Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics

Mehdi Khosrow-Pour, D.B.A.
Information Resources Management Association, USA

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI Global
DISSEMINATOR OF KNOWLEDGE

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Khosrow-Pour, Mehdi, 1951- editor.
Title: Advanced methodologies and technologies in system security, information privacy, and forensics / Mehdi Khosrow-Pour, D.B.A., editor.
Description: Hershey, PA : Information Science Reference, [2019] | Includes bibliographical references.
Identifiers: LCCN 2018029248| ISBN 9781522574927 (h/c) | ISBN 9781522574934 (eISBN)
Subjects: LCSH: Computer security. | Data protection. | Digital forensic science. | Computer networks--Security measures.
Classification: LCC QA76.9.A25 A353 2019 | DDC 005.8--dc23 LC record available at https://lccn.loc.gov/2018029248

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 15
Development of Personal Information Privacy Concerns Evaluation

Anna Rohunen
University of Oulu, Finland

Jouni Markkula
University of Oulu, Finland

ABSTRACT

Personal data is increasingly collected with the support of rapidly advancing information and communication technology, which raises privacy concerns among data subjects. In order to address these concerns and offer the full benefits of personal data-intensive services to the public, service providers need to understand how to evaluate privacy concerns in evolving service contexts. By analyzing the earlier privacy concerns evaluation instruments, we can learn how to adapt them to new contexts. In this chapter, the historical development of the most widely used privacy concerns evaluation instruments is presented and analyzed regarding privacy concerns' dimensions. Privacy concerns' core dimensions and the types of context dependent dimensions to be incorporated into evaluation instruments are identified. Following this, recommendations on how to utilize the existing evaluation instruments are given, as well as suggestions for future research dealing with validation and standardization of the instruments.

INTRODUCTION

Personal data collection and utilization are increasingly taking place today as a part of the application of personal data intensive systems and services. Both individuals and data collecting organizations benefit from this. Personal data are collected and processed by private companies and public organizations for various purposes, for example, for delivery of more personalized services and for marketing. Despite its usefulness, extensive personal data collection raises privacy concerns among data subjects, and these concerns are also discussed in public very often. For example, vehicle GPS tracking-based kilometer taxation has been recently under debate. This debate has shown that vehicle tracking data can also be

DOI: 10.4018/978-1-5225-7492-7.ch015

used for purposes other than taxation, and that it can be combined with other data, for example, for producing traffic information services by private or public organizations. Information privacy concerns derive from data subjects' desire to not be monitored, and their worries about the consequences of the use of their data. Privacy concerns often decrease data subjects' willingness to disclose their personal data or to use services that require personal data disclosure. For this reason, privacy concerns may lead to non-adoption of new services and technologies, dropping out of them, or a decline in data disclosure (i.e., omitting data or providing false information). To address these issues, we need to understand how to evaluate privacy concerns in current and future evolving service development contexts. We need insights into how privacy concerns have been evaluated in earlier contexts in order to adapt evaluations to new contexts.

In many countries, legislation sets the foundation for protecting personal data privacy and provides a framework for implementing privacy protection methods and technologies. However, it does not really suppress privacy concerns of the data intensive services' users. People's privacy concerns need to be understood to apply legislation in present-day data collection contexts, characterized by rapid technological change, expanded data collection, diverse uses for collected data, and possibilities to monitor individuals' behavior and combine data from different sources. This understanding can be gained with well-designed *privacy concerns evaluation instruments*. When privacy concerns are evaluated and analyzed, their negative effects on personal data disclosure can be mitigated. In this way, more efficient promotion of personal data intensive services and realization of their benefits for both service users and providers can be reached. In practice, privacy concerns can be addressed by various means based on their evaluation. First, the means of privacy protection and the real risks of data disclosure can be communicated to the data subjects and the general public. Second, data subjects can be given control over their information, and benefits can be offered to them for disclosing information. Third, privacy-preserving systems and service design can be facilitated by taking service users' privacy concerns into account.

