriers of different sorts; boundaries between public and private, between home and work, between personal time and the company's time, and so forth. These barriers are more or less flexible, subject to negotiation and adapted to the needs of the moment. However, they map poorly to the kinds of barriers that technological systems put into place.⁵⁵

Dourish's embodiment is about the establishment of meaning by considering the "place" of interaction⁵⁶ and in particular by examining the interpretations of interface presentation.⁵⁷

What an action within a given interface represents to users is heavily influenced by the aesthetic used by the designer of the interface. Hutchins et al. identify the "gulf of interpretation" as the difficulty of interpreting the system's state as a response to the user's command.⁵⁸ Dourish

⁵¹ Johnson, 19.

⁵² Paul Dourish, *Where the Action Is: The Foundations of Embodied Interaction* (Cambridge: MIT Press, 2001).

⁵³ Harold Garfinkel, *Studies in Ethnomethodology*. (Cambridge: Polity Press, 1967).

⁵⁴ Lucy Suchman, *Plans and Situated Actions: The Problem of Human-Machine Communication* (Cambridge: Cambridge University Press, 1987), 19.

⁵⁵ Dourish, 2001, 197.

⁵⁶ Steve Harrison and Paul Dourish, "Re-Place-ing Space: The Roles of Space and Place in Collaborative Systems," *Proceedings of ACM Conference on Computer-Supported Cooperative Work* (New York: Association for Computing Machinery, 1996), 67-76.

⁵⁷ Paul Dourish and Graham Button, "On Technomethodology: Foundational Relationships between Ethnomethodology and System Design." *Human-Computer Interaction*, 13:4 (1998), 395-432.

⁵⁸ Edwin L. Hutchins, James D. Hollan, and Donald A. Norman, "Direct Manipulation Interfaces." In Donald A. Norman and Steven W. Draper (Eds.), *User Centered System Design: New Perspectives on Human-Computer*

illustrated particular concerns about network security, as computers negotiate heterogeneous network protocols in the name of seamless access (and its corresponding aesthetic), which makes a user's knowledge about the particular security protocols at any given moment impossible, since the networking decisions are made at the architecture level, hidden from the user's view.⁵⁹

Analysis and Conclusions

Ishii and Ulmer have argued that Americans live in two worlds: the world of computation ("bits") and the world of physical reality ("atoms").⁶⁰ Recognizing both as part of a user's context, the designers of information collection interfaces bear a responsibility for communicating the implications of computation in terms of the effect of the physical reality. Whereas computer interactions have largely been described in the past in terms of objects (computers themselves), computing decisions now consist of a myriad of situations, all represented by aesthetics that imply context.

For most users, privacy is still considered in ways Warren and Brandeis defined in 1890 and Goffman articulated in 1959⁶¹: the manipulation of image in public space. Though that rendition of privacy is well protected by laws originating from the invasion of the mechanical technology in the beginning of the industrial age, the legal code protecting one's reputation do little to protect one's data or prepare users to make educated decisions regarding their data in response to the introduction of digital technologies in the present age.

Warren and Brandeis struggled to control the public display of images, but the challenges facing most consumer of information is the obscure display of personal data between unknown data brokers. Thus, agents trade credential "gossip" about users that does not defame anyone's public reputation, but nonetheless has no less real consequences for matters of authentication, trust and access.

Regulations pertaining to data practices do exist. The *Code of Fair Information Practices* is one such example, based on five noteworthy principles:

Interaction (Hillsdale, NJ: Erlbaum, 1985), 87-124.

⁵⁹ Paul Dourish, "What We Talk About When We Talk About Context," *Personal and Ubiquitous Computing*, 8:1 (2004), 19.

⁶⁰ Hiroshi Ishii and Brygg Ullmer, "Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms," *Proceedings of ACM Conference on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 1997), 234-241.

⁶¹ Goffman Erving, *The Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959).

Forum on Public Policy

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.⁶²

And yet, most users of the Internet report fears about data security but take no action to protect or account for how their data is being used. Because consumers do have legal protections, most sites create carefully worded disclosure statements about the use of data, but then present such disclosures in a way that makes it unlikely that a consumer will engage the disclosure statement in any meaningful way, hiding behind the aesthetic of intimacy that implies a context unrepresentative of the network structure of most tools.

The surveillance of user data will continue to be a growing part of computer and network interactions. For many, surveillance is seen as a negative side effect, apparently not seeming intrusive enough to make us give up new technology services. But are front-end aesthetics reflective of back-end structures? If privacy is something to be surrendered for greater ease of use and access, are we presented with an articulate representation of what we're being asked to give up?

Trust between individuals in our society continues to decline.⁶³ We are increasingly likely to interact with strangers without the information needed to assess reputation,⁶⁴ primarily because we are part of large impersonal communities with highly mobile populations.⁶⁵ As a

⁶² "Records, Computers, and the Rights of Citizens," *U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems* 8 (1973).

