Journal of the Association for Information Systems (2019) **20**(6), 848-856
doi: 10.17705/1jais.00554

EDITORIAL

ISSN 1536-9323

Policy to Avoid a Privacy Disaster

Mary J. Culnan[1]
[1]Bentley University, USA, mculnan@bentley.edu

Abstract

This paper argues that in the current data-rich environment, organizations need formal policies for privacy as a way to avoid "privacy disasters". Privacy disasters can occur when a company uses consumer data in a way that is legal, but violates public norms for acceptable use. The paper uses a case study to illustrate the elements that often characterize privacy disasters, and describes the principles and processes that can serve as the basis of a privacy policy capable of helping organizations avoid these negative events. The paper also highlights the implications of big data for privacy policy.

Keywords: Privacy, Data Governance, Policy.

John L. King was the accepting senior editor. This editorial was accepted on May 15, 2019.

1 Introduction

Today, data are an important asset because new and existing devices, platforms, and sensors generate data at an exponential rate. To remain competitive in this environment, DalleMule and Davenport (2017) argue firms need a coherent data strategy that makes appropriate trade-offs between offense and defense. Offense involves supporting business objectives using tools such as predictive analytics, while defense involves minimizing risks related to data use. In the same way, organizations have risk policies for financial and other valuable assets, defense requires that they also have policies to govern the risks associated with data use, including privacy (Markus, 2000).

Companies suffer privacy disasters when they use consumer data in ways that are legal and believed to provide business advantage, but are perceived by the public as violating expectations for acceptable use. Privacy disasters can result in negative publicity, reputational damage, loss of consumer trust, and possible legal action. The purpose of this paper is to argue the importance of having a formal privacy policy as a means to manage risks related to data use and avoid privacy disasters.

Within information systems (IS) and elsewhere, privacy is often equated with data security. Here, the focus is on data *use*. Security is about protecting personal data, while privacy is broader and encompasses permissions and acceptable use of data *as well as* protecting data from unauthorized access. Privacy cannot exist without security. However, organizations can successfully secure personal data in their custody and still make bad decisions about how they use the data.

While published accounts of privacy disasters may all seem to differ from one another because they involve different business models, different technologies, or different uses of information, this paper will argue that despite this perception, privacy disasters share

common elements. A comprehensive privacy policy that includes both systems development and data use can be the basis for end-to-end governance programs needed to avoid privacy disasters. To illustrate this point, we now turn to a historical example: Lotus Marketplace: Households. Some might wonder why we use such an old example. The case illustrates that privacy disasters reflect a management failure independent of technology, and calls into question why so many organizations still leave themselves exposed.

2 The Case of Lotus Marketplace: Households[1]

In 1990, Lotus Development announced a new application for Apple computers: Lotus Marketplace: Households. Marketplace turned out to be a spectacular early example of a privacy disaster. While it occurred before the Web and today's social media, it nonetheless had some of the hallmarks of many current privacy disasters and, as a result, provides lessons that are still relevant today, independent of the particular technology involved. The elements of the case included:

- *A large company*. Lotus Development was a large, prominent technology company. Founded in 1982, it developed and marketed business software and CD ROM databases. Its first product, Lotus 123, was a widely-adopted spreadsheet application. Lotus was purchased by IBM in 1995.
- *A new technology platform*. Here, the platform was the CD-ROM. Lotus was interested in being a first-mover for developing CD-ROM applications.
- *A controversial application involving personal information*. Marketplace was a mailing list for business-to-consumer marketing. The rationale for the product was to help small businesses use direct marketing to target prospective customers by using the database to identify prospects who met certain criteria.[2]
- *A data broker*. Data brokers or information resellers are businesses that acquire personal information about consumers from a variety of sources and sell that information to other organizations. Here, the data broker was Equifax, one of the three largest credit bureaus, which supplied the names and addresses as well as other data that could be used for targeting from its Consumer Marketing Database. The names and addresses in this database originated from the individual's credit report.
- *"Social Media"* to mobilize the public about the incident. In the early 1990s, this consisted of Internet mailing lists and discussion groups. Here, the RISKS Digest, a moderated forum published since 1985 by the ACM, was the basis for disseminating news and provided a platform for organizing opposition to Marketplace for the technology community.