Several researchers have contributed to development of information privacy concerns evaluation instruments since the beginning of the 1990s. Due to evolving technologies and new data collection contexts, the existing instruments do not necessarily match data subjects' privacy concerns anymore. Therefore, the validity of these instruments should be examined for their subsequent development and use. We have addressed this challenge by carrying out an analysis of the most widely used privacy concerns evaluation instruments. Through this analysis, we have gathered information specifically on different aspects of individuals' privacy concerns (referred to as privacy concerns' *dimensions* in the instruments) and how they should be taken into account in the instruments' development. We have identified both privacy concerns' core dimensions that have remained unchanged in the evaluations with time and the types of context dependent dimensions to be incorporated into evaluation instruments. When summarizing the results of our analysis, we pay attention to the fact that in addition to being valid and up-to-date, evaluation instruments should also be made easy-to-use enough. In this way, they can be applied to the practical development of personal data intensive services.

In this article, an overview of the existing privacy concerns evaluation instruments will be given and complemented with an outline of their future development. At first, the historical development of privacy concerns evaluation instruments is described, and the most widely used key evaluation instruments from different decades are introduced. Next, an analysis of these key evaluation instruments is presented, focusing on the privacy concerns' dimensions and their changes with technological development and evolving data collection contexts. After this, recommendations on how to utilize the existing

evaluation instruments are given, as well as suggestions for future research dealing with validation and standardization of the instruments.

BACKGROUND

Opportunities for automatic processing of personal data for business purposes have evolved from the first electronic records in the 1950s to present-day comprehensive data collection and processing systems with different data sources and diverse uses. With technological development enabling this change, companies are showing increasing interest in personal data use for developing their products and services and making their operations more effective.

The rapid progress of information technology in the 1960s enabled big enterprises to, for the first time, establish extensive databanks for their customers' personal data. Later on, data warehousing type systems made it possible to easily combine, process, and analyze the collected data for corporate decision making. Along with these changes, discussion on information privacy was evoked, bringing out the need for personal data protection (cf. Westin, 1967). With the launch of e-commerce and other Internet-based services in the mid-1990s, again, new and expanded opportunities for collecting and utilizing personal data of these systems' users appeared. For example, compared to traditional customer records, customers could now be profiled and their preferences could be identified in more detail based on their clickstream. A few years later—specifically, after the introduction of smart phones—development of location and mobility data-based services gained momentum, creating possibilities for gathering even more detailed and extensive data on individuals and their behavior. As a whole, nowadays, the current technology makes possible large-scale personal data collection, integration of data sources of different types, and combination of separate data pools for diverse uses of the collected data. This enables the production of big data that is highly valuable to society, as it has the potential to boost both economic growth and utility for individuals. Increased efficiency, quality, and productivity can be reached, and customers' needs can be better met through big data use. On the other hand, it is clear that there are substantive privacy issues associated with the present-day personal data collection. These issues are being regulated by legislation which needs to be adapted to individuals' privacy behavior and personal data collection technologies and contexts. The need for regulation of automatic data processing with ongoing technological development is reflected, for example, by the General Data Protection Regulation reform in the EU (European Commission, 2012).

Evaluation of individuals' information privacy concerns is not necessarily a straightforward task, as people may be concerned about different aspects of privacy (which are usually referred to as privacy concerns *dimensions*). There has been a tendency to learn to understand and take into account privacy concerns for decades, and these concerns have been measured in opinion polls and as a part of research studies as well. However, privacy concerns evaluation instruments and their dimensionality have been developed in a methodical way only since the beginning of the 1990s. Prior to this, information privacy concerns evaluations were relatively fragmented in nature, in that they considered privacy concerns to be either a unidimensional construct or varying in their dimensions. Culnan (1993) presented some burning questions related to secondary use and publishing of personal data for direct marketing purposes in the off-line context. She stated that companies collecting consumers' personal data may find it difficult to pursue the opportunities provided by data collection technologies if they do not comply with information practices responding to consumers' privacy concerns. This challenge has been extensively studied

in the literature on information privacy concerns and privacy behavior, indicating that individuals' privacy concerns often lead them to decline to disclose personal data if not being informed of appropriate privacy practices. For this reason, it is crucial to have well-designed, validated evaluation instruments for information privacy concerns evaluation. The development of these instruments initially focused on collection of off-line personal data such as customers' demographic and purchase data (e.g., Culnan, 1993; Smith et al., 1996; Stewart & Segars, 2002). With the development of e-commerce and Internet-based services, evaluation instruments specific to the Internet context started to become popular (e.g., Malhotra et al., 2004; Dinev & Hart, 2004; Castaneda et al., 2007). These instruments' items were adapted from the existing instruments, taking into account online threats and unforeseen uses of information. As for individuals' location and mobility data collection through smart mobile devices with GPS tracking, questionnaire items on continuous, large-scale mobility data collection were further developed in some studies on privacy behavior in this context (e.g., Junglas et al., 2008; Xu & Gupta, 2009, Raschke et al., 2014). People are exposed all the time to the possibility of increasingly severe privacy losses due to present-day production of big data together with mobile devices' and body sensors' collection of personal data. As data collection of this kind enables continuous monitoring of individuals and their health and physical condition, data that are often considered highly sensitive information, the need for checking the validity of the existing privacy concerns evaluation instruments is increasing.