⁶³ Pamela Paxton, "Trust in Decline?" *Contexts* 4:1 (2005), 40-46.

⁶⁴ Carol A. Heimer, "Solving the Problem of Trust." In Karen S. Cook (ed). *Trust in Society* (New York: Russell Sage Foundation, 2001), 40-89.

⁶⁵ Nock, 11-12.

result, the core assumptions of American privacy law, forged during the Industrial Revolution during a time of intensive class warfare does little to protect one's personal data from being collected, transmitted, stored and transferred between credentialing agencies.

As such, it would appear that the protection of a citizen's data is not enforceable until the core assumptions about what data means, what its value is and how those assumptions can be communicated to consumers are updated to take into consideration the digital information revolution. While more time and consideration should be devoted to the arena in which such changes should be made (law, culture, technology platforms, etc.), this work will conclude by offering the following recommendations:

- 1. Personal data should be considered the intellectual property of individuals rather than a component of one's right to privacy.** Setting aside the struggle to define privacy as a distinct right with a coherent and definable history, privacy laws and conventions would appear to empower corporations and governmental institutions to collect, store, transmit and even sell a person's person data without violating commonly understood privacy conventions because such activity occurs outside the public's view. Because reputation (the original "inviolable personality") is no longer the essential authenticating agent for social capital, the laws and conventions that specifically protect one's reputation are ill equipped to protect one from damage to one's credential dossier. Though such damage would not be known to one's neighbors, poor credentialing scores can limit both one's mobility and social capital within a society. One's data has inherent value to the individual. Like the reputations of Warren and Brandeis' day, credentials require investment and the expenditure of effort to ensure one's place in society is secure or advances. The legal definition of "inviolable personality" should be expanded to include one's data, with the recognition that data is often disclosed in a way that challenges the 20th Century notion of "public disclosure."
- 2. Policies, laws and conventions of protection must consider collection activities within the context of the communicated interfaces, not merely the underlying architecture.** Historically, computer interactions have been discussed in terms of machine operations without consideration for interface aesthetics. Aesthetics communicate implied values and expectations to the user, and the degree to which the implied expectations of use conflict with

actual architectural performance represents the degree of exploitation of users (particularly inexperienced users) by the corporation or governmental institution engaging in the data collection activities. Perhaps this bridge can be built by examining the differences between advertising and promotional constraints in regards to contractual obligations as a construct for examining the disparities between the interface and architecture of an information collection construct.

3. **While the *Code of Fair Information Practices* would theoretically seem to offer protections for a person's data, the burden placed upon the user is too onerous for most average computer users.** The gulf of interpretation is simply too vast for many users to understand what consequences their actions entail. Examination of the way in which personal information brokers conform to both the letter and the spirit of the code is a necessary area for future study. Currently, simplistic checkbox interactions are presented as representative of informed consent requirement for information disclosure. Future study should examine whether the spirit and letter of the laws invoking informed consent statutes are met by such interactions.

4. **Consumers of digital communication products and services appear to lack an understanding of how information architectures work and one avenue for improvement might entail educational initiatives.** Citizens in most countries are licensed before they can operate technology (such as firearms, motorized vehicles or heavy equipment) that could bring potential harm to themselves, others or society in general. Perhaps voluntary or even forced educational programs about the nature and dangers of online information brokerage would be a first step to raising awareness about these issues. Perhaps one should acquire an "information license" before being allowed to navigate the "information superhighway."

Though much is written about the Internet in the popular and scholarly press, users, developers, scholars and governing agencies should be reminded on a consistent basis that the Internet and its protocols are still quite young. At this stage in its development, online communication would seem to be more misunderstood than understood by most who use it, and those misunderstandings are leading to the emergence of new challenges and problems for our society.

Forum on Public Policy

Using technology always requires trade-offs from those who use them. Even for a society that endures rapid changes (or perhaps especially those societies), learning new ways of interacting with others and utilizing newly available resources is a disconcerting proposition for the most flexible among us and potentially incomprehensible for those with more rigid expectations of social capital and appropriate action.