Lotus Marketplace was announced in a direct marketing trade publication based on a Lotus press release. The article stated that Marketplace was designed for small businesses, a market underserved by the mailing list industry. As a result, Marketplace was expected to have a major impact on the current list industry. At the time, companies rented lists of prospects from list brokers who controlled access to the lists they managed. Subsequent use of a list was managed by seeding where the broker added "fake" names to the list so it could monitor whether or not use complied with the terms of the list rental. With Marketplace, control over the data was in the hands of the end user. Updated CD-ROMs were issued quarterly.

Several steps were taken to protect the data in Marketplace from misuse. The data on the CD-ROM were encrypted and compressed so the record for a particular individual could not be accessed; only names and addresses could be printed or accessed by the user. Marketplace could be ordered from retailers who sold computer software; however, it was not available for purchase by individuals, only businesses. Consumers could have their names removed from the database by writing Equifax or Lotus, or calling a toll-free number. Further, Marketplace users were expected to comply with the Direct Marketing Association's voluntary ethical guidelines. Equifax was aware of potential privacy issues with Marketplace. They did a privacy audit and conducted consumer focus groups.

The privacy disaster began to unfold in fall 1990. A privacy advocacy organization hosted a demo of Marketplace and invited a *Wall Street Journal* reporter to attend. The reporter subsequently published an article with the headline: "Lotus Product Spurs Fears about Privacy" (Wilkie, 1990).

Subsequently, the *Wall Street Journal* article and comments were posted on the *RISKS Digest* and these were widely recirculated on other networks. [3] In addition, an individual distributed the email address for Lotus CEO Jim Manzi, resulting in a flood of

[1] For the full case, see Culnan and Smith (1995).

[2] There was also a version of Marketplace: Business for B2B marketing, but since it did not contain personal information on consumers, it did not raise any privacy issues. Here all references to Marketplace are to the consumer version.

[3] See: *RISKS Digest*, *10*(61), 1990. Available at http://catless.ncl.ac.uk/Risks/10/61#subj2.

emails from angry Lotus customers. Approximately 30,000 people asked to opt out of the database. In the midst of the controversy, Equifax identified two key issues that needed to be addressed: (1) Was Marketplace a proper use of credit report data? and (2) How could an inexpensive opt out be developed? With mainframe-based mailing lists, opt-outs could be processed in real time. With a CD ROM, there was no way to remove a name from a prior version of Marketplace once the CD was in the hands of a user.

Finally, in January 1991, prior to actual the release of the product, Lotus and Equifax made a joint decision to cancel Marketplace: Households. Two factors were cited in the decision. First, they could not ignore the volume, tenor, or response from consumers, Lotus customers, or other important groups. Second, they could not address the substantial, unexpected additional costs necessary to address the privacy concerns.

3 Policy Can Help Avoid Privacy Disasters

Policy is a system of principles used to guide decisions toward desired outcomes in a wide range of settings. Policy differs from rules or law in that policy merely guides actions toward managerial or administrative mechanisms that can achieve particular goals (King & Kraemer, 2019). Privacy policy has two basic elements. First, organizations need principles to govern their information practices. Second, they need a process to ensure compliance with the principles as operationalized.

The principles of a privacy policy should reflect fair information practices (FIPs). FIPs are global norms that make personal information use fair for individuals and, if followed, minimize the risk to organizations of collecting and using personal data (Bruening & Culnan, 2016). The FIPs are based on principles which are both timeless and technology neutral. Since the 1970s, FIPs have served as the basis for privacy laws and self-regulatory programs around the world. At the heart of the FIPs is the principle of transparency, meaning there should be no secret systems. In the US, transparency has been primarily operationalized by posting a privacy notice.

The AICPAs generally accepted privacy principles (GAPP) represents a current version of the FIPs.[4] The GAPP consist of ten principles:

- *Notice:* The organization provides notices of the purposes for which personal information is collected, used and retained.
- *Choice and consent:* The organization describes the choices available to the individual related to how their personal information is used and disclosed. The organization obtains implicit or explicit consent regard to collection, use, and disclosure of personal information.
- *Collection:* Personal information is only collected for the purposes identified in the notice.
- *Use, retention and disposal:* Use of personal information is limited to the purposes described in the notice and is retained only for as long as needed to fulfill the purpose, or as required by law.
- *Access:* The organization provides individuals with access to their personal information for review or update.
- *Disclosure to third parties:* Personal information is disclosed to third parties only for the identified purposes and with the implicit or explicit consent of the individual.
- *Security for privacy:* Personal information is protected against unauthorized access.
- *Quality:* Personal information that is necessary for the purposes identified is maintained as complete, accurate and relevant.
- *Management:* the organization defines, documents, communicates and assigns accountability for its privacy policies and procedures.
- *Monitoring and enforcement:* The organization monitors compliance with its privacy policies and procedures and has procedures in place to address privacy-related complaints and disputes.