Information privacy concerns are changing along with evolving personal data collection contexts and the trend towards increasingly comprehensive data collection and modeling of data subjects' behavior. People's attitudes towards data use may change as it becomes a part of our everyday life and we accommodate to the present-day inclusive data collection culture (cf. Nosko et al., 2010). On the other hand, people are continuously exposed to privacy related news and public discussions and hence are increasingly aware of possible privacy issues regarding personal data use. All these aspects should be taken into account when developing privacy concerns evaluation instruments for new personal data intensive services; in other words, evaluation instruments should be adapted to changes in evaluation contexts and the data disclosure culture.

PRIVACY CONCERNS EVALUATION IN EVOLVING PERSONAL DATA INTENSIVE SERVICES

Present-day and future personal data intensive services are challenging privacy concerns evaluation due to evolving technologies and new data collection contexts. We need to understand existing evaluation instruments' historical evolution to further develop and validate them. Therefore, we present a historical description and analysis of key evaluation instruments and their dimensions in the literature. Our description and analysis covers the most widely used evaluation instruments that date back to different decades and represent different data collection contexts.

Evolution of Privacy Concerns Evaluation Instruments

In the times of electronic records and data warehousing systems, the data collected from customers typically consisted of their contact information and demographic and purchase data. These data were not only used for customer service and companies' operational and strategic aims, they were also often sold for secondary purposes, specifically to direct marketing companies. At the beginning of the 1990s,

Culnan (1993) conducted a survey on data subjects' attitudes towards secondary use of their personal data for direct marketing. She identified two dimensions of privacy concerns: *loss of control* over information and *unauthorized secondary use* of information. Culnan's work was followed by an instrument developed by Smith et al. (1996) for evaluating data subjects' concerns about data collecting companies' organizational information practices for personal data use. Smith et al. identified four dimensions of information privacy concerns, one of them similar to Culnan's dimension of *unauthorized secondary use*. The other three dimensions were *data collection* (i.e., whether excessive data are collected on a data subject), *improper access* to personal information (i.e., within an organization, whether a person without the "need to know" is able to access personal information stored in the files), and *errors* in personal data (e.g., accidental errors or obsolete data). Stewart and Segars (2002) further developed the instrument by Smith et al. Their results suggested that data subjects are concerned about all of the dimensions of organizational information practices simultaneously, rather than any one dimension in particular. Stewart and Segars also found that separate dimensions are interrelated and that the *control* over the information dimension possibly accounts for these interrelationships.

At the beginning of the 2000s, new information privacy concerns evaluation instruments, intended for the Internet context, were introduced. An instrument by Dinev and Hart (2004) for Internet users' privacy concerns evaluation was based on the instruments by Smith et al. and Culnan and Armstrong (1999), and these existing instruments were modified to reflect the nature of the online context. The results by Dinev and Hart suggested an instrument with only two privacy concerns' dimensions: information *finding* on the Internet (i.e., possibilities to track data subjects' activities and their personal information) and information *abuse*. Dinev and Hart also measured *perceived ability to control* information disclosure, recognizing it a separate construct from privacy concerns. However, they pointed out that different results could have been obtained if *need for control* was measured instead of *perceived ability to control*, and that need to control information disclosure may already have been captured by privacy concerns. Almost at the same time as Dinev and Hart, Malhotra et al. (2004) presented their instrument for evaluating Internet users' information privacy concerns related specifically to data disclosure in e-commerce. They proposed three privacy concerns' dimensions by drawing on social contract theory: *collection* of personal information, *control* over the collected information, and *awareness* of information use. The items incorporated into the collection dimension were based on Smith et al. and adapted to the Internet context by slightly changing their wording. Castaneda et al. (2007) further developed privacy concerns' measurements in the Internet context. They aimed to distinguish between general Internet privacy concerns and e-commerce web site-specific privacy concerns. Two dimensions were identified for these concerns, namely concern for personal information *collection* and concern for personal information *use*, the latter one corresponding to *unauthorized secondary use*. Castaneda et al.'s instrument items in the *collection* dimension include the aspects of *loss of control* and *improper access*, reflecting the intrusive side of the Internet context.

