EDITORIAL PRELUDE

JEFF LANGENDERFER AND ANTHONY D. MIYAZAKI

Privacy in the Information Economy

Although early notions of privacy focused on freedom from intrusion, modern privacy concerns are primarily directed toward control of personal information. Understanding of privacy-related decisions and consequences, or "privacy literacy," is an important antecedent to effective information control. A perspective of historical and modern privacy concepts provides directions for future research.

Privacy! It's difficult to escape a discussion of the topic. From bloggers to newspaper and magazine articles to television news and entertainment programming, discussions of privacy are ubiquitous. A Google search of the term "privacy" generates 1.8 billion hits (as of June 15, 2009) and an ABI/Inform Global search returns more than 7,000 articles with "privacy" in the title. Clearly, privacy is something that people of 2009 are concerned about. There is also nearly universal agreement that (1) we have less privacy than we used to, and (2) this is bad.

Privacy concern is not a new phenomenon, although the nature of the concern has changed over time. The founders of the United States were so concerned about privacy that privacy protection elements are embedded throughout the Bill of Rights. The First Amendment guarantees of religious freedom speak to concerns about the private right to practice religious beliefs as well as the right to be free from governmental impositions of religious practice that intrude into private decision making. The Third Amendment prohibition against quartering soldiers in private residences protects the sanctity of the home from governmental invasion—fundamentally, a privacy protection measure. The Fifth Amendment right against self-incrimination protects the privacy of individually held information, even against the interests of the state in enforcing criminal statutes. Finally, the Fourth Amendment

Jeff Langenderfer (jefflang@meredith.edu) is an associate professor of marketing & law in the School of Business at Meredith College. Anthony Miyazaki (miyazaki@fiu.edu) is Knight Ridder Research Professor and an associate professor of marketing in the College of Business Administration at Florida International University.

The Journal of Consumer Affairs, Vol. 43, No. 3, 2009
ISSN 0022-0078

"right of the people to be secure in their persons, houses, papers, and effects from unreasonable searches and seizures" is an explicit affirmation of privacy as a fundamental right.

Privacy, especially the right to be free from governmental intrusion into one's home, was clearly of great importance in the late 1700s and remains so today. Yet, the nature of privacy as a constitutionally based right has grown throughout U.S. history, particularly through Supreme Court interpretation.

Notwithstanding the fact that the word "privacy" is not in the Constitution, a fundamental right to privacy has been repeatedly enunciated based on constitutional provisions. In *Meyer v. Nebraska*,[1] the Court found a law prohibiting foreign language instruction prior to successful completion of the eighth grade repugnant to the fundamental right to life, liberty, and property as embodied in the Fourteenth Amendment. In *Griswold v. Connecticut*, the Court held that the guarantees of the Bill of Rights "create zones of privacy," including the right of doctors to educate their patients concerning contraception and prescribe contraceptives devices. The privacy rights associated with the marital relationship is so fundamental, the Court wrote, that it is "older than the Bill of Rights—older than our political parties, older than our school system."[2] In *Stanley v. Georgia*, the Court held that private possession of obscene material cannot be constitutionally prohibited and a Georgia statute criminalizing such possession violated the "personal liberties guaranteed by the First and Fourteenth Amendments."[3] More recently, in *Lawrence v. Texas*, the Court invalidated a law banning certain sexual contact between persons of the same gender. In striking down the statute, the Court explained that the "right to liberty under the Due Process Clause gives [adults] the full right to engage in their conduct without intervention of the government."[4] "It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter."[5]

From these constitutional amendments and court interpretations, it seems apparent that the right to be free from governmental intrusion is fundamental and protected. But this important aspect of privacy is but one dimension of a potentially expansive concept. Modern notions of privacy include not only the right to be left alone but also a person's right to control information about him or her. Indeed, most recent privacy

1. *Meyer v. Nebraska* (1923), 262 U.S. 390.
2. *Griswold v. Connecticut* (1965), 381 U.S. 479, statement on page 486.
3. *Stanley v. Georgia* (1969), 394 U.S. 557, stated on page 565.
4. *Lawrence v. Texas* (2003), 539 U.S. 558, statement on page 578.
5. *Lawrence* 2003, 578 quoting *Planned Parenthood v. Casey* 1992, 847.

discussions focus upon information control rather than intrusion, as the nature of the privacy debate has shifted over time.

