

Information Privacy: An *MIS Quarterly* Research Curation

Research Curation Team:

Aleš Popovič (*University of Ljubljana*)

H. Jeff Smith (*Miami University*)

James Y.L. Thong (*Hong Kong University of Science and Technology*)

Sunil Wattal (*Temple University*)

Although information privacy was first mentioned in *MIS Quarterly* in 1977 and was highlighted as an important research topic by 1980, it was only in the 1990s that empirical studies in the area began to appear, with momentum beginning to build by the late 1990s. In the subsequent two decades, the publication stream has grown quickly, with some studies applying theories from other disciplines and others moving towards the development of unique, privacy-specific theories.

1. Focus of the Research Curation

This curation highlights the 22 articles with a primary focus on information privacy that have been published in *MIS Quarterly* (see Table 1). Almost all of the definitions of information privacy in these articles have relied on the concept of a data subject's control of information about himself or herself, and we embrace such a definition here: "the ability of the individual to personally control information about one's self" (Awad and Krishnan 2006; Smith et al 1996). Note that Bélanger and Crossler (2011) offered definitions of information privacy concerns (distinct from, but obviously related to, definitions of information privacy itself) at the group, organizational, and societal levels.

Note that we distinguish information privacy, the focus of this curation, from physical privacy, which is associated with physical access and boundaries thereto. The articles deal with methodological approaches, theoretical issues, and qualitative or quantitative research. The goal of this curation is to offer a starting point for future research on information privacy. Although some articles that mention privacy as a derivative construct appear in the other curations (e.g., security), for scoping purposes, this curation highlights those publications in which information privacy is considered to be the central focus in the proposed model, hypotheses, or overall study. The curation, furthermore, excludes articles in which information privacy is used as part of another construct or in which information privacy is used as a synonym for other associated concepts.

2. Progression of Research in *MIS Quarterly*

Temporally, the first two papers in this curation (Mason 1986; Straub Jr and Collins 1990) are best viewed as “motivation” regarding the topic of information privacy as it fits in the information systems discipline, but the responses to calls for privacy-related research emerged somewhat slowly in the pages of *MIS Quarterly*. The first empirical study to focus primarily on privacy was Culnan (1993), which was followed by what has since proven to be an enabling event for many empirical studies: Smith et al. (1996), which validated the “concern for information privacy” instrument. Only one other privacy-focused paper appeared during the 1990s: Webster (1998) provided empirical evidence regarding employees’ unawareness of privacy controls and the manner in which their privacy concerns drove their wariness regarding videoconferencing.

The next collection of papers on information privacy appeared between 2006 and 2009. These papers examined privacy in the online context. Awad and Krishnan (2006) found that online consumers who value information transparency are less willing to be profiled online for personalized services/advertisement by websites. Hui et al. (2007) conducted a field experiment to investigate the values of two types of privacy assurance mechanisms (i.e., privacy statement vs. privacy seals) in encouraging online disclosure of personal information. Pavlou et al. (2007) found information privacy concerns to be one of the four antecedents to perceived uncertainty in online buyer-seller relationships. Son and Kim (2008) examined the effects of information privacy concerns on six types of user responses to information privacy threats. Angst and Agarwal (2009) found that an individual’s concern for information privacy can interact with argument framing and issue involvement to influence attitude toward use of electronic health records, and allowing their personal information to be digitized. Finally, Culnan and Williams (2009) argued that firms should combine a concern for the law with an emphasis on organizational privacy programs to enhance firms’ privacy behavior.

In the next collection of papers, three specifically examined the state of information privacy research to date. Smith et al. (2011) provided an interdisciplinary review of privacy-related research to facilitate a more cohesive treatment of the topic. Bélanger and Crossler (2011) provided important insights about information privacy research in IS field regarding the nature of the information privacy concept, the contributions of existing research, and sampling involved. Pavlou (2011) assessed the state of the IS literature on information privacy and identified promising research directions for advancing IS research on information privacy. Ayyagari et al. (2011) surveyed over 600 working professionals and found that individuals’ perception of invasion of privacy did not significantly relate to strain at work. Lee et al. (2011) found that privacy protection can work as a competition-mitigating mechanism by generating asymmetry in the consumer segments to which firms offer personalization, enhancing the profit extraction abilities of the firms.