Reference List

- Alexander, Kevin. 2007. "Fast times at make-believe high." *Boston Magazine*. February 4.
http://www.bostonmagazine.com/articles/fast_times_at_make_believe_high.
- Allen, Anita. 1988. *Uneasy Access: Privacy for Women in a Free Society* New Jersey: Rowman and Littlefield.
- Aspan, Maria. 2008. "How Sticky Is Membership on Facebook? Just Try Breaking Free." *The New York Times*. February 11. <http://www.nytimes.com/2008/02/11/technology/11facebook.html>.
- Benjamin, Walter. 1969. "The Work of Art in the Age of Mechanical Reproduction." *Illuminations: Essays and Reflections*. New York: Schochen Books: 217-252.
- Barth, Gunther. 1980. *City People: The Rise of Modern City Culture in 19th Century America*. New York: Oxford University Press.
- Bennett, Colin, Charles Raab and Priscilla Regan. 2003. "People and Place: Patterns of Individual Identification within Intelligent Transportation Systems," in David Lyon (Ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge: 153-175.
- Berndt, Ronald M. 1962. *Excess and Restraint*. Chicago: University of Chicago Press.
- Bloustein, Edward. 1964. "Privacy as an Aspect of Human Dignity: an answer to Dean Prosser." *New York University Law Review* 39: 962-1007.
- Bok, Sissela. 1984. *Secrets: On the Ethics of Concealment and Revelation* Oxford and New York: Oxford University Press.
- Brown, John Seely, and Mark Weisner. 1997. "The Coming Age of Calm Technology," *Beyond Calculation: The Next Fifty Years*. New York: Copernicus: 75 - 85.
- Calore, Michael. 2006. "Privacy fears shock Facebook." *Wired*. September 6.
<http://www.wired.com/news/culture/0,71739-0.html>
- Cassidy, John. 2006. "Me media," *New Yorker* 82(13): 50-59.
- Castells, Manuel, *The Rise of the Network Society*. (Cambridge, Mass.: Blackwell Publishers, 1996).
- Cherny, Robert W. 1997. *American Politics in the Guilded Age: 1868-1900*. Wheeling, Ill.: Harlan Davidson, Inc.
- Cohen, Julie E. 2000. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52: 1373-1437.
- Cooley, Thomas McIntyre. 1888. *A Treatise on the Law of Torts*. 2 Chicago: Callaghan & Co.

Forum on Public Policy

- Dey, A.K., G.D. Abowd and D. Salber. 2001. "A Conceptual Framework and a toolkit for Supporting the Rapid Prototyping of Context-aware Applications." *Human-Computer Interaction*, 16 (2-4): 97-166.
- Dourish, Paul. 2004. "What We Talk About When We Talk About Context," *Personal and Ubiquitous Computing*, 8(1): 19-30.
- Dourish, Paul. 2001. *Where the Action Is: The Foundations of Embodied Interaction*. Cambridge: MIT Press.
- Dourish, Paul, and Graham Button. 1998. "On Technomethodology: Foundational Relationships between Ethnomethodology and System Design." *Human-Computer Interaction*, 13(4): 395-432.
- Fried, Charles. 1968. "Privacy" *Yale Law Journal* 77: 475-493.
- Friedman, Batya. (1997). Social Judgments and Technological Innovation: Adolescents' Understanding of Property, Privacy, and Electronic Information. *Computers in Human Behavior*, 13 (3): 327-351.
- Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo.: Westview.
- Garfinkel, Harold. 1967. *Studies in Ethnomethodology*. Cambridge: Polity Press.
- Garrett, Roland. 1974. "The Nature of Privacy," *Philosophy Today* 89: 421-72.
- Gavison, Ruth. 1980. "Privacy and the Limits of the Law," *Yale Law Journal* 89: 421-71.
- Gerstein, Robert (1978). "Intimacy and Privacy," *Ethics* 89: 86-91.
- Gibson, J.J., 1979. *The Ecological Approach to Visual Perception*. Boston: Houghton Mifflin.
- Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.
- Green, Lelia. 2001. *Communication, Technology and Society*. London: Sage.
- Grudin, Jonathan. 1990. "The Computer Reaches Out: The Historical Continuity of Interface Design," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Empowering People*: 141-144. New York: Association for Computing Machinery.
- Grudin, Jonathan. 2001. Desituating Action: Digital Representation of Context. *Human Computer Interaction*, 16 (2-4): 269-286.
- Harrison, Steve and Paul Dourish. 1996. "Re-Place-ing Space: The Roles of Space and Place in Collaborative Systems." *Proceedings of ACM Conference on Computer-Supported Cooperative Work*: 67-76. New York: Association for Computing Machinery.
- Heimer, Carol A. 2001. "Solving the Problem of Trust." In Karen S. Cook (ed). *Trust in Society*. New York: Russell Sage Foundation: 40-89.
- Hutchins, Edwin L., Hollan, James D., and Norman, Donald A. 1985. "Direct Manipulation Interfaces." In Donald A. Norman and Steven W. Draper (Eds.), *User Centered System Design: New Perspectives on Human-Computer Interaction*: 87-124. Hillsdale, NJ: Erlbaum.
- Ishii, Hiroshi, and Brygg Ullmer. 1997. "Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms," *Proceedings of ACM Conference on Human Factors in Computing Systems*: 234-241. New York: Association for Computing Machinery.
- Johnson, Steven. 1997. *Interface Culture: How New Technology Transforms the Way We Create and Communicate*. San Francisco: HarperEdge.