Relatively early in the computer age, it became apparent to U.S. lawmakers that the ability to assemble vast amounts of electronic information implicated privacy rights. The Privacy Act of 1974[6] controls the use of information held in federal government records by restricting disclosure of personally identifiable data, granting individuals the right to access information about them held in governmental records, allowing individuals the opportunity to amend federal records upon a demonstration of inaccuracy, and requiring federal agencies to adhere to particular standards of record keeping and maintenance.[7] The Act was later amended to establish standards when federal agencies exchange computer records through matching programs under the Computer Matching and Privacy Protection Act.[8]

Although these statutes accomplished a great deal to ensure the fairness of governmental record keeping within the United States, federal regulation of private information practices is uneven at best and applies only to certain kinds of records. Educational,[9] medical,[10] and credit data[11] are all subject to specific legislative provisions as are video rental records,[12] but for many areas of record keeping in private hands, federal regulation is minimal or absent.

Largely free from federal control are such potentially sensitive areas as purchases histories for consumer products, web surfing history, employment records, and many types of insurance data. Even financial records, some of the most sensitive of any kind of privately held personal information, is only minimally federally regulated, with financial institutions required to provide consumers with opt-out options from information sharing among unaffiliated companies. In other words, it is possible, if a person takes the affirmative step, to prevent a financial institution from selling a customer's bank balance, loan payment history, and debt level to other interested companies willing to buy the data.[13] But few customers take actually opt out, most don't even read the privacy notices (Winkler 2001), and many have little knowledge regarding the privacy regulations affecting various types of firms (Turow, Hennessy and

6. 93 P.L. 579.
7. 5 U.S.C. § 552a.
8. 100 P. L. 503 1988.
9. Family Educational Rights and Privacy Act 1974 (93 P. L. 380).
10. Health Insurance Portability and Accountability Act 1996 (104 P. L. 191).
11. Fair Credit Reporting Act 1970 (91 P. L. 508).
12. Video Privacy Protection Act 1988 (100 P. L. 618).
13. Gramm-Leach-Bliley Financial Services Modernization Act 1999 (106 P. L. 102).

Bleakley 2008). The onus is on the customers to control data sharing—the institution owns the data, not the customer—and information flow is largely unimpeded.

The consequence of this regulatory void is that as private data collection has grown—commensurate with the development of inexpensive computing power—concern about the privacy implications of nongovernmental data sharing has grown also. A May 20, 2009 ABI/Inform Global search for "privacy" in the title of a scholarly journal articles published since January 1, 2003 reveals 568 papers. Of these, virtually all of them deal with the threat to privacy posed by private data collection or the mechanics of information safeguarding. One hundred fifty-eight articles focused on computer security, 108 on electronic commerce, 144 dealt with governmental privacy regulation, 46 focused on medical data, 23 on privacy in the workplace, and 11 on identity theft. Only 32 dealt in any way with consumer responses to the current commercial data explosion, and of those, all but 10 were devoted to online privacy. In a world that relies largely on consumers to manage their own privacy, privacy concern has evolved from a fear of intrusion to a generalized unease regarding the power that comes from easily accessible, personally identifiable data, with each area of sensitive information the subject of separate scrutiny.

To be sure, intrusion has not disappeared completely from the radar of privacy advocates, particularly in the wake of heightened governmental security practices put into place following the events of September 11, 2001. But the lion's share of the attention is surely on information gathering and exchange and the felt intrusion that comes with the knowledge that anyone can easily discover a great deal about anyone else, from their desktop, with a modicum of skill, at little or no cost.

Against this backdrop of shifting privacy attention comes this special issue on privacy literacy. Because federal lawmakers have adopted, in the main, a hands-off approach with respect to private data collection and exchange, it has become increasingly incumbent upon individuals to take an active role in the ways they safeguard their own personal information. Privacy literacy is the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape. It is an area that demands understanding in a climate where the responsibility for privacy rests largely in the hands of the consuming public, and lack of literacy may have important implications.