The literature following the publication of three review articles on information privacy in 2011 attempted to expand the frontiers of research in this area. Hong and Thong (2013) analyzed the information privacy construct and its factor structure to resolve discrepancies between various conceptualizations of Internet Privacy Concerns (IPC) in prior literature. Sutanto et al. (2013) examined the personalization-privacy tradeoff in the context of smartphone applications and examined the impact of privacy on process and content gratification. Kane et al. (2014) explored privacy in the context of online social networks and suggested how the unique characteristics of these social networks present challenges and opportunities for privacy research. Li and Sarkar (2014) discussed the inherent risks of using regression to analyze data and how privacy can be compromised by these analytics techniques. They propose a new method called digression to take privacy into cognizance while building a regression model. Kohli et al. (2016) suggested that privacy concerns are a key factor in the adoption of Electronic Health Record (EHR) systems and that traditional concepts in privacy such as privacy calculus and psychological ownership need to be re-examined in the context of health care data. Menon and Sarkar (2016) discussed methods to improve the accuracy of shared database while maintaining privacy at the same time when the shared databases are excessively large (tens or hundreds of millions of records).

In reviewing the progression of research on information privacy in *MIS Quarterly*, we observe that a diversity of methodological approaches have been used, including conceptual papers (Culnan and Williams 2009; Kane et al. 2014; Kohli and Tan 2016; Mason 1986; Straub Jr and Collins 1990), literature reviews (Bélanger and Crossler 2011; Pavlou 2011; Smith et al. 2011), case studies (Webster 1998), surveys (Awad and Krishnan 2006; Culnan 1993; Hong and Thong 2013; Pavlou et al. 2007; Smith et al. 1996; Son and Kim 2008), experiments (Angst and Agarwal 2009; Hui et al. 2007; Sutanto et al. 2013), mathematical modeling (Lee et al. 2011), algorithms (Li and Sarkar 2014; Menon and Sarkar 2016), and a combination of methodologies (Ayyagari et al. 2011).

3. Thematic Advances in Knowledge

We roughly identified four main themes from the studies listed in Table 1: (1) conceptual papers that include literature reviews, research agendas, and instrument development; (2) papers that investigate the antecedents of privacy; (3) papers that examine the consequences of privacy; and (4) privacy protection methods and programs. Note that some papers may be classified in more than one theme. Below, we discuss each of these themes.

First, a number of articles are best classified as conceptual papers, which fall into three categories. The first group comprise literature reviews, all of which appeared in the December 2011 issue of *MIS Quarterly*. Bélanger and Crossler (2011) reviewed previous work in the information systems discipline and provided a multilevel

framework for empirical studies. Smith et al. (2011) provided an interdisciplinary review and highlighted three major themes in previous research, one of which centered on an "antecedents – privacy concerns – outcomes" framework. In that same issue, Pavlou (2011) provided an integrative overview of the Beaulanger and Crossler (2011) and Smith et al. (2011) papers. The second group of conceptual papers provides forward-looking research agendas. In the first paper to focus specifically on information privacy in *MIS Quarterly*, Mason (1986) provided a "call to arms" for future research by detailing "four ethical issues of the information age." Some three decades later, Kane et al. (2014) called out a research agenda for social media, with information privacy an important component thereof, and Kohli and Tan (2016), in their focus on electronic health records, highlighted a research question associated with information privacy. The third group of conceptual papers develops and validates measurement instruments that can be used by other researchers who conduct empirical studies. Smith et al. (1996) offered the Concern for Information Privacy (CFIP) instrument, which they developed through a process that entailed bounding the construct and testing draft versions of the instrument, which measured four dimensions of concern. Hong and Thong (2013) extended the CFIP instrument by creating and validating the Internet Privacy Concerns instrument, which included two additional dimensions of information privacy concern and was subjected to extensive nomological validation.

A second theme is antecedents of information privacy. This set of *MIS Quarterly* articles deals with factors that amplify or suppress an individual's perceptions about information privacy. Pavlou et al. (2007) showed that a set of personal beliefs – trust, website informativeness, and social presence – mitigate a buyer's information privacy concerns when engaging in online exchange relationships with sellers. Ayyagari et al. (2011) explored how intrusive features of ICTs – presenteeism (i.e. the degree to which the technology enables users to be reachable) and anonymity (i.e. the degree to which an individual perceives that the use of ICTs is not identifiable, or cannot be tracked) – affect an individual's perception of privacy invasion. They found that an individual's perception of technology presenteeism is positively related to perceived invasion of privacy whereas an individual's perception of technology anonymity lessens the perceived invasion of privacy. Sutanto et al. (2013) showed that an IT solution delivering a personalized service while avoiding disclosing users' personal information to third parties, reduces users' perceptions that their information privacy is being infringed upon, thus mitigating the personalization–privacy paradox and increasing both process and content gratification.