The recent development of information privacy concerns evaluation comprises themes such as identification of different conceptualizations of privacy concerns (Hong and Thong, 2013), revisiting of existing privacy concerns evaluation (Sipior et al., 2014), privacy concerns' dependency on the types of digital applications for which data are disclosed (Bergström, 2015), and comparison of different privacy concerns evaluation instruments as a part of a privacy behavior model (Fodor and Brem, 2015). All this research reflects the nature of present-day personal data collection, characterized by high volume and continuity of data collection, digital traces, and possibilities of data mining.

It is worth noting that aspects corresponding to privacy concerns' dimensions are defined in data privacy legislation, but from the data controller's (the body collecting data and legally responsible for its processing) viewpoint instead of the viewpoints of individuals whose data are collected. The aforementioned EU privacy regulation aims to minimize personal data collection by requiring specified, predetermined, and legitimate purposes of use (cf. *collection*, *finding*, and *abuse*). It also sets conditions on data disclosure to third parties (cf. *unauthorized secondary use*), imposes data subjects' right of access to their data and right to demand its rectification or removal (cf. *control*), and sets right to obtain rectification of incorrect data (cf. *errors*). Further, the regulation requires implementation of appropriate technical and organizational data protection measures (cf. *improper access*), informed consent for data processing (cf. *awareness*), and provision of data subjects with specified information on processing of their data (cf. *awareness*). It should be borne in mind, however, that not all individuals' information privacy concerns are covered by legislation. This applies specifically to concerns brought up by the new data collection contexts.

A comparison of the described key information privacy concerns evaluation instruments, as regards their dimensions, is presented in Table 1.

Information privacy concerns evaluation instruments by Smith et al. (1996) and Malhotra et al. (2004) have served as standard evaluation instruments in both offline and Internet contexts. Subsequent studies have often used them as a starting point or reference for their instrument development. The instruments by Smith et al. and Malhotra et al. have been adapted into the evolving data collection contexts by modifying the wording of their items and adding new items relevant to the context. When moving to the Internet context, items originally dealing with companies' data collection and privacy practices in the offline context have been reworded to reflect online data collection. New items on Internet threats incorporated into the instruments deal with stealing or misuse of submitted information, uncertainty about its subsequent use, and continuous tracking of individuals' actions on the Internet. Furthermore, a tendency to adapt instruments better to increasing personal data collection and monitoring of individuals' behavior can be identified in some recent studies (cf. Mao & Zhang 2013, Raschke et al. 2014).

Analysis of Privacy Concerns' Dimensions

Three privacy concerns' dimensions are incorporated into most evaluation instruments regardless of their application contexts: extent of *data collection*, *unauthorized secondary use* of information, and *control* over personal information. Specifically, *collection* is relevant to different kinds of data collection

Table 1. Comparison of the key information privacy concerns evaluation instruments

Dimensions Incorporated Into the Instruments	Unauthorized Secondary Use	Control	Collection	Errors	Improper Access	Awareness	Finding	Abuse
Culnan (1993)	x	x						
Smith et al. (1996)	x		x	x	x			
Stewart & Segars (2002)	x	x	x	x	x			
Dinev & Hart (2004)		(x)					x	x
Malhotra et al. (2004)		x	x			x		
Castaneda et al. (2007)	x		x					

contexts, and it possibly captures the tendency toward increasingly intrusive data collection. It is worth noting that when adapting the instruments to the new contexts, the *collection* dimension has specifically been modified. In the instrument by Smith et al., developed for off-line contexts, the *collection* dimension's items reflect data subjects' views on and reactions to personal data collection by companies, that is, whether data collection and its extent bothers them, and whether they hesitate to disclose their data. Malhotra et al. adapted these items to their online context study. Castaneda et al., instead, based their items on the possibilities of non-transparent and unauthorized data collection in online contexts. *Unauthorized* s*econdary use*, which mainly refers to direct marketing purposes in early evaluation instruments, is a relevant dimension in present-day data collection contexts as well due to the diverse uses and possibilities of combining the data. This dimension has remained relatively unchanged despite the transition in data collection contexts. It deals with data use and sharing without the data subject's permission and using of it for other purposes that it was collected for. *Control* over personal information is a key concept related to the definition of information privacy and has hence been a part of privacy concerns evaluations since their inception. It can be said that its role in privacy protection is becoming even more important with the evolution of data collection contexts and individuals' will to decide the types and uses of their data they should disclose. The *control* dimension reflects data subjects' need for control, their perceptions of loss of privacy, and their opinions on the importance of being able to make decisions about their data collection and use.