A series of articles focusing on privacy literacy highlight the Fall 2009 issue of the *Journal of Consumer Affairs*. Youn writes insightfully

and eloquently about student privacy concerns and their coping behavior (Youn 2009). Podar, Mosteller, and Ellen (2009) explore, through a series of depth interviews, the ways in which consumers protect themselves online. Using a more quantitative approach, Milne, Labrecque and Cromer (2009) also examine privacy protection practices in risky environments. And Stanaland, Lwin and Leong (2009) detail the responses that web sites make to different regulatory environments. To finish the special issue, an intuitive article by Norberg, Horne and Horne (2009) calls for the inclusion of the self in the privacy debate, an alert that may help set the agenda for the privacy debates to come.

But to where from here? Though state legislators and, in some cases, state courts have periodically stepped into the regulatory void, the state of information control remains an uneven regulatory patchwork (Langenderfer and Cook 2001).

The debate has changed from government invasion to private information sharing, with intrusion and loss of privacy experienced not from police entering the sanctity of the home, but from corporate entities compiling long and accurate dossiers regarding virtually every aspect of our existence. Indeed, it seems that, given the ubiquity of private data sharing and the importance of the accuracy of many data centers, we are increasingly defined by the information that databases store about us. For celebrities, being defined by others may seem normal. For most citizens who have yet to experience their 15 minutes of fame, self-definition would seem to be an inalienable right.

As databases play an increasingly important role in our lives, there is a danger that we will lose the ability to define ourselves, having surrendered the definition of ourselves to the data gathering entities, often unregulated and beyond our control. Imagine the frustration of the frequent traveler, erroneously added to the terror watch list because his or her name is similar to some unknown and unrelated criminal fanatic. It is easy to understand the anger of the loan applicant, denied a mortgage due to erroneous credit data, whose repayment history has never been blemished. Under such conditions, rather than define the data about us, we are defined by it. And when this occurs, we run the risk of surrendering ourselves to the databases that house the histories of our lives, accurate or not.

PRIVACY'S FUTURE

The next steps in privacy regulation, privacy practices, privacy self-protection, and even privacy-related attitudes, will depend greatly on

the scope and direction of research conducted over the next five to ten years—a time period that will witness an even greater consumer reliance on the electronic connectivity that is often the very means to privacy invasion. In the 1990s, consumer privacy issues moved to the forefront of consumer affairs and public policy research. According to Google Scholar, ISI Journal Citation Reports, and the Social Science Citation Abstracts, the most cited article of the past 40 years in *Journal of Consumer Affairs* by Miyazaki and Ferndandez (2001) examines consumer privacy (James and Cude 2009). Similarly, according to the American Marketing Association's web site, the top five most-cited articles this decade for the *Journal of Public Policy & Marketing* all deal with privacy issues.

Unfortunately, although much has been accomplished over the past 20 years in terms of privacy research, there yet remains a void of research in areas that will undoubtedly spur both new attempts at legislation and legal challenges to the existing regulatory environment. Some of these areas involve online access to government database information, the use of public and private video surveillance, children's privacy protection, and how consumers view the value of privacy as a commodity to be exchanged.

Information collected and stored by various government entities has long been available in various forms, but the online provision of information has made such availability more rapid, less costly, and more far-reaching. Government-controlled information that was once only available by visiting a local government clerk during operating hours can now be accessed around the world at any time of day. By providing unfettered electronic access to its various data sets, the government effectively allows privacy invasion of its key constituency—the people (Belanger and Hiller 2006).

As consumers find more of their information available to marketers, other governments, and other consumers, consumer attitudes toward feelings of control over privacy and accompanying desire for privacy must be examined. Third-party organizations that purport to assure consumer privacy by issuing "seals of approval" (LaRose and Rifon 2007; Miyazaki and Krishnamurthy 2002; Rifon, LaRose and Choi 2005) may find a renewed purpose in monitoring government agencies in addition to commercial enterprises. Nevertheless, research is needed to understand the legal implications of such widespread availability of government-controlled information and how it affects consumer views of government, privacy and security.