The third theme focuses on the consequences of information privacy. These consequences include reduced effectiveness of direct marketing, resistance toward new technologies, and slowing participation in e-commerce. In the case of direct marketing, Culnan (1993) found that people who are less sensitive about secondary use of personal information have more positive attitudes toward shopping by mail. In

the case of new technology, Webster (1998) found that wary users of desktop videoconferencing in an organization are concerned about loss of personal privacy, and possible video monitoring by their superiors. The majority of studies are in the domain of e-commerce. Pavlou et al. (2007) found that information privacy concerns lead to higher perceived uncertainty resulting in reduced purchase intentions and actual purchases of books and prescription drugs filling online. Son and Kim (2008) examined how online users may respond to privacy threats from online companies. They concluded that those with high information privacy concerns are more likely to refuse to provide their information, instigate removal of their information from the company database, spread negative word-of-mouth, and complain directly to the online company or indirectly to 3rd party organizations. Hong and Thong (2013) found that online users with high information privacy concerns will have lower trust in how websites handle personal information and perceive a higher risk in providing personal information to websites. There are also studies that address the privacy-personalization paradox. Awad and Krishnan (2006) found that online customers who desire greater information transparency are less willing to be profiled by companies. Sutanto et al. (2013) proposed a personalized, privacy-safe solution implemented on smartphones. They found that (compared to the non-personalized application), while personalized (privacy-safe or not) increased application usage, it was only when it was privacy-safe that users saved product messages more frequently. Lee et al. (2011) explored the motivation of firms for privacy protection and its impact on competition and social welfare in the context of product and price personalization.

The fourth theme focuses on privacy protection, which falls into two categories. The first category focuses on a series of social and organizational processes which seek to preserve the privacy rights of individuals. Straub Jr and Collins (1990) emphasized the importance of protecting privacy and recommend steps to be taken by managers to protect privacy. Hui et al. (2007) examined the use of privacy statements and privacy seals, and their impact on individuals' willingness to provide information. Culnan and Williams (2009) suggested that firms should protect consumer privacy by creating a culture and implement governance process for privacy with the involvement of top management. The second category is comprised of emerging work on building systems that are designed to better preserve individual privacy. This includes work on algorithms and techniques which handle data analysis and sharing in a manner that does not compromise individual privacy. Li and Sarkar (2014) discussed the inherent risks to privacy through the use of regression trees which can reveal sensitive data. They proposed a new method called digression which takes privacy into cognizance while building a regression model. Menon and Sarkar (2016) discussed methods to sanitize data for privacy by building scalable algorithms to share data between organizations when the shared databases are excessively large (tens or hundreds of millions of records).

Conclusion

This curation illustrates the breadth of research on information privacy over the past 40 years in *MIS Quarterly*. We hope that these articles will provide a foundation for further research on the critical issue of information privacy in a digitally-enabled world.