Unlike the three dimensions described above, some privacy concerns' dimensions seem to be context dependent. *Awareness* about the use and processing of collected data is an aspect closely related to *control* because the ability to control information requires knowledge and understanding about its uses. This dimension likely becomes more important with increasing, more diverse data collection. It is noteworthy that the instruments intended for online contexts do not incorporate dimensions of *improper access* or *errors* that reflect data subjects' demand for procedures to protect personal data and to ensure its accuracy. These dimensions have been highly relevant to earlier offline contexts' data collection with electronic records accessible to companies' employees and prone to errors with regard to data input. In present-day contexts, *improper access* to data can be considered included in concerns about tracking. This idea may support the exclusion of the *improper access* dimension from the instruments when more parsimonious and simple instruments are needed.

In conclusion, it seems that there are some core dimensions to be incorporated even in present and future privacy concerns evaluation instruments. On the other hand, the relevant dimensions may be dependent on the characteristics of the data collection context. Interrelationships between dimensions and their overlapping should also be taken into account when developing evaluation instruments.

SOLUTIONS AND RECOMMENDATIONS

Information privacy concerns evaluation instruments can be used to gain an understanding of users' privacy concerns regarding personal data intensive services. The existing instruments provide a solid, validated base for the development of privacy concerns evaluation. For this reason, they should be used as a starting point for evaluations and then adapted to the context in question. Our analysis showed that information privacy concerns' core dimensions are incorporated into privacy concerns evaluation instruments independently of the data collection context. These core dimensions are extent of *data collection*, *unauthorized secondary use* of information, and *control* over personal information. Adaptation of

evaluation instruments to the data collection context can be done by varying the rest of the instruments' dimensions. Privacy concerns' dimensions specific to different data collection contexts typically reflect the extent of data collection, the level of data collection's continuity (i.e., its potential for tracking users' behavior either online or in a physical environment), and diversity of subsequent uses of the collected data. It is worth noting that in continuously evolving data collection contexts, new privacy concerns' dimensions may emerge regarding the context's nature and, for example, perceived sensitivity of data. In our research, we have identified the studies presented in this article as the key studies involving evaluation instruments that should be taken into account in privacy concerns evaluation.

FUTURE RESEARCH DIRECTIONS

This article has presented an analysis of key privacy concerns evaluation instruments and their dimensions. Due to technological changes and new data collection contexts, privacy concerns' dimensions should be investigated even in future research, specifically to identify the context-specific dimensions to be applied in the evaluations. As the literature contains a large number of studies on information privacy concerns evaluation, the present analysis should be advanced by analyzing these studies systematically. In addition to the scientific literature, it would be reasonable to extend the analysis to the privacy aspects present in legislation. Similarly, people's changing attitudes towards personal data collection as a part of cultural change should be taken into account in future research. In this way, a validated, standardized, and easy-to-use evaluation framework could be constructed for facilitating application of knowledge to different and new data collection contexts. Relations between separate privacy concerns' dimensions could be another relevant topic of research in order to determine whether different dimensions of privacy concerns always need to be incorporated into the evaluation instruments or whether there are situations in which simplified instruments could be used.

CONCLUSION

This article explored how existing information privacy concerns evaluation instruments could be adapted to match data subjects' privacy concerns in evolving data collection contexts. An overview was presented of the historical development of the information privacy concerns evaluation instruments, spanning a period from the beginning of the 1990s, with its data warehousing systems, to the 2000s, with its continuous monitoring of individuals' actions on the Internet. This overview was followed by an analysis of the key evaluation instruments, which provided insight into their validity for present-day personal data collection contexts. The analysis focused on the dimensions incorporated into privacy concerns evaluation instruments. It showed that these dimensions have changed with evolving data collection contexts and the tendency toward extensive, continuous personal data collection. However, there are core dimensions that seem to be valid even for current data collection contexts. These dimensions, namely extent of *data collection*, *unauthorized secondary use* of information, and *control* over personal information, can be used as a starting point for privacy concerns evaluation. Evaluation should then be adapted to the data collection context in question by varying the instrument's dimensions. Regarding future research, it is suggested to start construction of a validated, standardized, and easy-to-use evaluation framework for facilitating privacy concerns evaluations in different contexts.