The process component of the privacy policy is needed to ensure that the organization implements and complies with the policy and can demonstrate its compliance. Currently, there is an emerging consensus that the process should be a risk-management program based on accountability principles. The specifics should reflect the data the organization collects, its business model, and the risks its data practices pose for individuals. There are nine accountability principles[5]:

[4] See https://www.cippguide.org/20100701/generally-accepted-privacy-principles-gapp/. "Notice" is the first principle of the original FIPs. In the GAPP, "management" is the first principle but for the purposes of this discussion, "notice" is discussed first as part of the policy rules while "management" is discussed as part of the policy process.

[5] See http://informationaccountability.org/wp-content/uploads/CIPL_Accountability_Phase_II_Paris_Projec

- *Policies:* Binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations, and industry standards.
- *Executive oversight:* Oversight and responsibility for data privacy and protection.
- *Staffing and delegation:* Resource allocation to ensure the organization's privacy program is appropriately staffed by adequately trained personnel.
- *Education and awareness:* Existence of ongoing, up-to-date programs to keep employees and relevant business partners aware of privacy obligations.
- *Ongoing risk assessment and mitigation*: Implementation of a process to assist the organization in understanding the privacy risks raised by new products, services, technologies, and business models, and to mitigate those risks. This principle is often operationalized by a cross-functional committee. The committee needs to include software developers to insure that privacy is built into new systems from the beginning.
- *Privacy program risk assessment oversight and validation:* Periodic review of the totality of the accountability program to determine whether modification is necessary.
- *Event management and complaint handling:* Procedures for responding to inquiries, complaints and privacy breaches.
- *Internal enforcement*: Internal enforcement of the organization's policies and discipline for non-compliance.
- *Redress:* The method by which an organization provides remedies for those whose privacy has been put at risk.

Having a privacy program that defines principles and formal processes for responsible data governance can help organizations avoid privacy disasters such as Lotus Marketplace. At the time of the case, however, such privacy programs were largely nonexistent. Further, Lotus Marketplace violated two fundamental privacy principles, notice, and choice, allowing its lessons to be generalized despite the age of the case. People were surprised to learn that information from their credit report was going to be used for marketing by a third party. The ability to provide meaningful advance notice was challenged by the fact that consumers did not have a direct relationship with either Equifax or Lotus, unlike other firms which market directly to consumers. While the two companies technically offered choice by allowing people to opt out of the product, real choice was made infeasible by the lack of notice and the fact it was difficult to remove names from an existing CD-ROM.

In the early 1990s, Smith (1993) conducted a landmark case study of how seven large companies handled sensitive personal information. He characterized what he learned as a cycle of "wandering in the maze"; unofficial information practices drifted until the organization perceived some type of external threat, such as legislative scrutiny or negative publicity, resulting in some type of a formal organizational reaction to the threat. Where explicit policies existed, there was often a mismatch between these policies and the organization's actual practices. Further, executive neglect signaled to employees that privacy was not a strategic corporate issue as senior executives rarely sought information about the policy implications of new uses of information.

Approximately fifteen years later, Bamberger and Mulligan (2011) noted that corporate privacy management in the United States was undergoing a significant change from Smith's findings as firms created chief privacy officer (CPO) positions with responsibility for privacy governance. They interviewed nine CPOs at large organizations who had been identified as leaders in the privacy field by their peers. In addition to developing policies to ensure organizational compliance with privacy laws around the world, all nine firms based their privacy policy on consumer expectations, even if these expectations exceeded what was required by law. Essentially privacy was equated with consumer trust and this led to operationalizing privacy within the firms as risk management rather than pure legal compliance. The importance of this approach to successful privacy management will be discussed subsequently.