In some cities, the rapidly growing network of public and private surveillance cameras has created a public environment in which people are almost continuously recorded when they are outside of their homes. Even satellite images and still photographs of street-level mapping have prompted consumer outrage and accompanying legal responses (Kirk 2009). A number of recent concerns regarding potential and actual abuses of surveillance systems have spurred legislators to take a more cautious approach to the expansion of such systems (Biale 2008; EPIC 2009). However, even though recent academic work has considered the ethical and legal aspects of video surveillance in both public (Lai 2007) and private (Minuk 2006), no one has examined active consumer response to such privacy intrusions. As video surveillance and accompanying biometric identification programs become more popular, research is needed to understand their impact on marketer usage of such technologies and the resultant consumer behavior.

Children's privacy is another issue that likely will continue to drive attempts at new privacy legislation, particularly in the online arena. Early academic research examining online privacy disclosures was based on guidelines arising from the Children's Online Privacy Protection Act (COPPA) of 1998 and the accompanying Federal Trade Commission's "Children's Online Privacy Protection Rule" (e.g., Miyazaki and Fernandez 2000). However, both COPPA and the FTC rule have been widely criticized for both offering limited protection to children and the lack of meaningful enforcement standards (Lwin, Stanaland, and Miyazaki 2008; Miyazaki 2008). Although recent research has begun to examine how education, parental mediation styles, and regulation can work in tandem to protect children's privacy online (e.g., Lwin, Stanaland, and Miyazaki 2008; Miyazaki, Stanaland, and Lwin 2009; Youn 2008), there are ample opportunities to explore children's understanding, attitudes, and responses to privacy invasions and potential regulatory environments wherein children's privacy is sufficiently protected. In particular, much more should be examined with respect to how children understand and react to privacy warnings and disclosures that are meant to protect them from online disclosure of information, how parenting styles interact with disclosures in various situational environments, and how usage of and exposure to popular social networking websites are affecting children's attitudes toward and desire for privacy.

Finally, as the burden of privacy protection shifts more and more onto consumers (Nehf 2007), they are increasingly becoming accustomed to the concept of paying (in time, money, and/or effort) to protect their privacy. More and more consumers understand that their privacy is for

sale in the form of trading information for discounts and special offers as with buyer loyalty programs. Yet, more intrusive attacks on privacy are being put forth in a manner that will prevent consumers from enjoying the prices they currently pay unless they are willing to forego their privacy in various forms.

For example, automobile insurers have recently begun to offer some of their lowest priced policies only to drivers who are willing to install a monitor that would record distance traveled, speed, and even driving habits (Diel 2008). Other, more sophisticated devices are presently installed in many new cars that also monitor acceleration, braking, and seatbelt usage (Benton 2006). Thus, to claim the lower fees once accorded to drivers based on less intrusive methods, many consumers will presumably pay now with their privacy. Research is needed to examine these more explicit exchanges of privacy for benefits and whether such exchanges become more palatable for consumers as attitudes toward privacy and the ability to protect privacy change.

Overall, while the basic concepts of privacy have remained fairly constant over the years (e.g., see Westin 1967), there have been many changes in how privacy can be invaded, protected, and perceived. Privacy literacy is an essential element in a consumer's arsenal of protective devices, although much needs to be done to establish sufficient knowledge so that legislators, judges, consumers, and business people can work toward a balance of privacy protection and information disclosure that is agreeable to all involved.

REFERENCES

Belanger, France and Janine S. Hiller. 2006. A Framework for e-Government: Privacy Implications. *Business Process Management Journal*, 12 (1): 48–60.

Benton, Joe. 2006. States Consider Black Box Laws. *ConsumerAffairs.Com.* http://www.consumeraffairs.com/news04/2006/02/black_boxes_states.html.

Biale, Noam. 2008. Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found. *American Civil Liberties Union*. http://www.aclu.org/privacy/35775res20080625.html.