REFERENCES

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426. doi:10.1016/j.chb.2015.07.025

Castaneda, J. A., Montoso, F. J., & Luque, T. (2007). The dimensionality of customer privacy concern on the Internet. *Online Information Review*, *31*(4), 420–439. doi:10.1108/14684520710780395

Culnan, M. J. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *Management Information Systems Quarterly*, *17*(3), 341–363. doi:10.2307/249775

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. doi:10.1287/orsc.10.1.104

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. doi:10.1080/01449290410001715723

European Commission. (2012). *Proposal for a regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final*. Brussels: European Commission.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Management Information Systems Quarterly*, *37*(1), 275–298.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. doi:10.1287/isre.1040.0032

Mao, E., & Zhang, J. (2013). The role of privacy in the adoption of location-based services. *Journal of Information Privacy and Security*, *9*(2), 40–59. doi:10.1080/15536548.2013.10845678

Nosko, S., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, *26*(3), 406–418. doi:10.1016/j.chb.2009.11.012

Raschke, R. L., Krishen, A. S., & Kachroo, P. (2014). Understanding the components of information privacy threats for location-based services. *Journal of Information Systems*, *28*(1), 227–242. doi:10.2308/isys-50696

Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, *26*(6), 661–178. doi:10.1108/JEIM-07-2013-0043

Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information privacy: Measuring individuals concerns about organizational practices. *Management Information Systems Quarterly*, *20*(2), 167–196. doi:10.2307/249477

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. doi:10.1287/isre.13.1.36.97

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

ADDITIONAL READING

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security and Privacy*, *7*(6), 82–85. doi:10.1109/MSP.2009.163

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumers dilemma. *Information Technology Management*, *6*(2-3), 181–202. doi:10.100710799-005-5879-y

Chen, K., & Rea, A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems*, *44*(4), 85–92.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886. doi:10.1016/j.jbusres.2006.02.006

European Commission (1995). Directive 95/46/EC. Official Journal of the European Communities (No L 281/31).

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and integrative framework. *Communications of the Association for Information Systems*, *28*, 453–496.

Li, Y. (2012). Theories in online information-privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. doi:10.1016/j.dss.2012.06.010

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289–304. doi:10.1016/j.im.2004.01.003

Liu, Z., Bonazzi, R., Fritscher, B., & Pigneur, Y. (2011). Privacy-friendly business models for location-based mobile services. *Journal of Theoretical and Applied Electronic Commerce Research*, *6*(2), 90–107. doi:10.4067/S0718-18762011000200009

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. doi:10.100711747-006-0003-3

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *Management Information Systems Quarterly*, *32*(3), 503–529.

The Privacy Act of 1974, 5 U.S.C. § 552a (1974).

U.S. Department of Health. Education & Welfare (1973). Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on automated personal data systems. Chapter IV: Recommended safeguards for administrative personal data systems. Washington, DC: U.S. Government Printing Office.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444.

Zhou, T. (2011). The impact of privacy concerns on user adoption of location-based services. *Industrial Management & Data Systems*, *111*(2), 212–226. doi:10.1108/02635571111115146

KEY TERMS AND DEFINITIONS

Information Privacy: An individual's capability to control disclosure of information about him/her to others by determining the type, extent, uses, and users of the data to be disclosed.

Information Privacy Concerns: An individual's concerns about collection, processing, and use of information about him/her, and about the related consequences.

Personal Data: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity (EC Directive 95/46/EC).

Personal Data Intensive Services: Services substantially based on collection, processing, and utilization of users' personal data for service provision. These services can be produced by private companies, public sector organizations, or non-governmental parties.

Privacy Concerns Evaluation Instrument: A way or method to measure individuals' privacy concerns, for example, a survey.

This research was previously published in the Encyclopedia of Information Science and Technology, Fourth Edition edited by Mehdi Khosrow-Pour, pages 4862-4871, copyright year 2018 by Information Science Reference (an imprint of IGI Global).