Table 1. MIS Quarterly Papers on Information Privacy

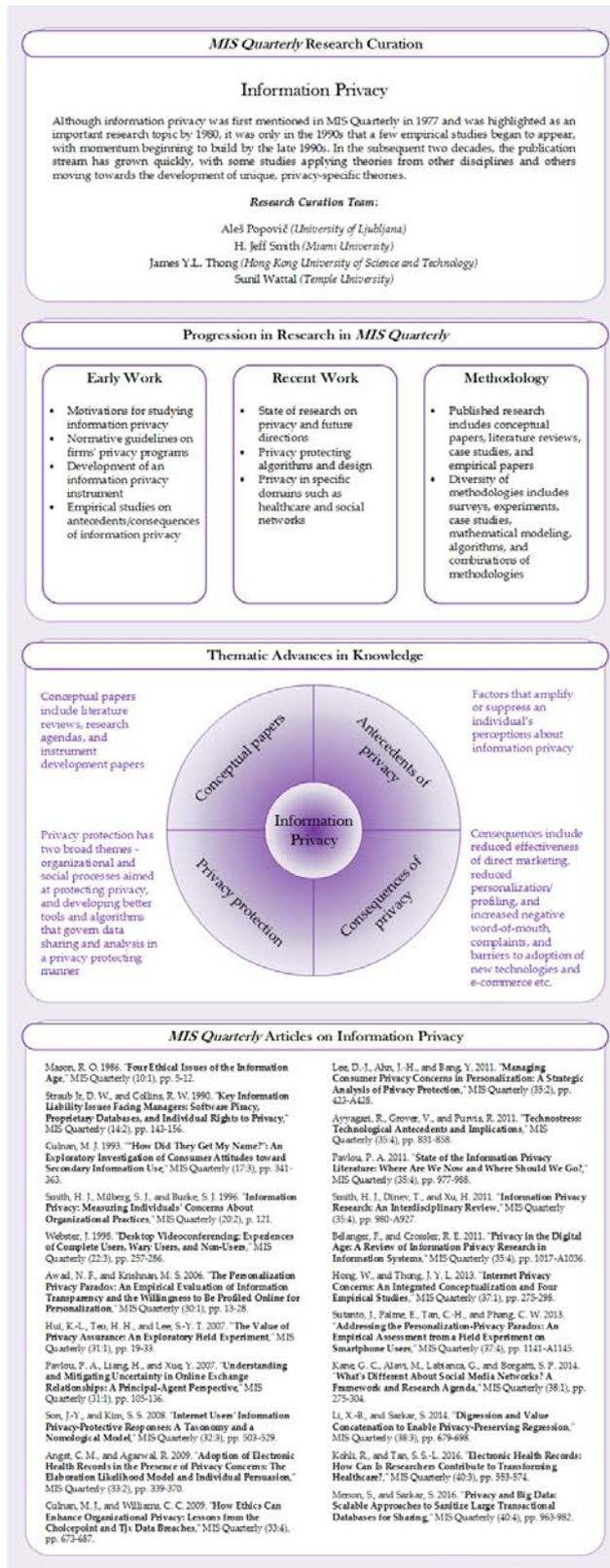
ID	Author(s)	Title	Year	Vol.	Iss.
1	Richard O. Mason	Four Ethical Issues of the Information Age	1986	10	1
2	Detmar W. Straub, Jr., and Rosann Webb Collins	Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy	1990	14	2
3	Mary J. Culnan	"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use	1993	17	3
4	H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke	Information Privacy: Measuring Individuals' Concerns About Organizational Practices	1996	20	2
5	Jane Webster	Desktop Videoconferencing: Experiences of Complete users, Wary Users, and Non-Users	1998	22	3
6	Naveen Farag Awad and M. S. Krishnan	The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization	2006	30	1
7	Kai-Lung Hui, Hock Hai Teo, and Sang-Yong Tom Lee	The Value of Privacy Assurance: An Exploratory Field Experiment	2007	31	1
8	Paul A. Pavlou, Huigang Liang, and Yajiong Xue	Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective	2007	31	1
9	Jai-Yeol Son and Sung S. Kim	Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model	2008	32	3
10	Corey M. Angst and Ritu Agarwal	Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion	2009	33	2
11	Mary J. Culnan and Cynthia Clark Williams	How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches	2009	33	4
12	Dong-Joo Lee, Jae-Hyeon Ahn,	Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection	2011	35	2

ID	Author(s)	Title	Year	Vol.	Iss.
	and Youngsok Bang				
13	Ramakrishna Ayyagari, Varun Grover, and Russell Purvis	Technostress: Technological Antecedents and Implications	2011	35	4
14	Paul A. Pavlou	State of the Information Privacy Literature: Where Are We Now and Where Should We Go?	2011	35	4
15	H. Jeff Smith, Tamara Dinev, and Heng Xu	Information Privacy Research: An Interdisciplinary Review	2011	35	4
16	France Belanger and Robert E. Crossler	Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems	2011	35	4
17	Weiyin Hong and James Y. L. Thong	Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies	2013	37	1
18	Juliana Sutanto, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang	Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users	2013	37	4
19	Gerald C. Kane, Maryam Alavi, Giuseppe (Joe) Labianca, and Stephen P. Borgatti	What's Different about Social Media Networks? A Framework and Research Agenda	2014	38	1
20	Xiao-Bai Li and Sumit Sarkar	Digression and Value Concatenation to Enable Privacy-Preserving Regression	2014	38	3
21	Rajiv Kohli and Sharon Swee-Lin Tan	Electronic Health Records: How Can IS Researchers Contribute to Transforming Healthcare?	2016	40	3
22	Syam Menon and Sumit Sarkar	Privacy and Big Data: Scalable Approaches to Sanitize Large Transactional Databases for Sharing	2016	40	4

Acknowledgement: We thank Jie Tang for providing research assistantship on this curation. She helped to go through 40 years of *MIS Quarterly* papers, count the number of times “privacy” was mentioned and highlight

where it was mentioned in each paper, and summarize the main findings. All errors remain with the curation team.

Figure 1. Information Privacy Infographic



Please cite this curation as follows: Popovic, A., Smith, H.J., Thong, J.Y.L., and Wattal, S. "Information Privacy," in *MIS Quarterly Research Curations*, Ashley Bush and Arun Rai, Eds., <http://misq.org/research-curations>, April 30, 2017.