Diel, Stan. 2008. State's Drivers Can Monitor Driving Habits with 'Black Box' for Insurance Rates. *The Birmingham News.* http://www.al.com/news/birminghamnews. (August 13).

EPIC. 2009. Video Surveillance. http://www.epic.org/privacy/surveillance.

James, Russell N., III and Brenda J. Cude. 2009. Trends in *Journal of Consumer Affairs* Feature Articles: 1967–2007. *Journal of Consumer Affairs*, 43 (Spring): 155–169.

Kirk, Jeremy. 2009. Google Street View Hits Privacy Gridlock in Germany: Germany Wants Partially Blurred Images Removed from Google Databases. Computerworld. http://www.computerworld.com/action/article.do?command=viewArticleBasic & articleId=9133309. (May 20).

Lai, Derek. 2007. Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter. *Alberta Law Review*, 45 (1): 43–77.

Langenderfer, Jeff and Don Lloyd Cook. 2001. Copyright Policies and Issues Raised by A & M Records v. Napster: 'The Shot Heard 'Round the World' or 'Not With a Bang, But a Whimper? *Journal of Public Policy & Marketing*, 20 (Fall): 280–288.

LaRose, Robert and Nora J. Rifon. 2007. Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, 41 (Spring): 127–149.

Lwin, May O., Andrea J.S. Stanaland, and Anthony D. Miyazaki. 2008. Protecting Children's Privacy Online: How Parental Mediation Strategies Affect Website Safeguard Effectiveness. *Journal of Retailing*, 84 (June): 205–217.

Milne, George R., Lauren I. Labrecque, and Cory Cromer. 2009. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43 (Fall): 449–473.

Minuk, Lisa. 2006. Why Privacy Still Matters: The Case Against Prophylactic Video Surveillance in For-Profit Long-Term Care Homes. *Queen's Law Journal*, 32 (Fall): 224–277.

Miyazaki, Anthony D. 2008. Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, 27 (Spring): 19–33.

Miyazaki, Anthony D. and Ana Fernandez. 2000. Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing*, 19 (Spring): 54–61.

Miyazaki, Anthony D. and Ana Fernandez. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, 35 (Spring): 27–44.

Miyazaki, Anthony D. and Sandeep Krishnamurthy. 2002. Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36 (Summer): 28–49.

Miyazaki, Anthony D., Andrea J.S. Stanaland, and May O. Lwin. 2009. Self-Regulatory Safeguards and the Online Privacy of Preteen Children: Implications for Advertisers. *Journal of Advertising*, 38 (Winter), in press.

Nehf, James P. 2007. Shopping for Privacy on the Internet. *Journal of Consumer Affairs*, 41 (Winter): 351–365.

Norberg, Patricia A., David A. Horne, and Daniel R. Horne. 2009. Standing in the Footprint: Including the Self in the Privacy Debate and Policy Development. *Journal of Consumer Affairs*, 43 (Fall): 495–515.

Poddar, Amit, Jill Mosteller, and Pam Scholder Ellen. 2009. Consumers' Rules of Engagement in Online Information Exchanges. *Journal of Consumer Affairs*, 43 (Fall): 419–448.

Rifon, Nora, Robert LaRose, and Sejung Marina Choi. 2005. Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *Journal of Consumer Affairs*, 39 (Winter): 339–362.

Stanaland, Andrea J.S., May O. Lwin, and Susanna Leong. 2009. Providing Parents with Online Privacy Information: Approaches in the US and the UK. *Journal of Consumer Affairs*, 43 (Fall): 474–494.

Turow, Joseph, Michael Hennessy, and Amy Bleakley. 2008. Consumers' Understanding of Privacy Rules in the Marketplace. *Journal of Consumer Affairs*, 42 (Fall): 411–424.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Winkler, Stacey. 2001. Privacy: A Modern Challenge. City of Cambridge, MA Consumer's Council, http://www.ci.cambridge.ma.us/čonsumer/Privacy1.html.

Youn, Seounmi. 2008. Parental Influence and Teens' Attitudes Toward Online Privacy Protection. *Journal of Consumer Affairs*, 42 (Fall): 362–388.

Youn, Seounmi. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*, 43 (Fall): 389–418.