Forum on Public Policy

- Katyal, Neil. 2002. "Architecture as Crime Control," *Yale Law Journal* 111: 1039-1139.
- Leathern, Robert. 2002. "Online Privacy: Managing Complexity to Realize Marketing Benefits." *Jupiter Research*, May 17.
- Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Cambridge, UK: Polity Press.
- Mathiesen, Thomas. 1997. "The Viewer Society: Michel Foucault's 'Panopticon' Revisited." *Theoretical Criminology* 1(2): 215-234.
- Mayer Michael F. 1972. *Rights of Privacy* New York, Law-Arts Publishers.
- Mok, Clement. 1996. *Designing Business*. San Jose: Adobe Press.
- Murphy, Robert F. (1964). Social Distance and the Veil. *American Anthropologist* 66: 1257-1274.
- Machlup, Fritz. 1962. *The Production and Distribution of Knowledge in the United States*. Princeton, N.J.: Princeton University Press.
- McMillan, Sally J. and Margaret Morrison. 2006. "Coming of Age in the E-Generation: A Qualitative Exploration of How the Internet has Become an Integral Part of Young People's Lives." *New Media & Society* 8(1): 73-95.
- Nashaw, David. 1985. *Children of the City: At Work and At Play*. New York: Oxford University Press.
- Nock, Steven L. 1993. *The Costs of Privacy: Surveillance and Reputation in America*. New York: A. De Gruyter.
- Palen, Leysia, and Paul Dourish. 2003. "Unpacking 'Privacy' for a Networked World." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: 129-136. New York: Association for Computing Machinery.
- Parent, William. 1983. "Recent Work on the Concept of Privacy," *American Philosophical Quarterly* 20: 341-54.
- Paxton, Pamela. 2005. "Trust in Decline?" *Contexts*. 4(1): 40-46.
- Prosser, William L. 1960. "Privacy." *California Law Review* 48: 338-423.
- Rachels, James. 1975. "Why Privacy is Important," *Philosophy and Public Affairs* 4: 232-33.
- Ramasastry, Anita. 2008. "On Facebook Forever? Why the Networking Site was Right to Change its Deletion Policies, And Why Its Current Policies Still Pose Privacy Risks." *FindLaw.com*. February 29. <http://writ.news.findlaw.com/ramasastry/20080229.html>.
- Raskin, Jef. 2000. *The Human Interface: New Directions For Designing Interactive Systems*. Reading: Addison Wesley.
- Reiman, Jeffrey. 1976. "Privacy, intimacy and Personhood," *Philosophy and Public Affairs* 6: 26-44.
- Rosen, Jeffrey. 2000. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.
- Stevens, J. Richard. 2007. "Facing Change: The Role of Context and Privacy Expectations in Facebook Disclosure Decisions." Paper presented at the midwinter meeting for the Association for Education in Journalism and Mass Communication, February 23-24, 2007, in Reno, NV.

Forum on Public Policy

- Story, Louise. 2007. "The Evolution of Facebook's Beacon." *The New York Times BITS blog*. November 29. <http://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/>.
- Story, Louise and Brad Stone. 2007. "Facebook Retreats on Online Tracking." *The New York Times BITS blog*. November 30. <http://www.nytimes.com/2007/11/30/technology/30face.html>.
- Stutzman, Fred. 2006. "An Evaluation of Identity-sharing Behavior in Social Network Communities." *International Digital Media and Arts Association Journal* 3(1).
- Suchman, Lucy. 1987. *Plans and Situated Actions: The Problem of Human-Machine Communication*. Cambridge: Cambridge University Press.
- Solove, Daniel J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
- Thomas, Brook. 1992. "The Construction of Privacy in and Around The Bostonians," *American Literature*, 64:4 (December), 719-747.
- Tuan, Yi-fu. 1977. *Space and Place: The Perspective of Experience*. Minneapolis: University of Minnesota Press.
- "Records, Computers, and the Rights of Citizens." 1973. *U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems* 8.
- Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy" *Harvard Law Review* 4: 193-220.
- Wasserstrom, Richard. 1978. "Privacy: Some Arguments and Assumptions," in Richard Bronaugh, ed., *Philosophical Law* Westport, CT: Greenwood Press: 148-66.
- Wood, Arthur L. 1974. *Deviant Behavior and Control Strategies*. Lexington, MA: D.C Health.
- Zuckerberg, Mark. 2006. "Calm down. Breathe. We hear you." *Facebook Blog*. Sept. 5. <http://blog.facebook.com/blog.php?post=2208197130>

Published by the Forum on Public Policy

Copyright © The Forum on Public Policy. All Rights Reserved. 2008.