4 Two Contemporary Privacy Disasters

Today, the outcry over a CD-ROM database seems quaint. We now fast forward to two contemporary privacy disasters which while involving current technologies, reflect similar failures of corporate decision-making related to strategic uses of new technologies as Marketplace. In the first case, the *New York Times* published an article in 2012 describing how Target used big data analytics (a new

t-2.pdf. There is some overlap between the GAPP and the accountability principles, as some of the GAPP specify process requirements.

technology) of customer purchase data to build a "pregnancy prediction model" which identified female shoppers who were most likely to be pregnant (a controversial application based on personal data). Target subsequently mailed coupons for baby items to the customers identified by the model. One of the mailings went to a teenager, resulting in an angry phone call to Target from her father who didn't know she was pregnant. In subsequent testing, Target quickly learned that while the mailings were legal, they were perceived as creepy by many people because the company knew about their pregnancies in advance, thus violating social norms about being "spied on" (Duhigg, 2012; Hill, 2012). Years later, "Target" is still used as shorthand in discussions about privacy issues raised by the use of predictive analytics to draw inferences about individuals from big data.

In another example, Mattel canceled plans to introduce a smart device called Aristotle. Aristotle was targeted for children from infancy to adolescence (a vulnerable population). It was a voice-activated Wi-Fi device with a companion camera and e-commerce functionality based on Amazon's Alexa (a new technology) and was designed as a "first-of-its-kind connect kids room platform" (a controversial application). The product was criticized by child advocacy groups, parents, and lawmakers based on concerns about profiling and the negative impact an AI device could on have on a child's privacy and development. Following a leadership change and a product review, Mattel decided that Aristotle did not "fully align with Mattel's new technology strategy". It is interesting to note that Mattel had been previously criticized for its Wi-Fi Interactive Hello Barbie in 2015 (Peachman, 2017).

5 New Challenges of Big Data

Big data presents two major challenges for privacy policy. First, there can be significant challenges for organizations to provide meaningful notice to consumers. Without notice, consumers are likely to be surprised about a particular use of their data, as was the case with Marketplace. Today, complex technologies, new business models and data practices, IoT devices without screens, as well as digital services such as big data analytics and behavioral advertising that are difficult to explain provide additional challenges. Even if, at a given moment, it were feasible to provide a notice that could reasonably describe a company's information practices, rapid changes in technology, analytics, and business relationships could quickly render the notice inaccurate (Bruening & Culnan, 2016).

Further, data analytics, by definition, are applied to data originally collected for a different purpose and often combined with data from other sources. The individual may be aware of the initial collection and uses of data, but not of the subsequent analytic processing. Data scientists may use large data sets for exploratory analysis, meaning data are used in ways that could not have been anticipated and would not have been described in a privacy notice. Analytics may also be used to create new personal data from nonpersonal data—illustrated, for example, by the inferences drawn from the customer purchase data used to infer pregnancy in the Target example (Sax 2016). Providing effective notice to consumers when these new uses actually occur is not practical. As a result, organizations need to craft and implement processes to help them successfully navigate current and future privacy risks posed by big data and predictive analytics, as well as other new technology applications.

Second, companies often fail to understand the importance of contextual norms for acceptable use of personal information. These norms reflect expectations for what information practices are acceptable in a *particular context at a given point in time* and, as a result, do not raise privacy concerns in *that* context. One hallmark of uses that violate contextual norms is that they may often be viewed as "creepy"—for example, unexpected data sharing with third parties or new technology features, both of which may violate current expectations and norms for acceptable data practices. Problems are less likely to occur when a technology operates in a way people expect, or when people provide data for a particular purpose that they understand and their data are used in a way that is consistent with that purpose.

As the preceding discussion illustrates, the old model of "notice and choice"—in which the firm posts a notice of its information practices and it is left to the individual to decide whether or not to participate with the firm—is broken. As a result, consumers are currently vulnerable in their dealings with organizations because they suffer from significant deficits of information and control about how their personal information is collected and used that did not exist previously. Given the current limits of notice described previously, these deficits make it impossible for people to be fully informed about an organization's information practices. Similarly, consumers have few opportunities to exercise control over the ways their personal data are reused once information practices have been disclosed (Culnan & Williams, 2009). As a result, people depend on companies to act in their best interest and do no harm.

One way for organizations to do this is to broaden the scope of their formal risk assessment and mitigation reviews beyond privacy compliance to include ethics. The prior examples in the paper were all legal, but subsequent reviews by the organizations suggested they should not have been undertaken. Some have proposed

that ethical reviews might be modeled after existing reviews for human subject research (Calo, 2013).

Privacy governance also must include software development. Reviews to ensure that new applications both comply with a firm's privacy rules and respect consumer expectations need to be conducted before systems are developed and throughout the development process and should include the people building the applications. [6] The assumptions underlying the algorithms that perform automated decisions and have the potential to result in illegal discrimination or errors also need to be reviewed. In a recent study, Waldman (2018) investigated how designers of technology products think about privacy and integrate privacy into their work. He found that for some in his sample, designers were not part of the privacy governance processes being managed by the CPOs in their organizations, with the result that privacy barely factored into design. He concluded that this might explain why so many products seem to ignore our privacy expectations.

6 Implications for IS Research

Privacy is now a mainstream business issue. The International Association of Privacy Professionals (IAPP) now has 50,000 members. Organizations continue to be challenged to avoid privacy disasters resulting from missteps involving new technologies and new sources of data. New regulations such as the EU General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) impose comprehensive requirements on organizations for data use and data governance. In the US, there is heightened congressional interest in privacy, fueled in part by publicized incidents involving some of the large platforms. The time is right for IS researchers to take an interest in privacy policy.

Within the IS field, the privacy issues related to data use have received little attention compared to other privacy issues (Smith, Dinev, & Xu 2011). Given the importance of data to organizations today, there is both a tremendous need and opportunity to conduct impactful research that can help understand and potentially influence both public and organizational privacy policy. Such research can focus on a wide range of interesting questions. For example, what should public policy related to data use look like and what are the possible unintended consequences of new regulation to organizations? Within organizations, privacy policy can be viewed through the lens of existing theories related to implementation. How should different types of organizations operationalize privacy principles in their policies? How does privacy policy function "on the ground" in organizations? What are successful models for ethical review panels? For those interested in research that focuses on consumers, research is needed on how individuals react to particular elements of an organization's privacy policy and how this is related to implementation. For example, Xu, Dinev, Smith, & Hart (2011) studied the link between organizational privacy assurances such as privacy notices and individual responses to the notice and found preliminary evidence that respectful practices can instill perceptions of confidence and fairness. While conducting research within organizations presents challenges such as gaining access, content analysis of privacy disasters based on press accounts or summaries of FTC enforcement actions is one way to provide interesting and useful insights about outcomes related to the implementation of privacy policy.[7]

Finally, there is also a need to address privacy in IS curricula so our students will be well prepared to address the data issues they encounter over the course of their careers. While a detailed discussion of curriculum is beyond the scope of this paper, the skills needed include privacy engineering for systems development and data ethics for data science. For example, the 2016 Joint ACM/AIS MSIS Model Curriculum states that the protection of privacy and integrity should guide all IS practices, including requirements to analyze the privacy implications of key IS decisions, and should incorporate technical safeguards to protect individual privacy as part of IS design and implementation.[8]

7 Conclusion

A recent IDC study predicted that by 2025, 75% of the world's population will interact with data every day and that each connected person will have at least one data interaction every eighteen seconds (Reinsel, Gantz & Rydning, 2018). In addition to current data sources such as online activity, mobile apps, data brokers and other third parties, new sources of consumer data will include the Internet of things (IoT) and other smart devices, connected cars, voice input, and sensors, among others.

It is highly unlikely that consumers will understand fully the new forms of data these devices collect, with whom the data are shared, and how the data are

[6] Privacy engineering is one way to help ensure privacy is built into new applications. It is an emerging discipline which seeks to provide methodologies, tools and techniques to ensure that software applications provide acceptable levels of privacy. See Brooks et al. (2017) and Dennedy, Fox & Finneran (2014).

[7] See Culnan (2011) for an example of how to use FTC enforcement actions to assess accountability.

[8] See MSIS 2016, Global Competency Model for Graduate Degree Programs in Information Systems, May 23, 2017, retrieved from: https://doi.org/10.1145/3127597.

subsequently used. It will also take time for shared norms to evolve about which new practices are appropriate, suggesting that in this data-rich environment, privacy disasters will continue to pose a risk for organizations. Having a comprehensive privacy policy focusing on respect for customer expectations is one way organizations can avoid privacy disasters and capitalize on the opportunities provided by the new sources of data and new analytic tools. Privacy policy is an area ripe for interesting and important research. Hopefully, the IS field will rise to this challenge.

Acknowledgments

This paper is dedicated to my colleague and friend, Jeff Smith. The author acknowledges the helpful comments of John King and the "Privacy Posse" on an earlier version of the paper.

References

Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the books and on the ground. *Stanford Law Review, 63*(2), 247-315.

Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S. & Nadeau, E. (2017). *An introduction to privacy engineering and risk management in federal systems.* Gaithersburg, MD: National Institute of Standards. Retrieved from https://doi.org/10. 6028/NIST.IR.8062.

Bruening, P. J. & Culnan, M. J. (2016). Through a glass darkly: From privacy notices to effective transparency. *North Carolina Journal of Law & Technology*, *17*(4), 515-579.

Calo, R. (2013). Consumer subject review boards: A thought experiment. *Stanford Law Review Online*, *66*, 97-2013. Retrieved from: https://www.stanfordlawreview.org/online/privacy-and-big-data-consumer-subject-review-boards/.

Culnan, M. J. (2011). Accountability as a basis for regulating privacy: Can information security laws inform privacy policy? *Privacy Papers for Policy Makers*. Washington, DC: Future of Privacy Forum. Retrieved from: https://fpf.org/ privacy-papers-for-policy-makers/privacy-papers-2011/.

Culnan, M. J. & Smith, H. J. (1995). Case: Lotus marketplace households . . . managing information privacy concerns (A) & (B). In. D. G. Johnson and H. Nissenbaum, H (Eds.). *Computer ethics & social values* (pp. 269-278). Upper Saddle River, NJ: Prentice Hall.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673-687.

DalleMule, L. & Davenport, T. H. (2017). What's your data strategy*? Harvard Business Review*, *95*(3), 112-121.

Dennedy, M. J., Fox, J., & Finneran, T. R. (2014). *The Privacy engineer's manifesto*. New York, NY: Apress Media.

Duhigg, C. (2012, February 16). How companies learn your secrets. *New York Times Magazine*. Retrieved from https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Hill, K. (2012, February 16). How Target figured out a teen girl was pregnant before her father did. *Forbes*. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4c21bef16668

King, J.L. & Kraemer, K.L. (2019). Policy: An information systems frontier. *Journal of the Association for Information Systems, 20*(6), forthcoming.

Markus, M.L. (2000). Toward an integrated theory of IT-related risk control. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), *Organizational and social perspective on information technology*. Laxenburg, Austria: International Federation for Information Processing.

Peachman, R. R. (2017, October 5). Mattel pulls Aristotle children's device after privacy concerns. *New York Times*. Retrieved from https://www.nytimes.com/2017/10/05/well/family/mattel-aristotle-privacy.html

Reinsel, D., Gantz, J., & Rydning, J. (2018). *The digitization of the world: From edge to core* (IDC White Paper #US44413318). Retrieved from: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

Sax, M. (2016). Big data: Finders keepers, losers weepers? *Ethics and Information Technology, 18*(1), 25-31.

Smith, H. J. (1995). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*(12), 105-122.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798-824.

Waldman, A. E. (2018). Designing without privacy. *Houston Law Review*, *55*(3), 659-727.

Wilkie, J. R. (1990, November 13). Lotus product spurs fears about privacy. *Wall Street Journal*, p. B1.

About the Authors

Mary J. Culnan is a professor emerita at Bentley University. She currently serves as vice president of the Board of the Future of Privacy Forum, a Washington-based think tank and as an alumni trustee of the College of Wooster. She has thirty years of experience in the privacy field; her current research interests focus on privacy governance. Her research has been published in a range of academic journals including the *MIS Quarterly, Organization Science, Management Science, Communications of the ACM, MIS Quarterly Executive, Journal of Public Policy and Marketing,* and the *Journal of Interactive Marketing,* and has also been published in the *New York Times,* the *Washington Post*, and the *Wall Street Journal*. Prof. Culnan has testified before Congress, the Massachusetts House and Senate, and other government agencies on a range of privacy issues. She also served as a commissioner on the President's Commission on Critical Infrastructure Protection. Business Week's e-biz website profiled her as a "Mover & Shaker" in 1999. She holds a PhD in computers and information systems from UCLA.