Understanding Nuances of Privacy and Security in the Context of Information Systems

Emergent Research Forum Paper

Ersin Dincelli
University at Albany, SUNY
edincelli@albany.edu

Sanjay Goel
University at Albany, SUNY
goel@albany.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Abstract

The concepts of privacy and security are interrelated but the underlying meanings behind them may vary across different contexts. As information technology is becoming integrated in our lives, emerging information privacy and security issues have been catching both scholars' and practitioners' attention with the aim to address these issues. Examples of such issues include users' role in information security breaches, online information disclosure and its impact on information privacy, and the collection and use of electronic data for surveillance. These issues are associated with and can be explained by various disciplines, such as psychology, law, business, economics, and information systems. This diversity of disciplines leads to an inclusive approach that subsumes interrelated constructs, such as security, anonymity, and surveillance, as a part of privacy in the current literature. However, privacy and security are distinct concepts. In this paper, we argue that to better understand the role of human factors in the context of information privacy and security, these two concepts need to be examined independently. We examine the two concepts and systematically present various nuances of information privacy and security.

Keywords

Information security, information privacy, heuristics, hedonic, utilitarian, benefits

Introduction

Privacy is the individual's right to be left alone from intrusion and be able to freely express views to selective individuals or disclose personal information at one's will (Warren and Brandeis 1890). As our information systems (IS) become more complex and integrated into society, both the type and volume of data being collected continues to evolve with increasing threat to individual privacy. Thus, in order to better understand how to protect individuals' privacy rights, previous literature has focused privacy-related topics, including online data collection, dissemination, and exploitation of information. On the other hand, there is a huge impetus on data protection by ensuring information security in organizations to prevent data leaks and theft. Despite these links, these are two distinct concepts; information security is focused on ensuring the protection of data from attackers and breaches; while information privacy is focused on disclosure, sharing, and use of personal data (Bansal 2016).

The distinction between privacy and security has endured in literature and popular press (Smith et al. 2011). More recently, privacy and security have been thoroughly examined from a legal and ethical perspective in the context of surveillance and bulk data collection of citizens following revelations by Edward Snowden. This debate centers on the protection of citizens through the 4th Amendment of the US Constitution, which bans unreasonable search and seizure of personal information. Gathering electronic data is an extension of physical search and seizure. In the modern world, a careful balance must be maintained between the need for individual privacy and the national security threats posed by terrorists and hostile nation states. However, the focus of this paper is not on government surveillance and national security but the importance of information privacy and security.

Though this privacy-security debate in the context of government surveillance has been well studied, nuances of privacy and security have not been sufficiently distinguished in the IS literature, especially from the behavioral perspective. The *privacy enigma* is that privacy advocates continue to lobby for better protection of user privacy through legislative means, yet users continue to voluntarily disclose their personal information on social media platforms. Krasnova et al. (2010) posited that despite people's concern over privacy they readily reveal personal information on online social networks in exchange for small rewards. The fundamental premise of such behavior has been laid out in Social Exchange Theory, which argues that interpersonal relationships are based on subjective evaluations of benefits and costs (Homans 1958). This theory forms the basis of privacy calculus, which suggests that users weigh the benefits and costs of personal information disclosure and the gains offset the risks associated with disclosure (Culnan and Armstrong 1999; Dinev and Hart 2006). The risks derived from such disclosure can include becoming targeted by marketers, discrimination, ostracization, identity theft, embarrassment, and profiling. But the benefits can include trust, empathy, and reciprocation (Joinson and Paine 2007), as well as image enhancement and fostering a sense of belongingness (James et al. 2017).

We propose three mechanisms that may cause the potential nuance between online privacy and security. We believe that understanding the underlying distinct mechanisms of these two concepts and identifying predictors of each will contribute towards better design and implementation of information privacy and security related interventions. Such interventions (e.g., contextualized security education, security policies, warnings, and messages) can motivate individuals to adopt better privacy and security behaviors in various contexts and improve individual, as well as organizational, privacy and security.

Information Privacy vs. Information Security

Privacy has been defined from different perspectives across various disciplines. Smith et al. (2011) have categorized these approaches, *value-based* (privacy as a commodity and right) and *cognate-based* (privacy as a control and state), under five disciplines, namely economics, psychology and marketing, law, social and political sciences, and management information systems. This broad classification takes an inclusive approach that captures the essence of other related constructs, such as security.

Information privacy, in general, is concerned about the collection and use of private information. In fact, one of the earliest definition of information privacy, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, p. 5), centers on *privacy as control*. However, a more modern definition of information privacy considers the self as an advocate who is desired to have the *ability to control* privacy and refers to individuals' ability to control how and to what extent their personal information would be collected and used (Smith et al. 2011).

Information security, on the other hand, refers to protection of private information and IS assets from vulnerabilities and potential threats (Crossler et al. 2013). By definition, information security has been defined as a sub-construct of information privacy (Smith et al. 2011), which leads to interchangeable use of the two concepts, both in literature and society. However, with the advances of online communication technologies and living in a highly connected world, information security became a necessity not only to protect individuals' information privacy, but also their assets, such as credit cards and personal computers, as well as the private information of others whom they interact with. Therefore, information security should no longer be studied as a sub construct of information privacy but as a concept on its own.

One important distinction between information privacy and security is the decision mechanism individuals use to take actions regarding privacy and security related activities. Individuals tend to see information security as a burden, a necessity to protect their information, as it needs extra effort to fulfill without giving salient positive outcomes (e.g., as long as nothing bad happens, such as losing credit card information, I should be fine). On the other hand, information privacy is considered as a commodity, a right which individuals can give up control of freely to achieve a social goal or a monetary reward. In this sense, individuals' judgement regarding information privacy and security decisions, and benefit formulation for their calculus vary. Individuals' decisions and their subsequent behavior are also likely to be influenced by different psychographic factors. Thus, we will describe three mechanisms that may cause the nuances between information privacy and security, namely, heuristics, benefit structure, and influential factors across multiple levels.

Benefit Structure for Information Privacy and Security

Literature identifies two types of benefits that individuals would gain from the use of IS: *hedonic* and *utilitarian benefits*. *Hedonic benefits* provide users self-fulfilling values, such as enjoyment and happiness, whereas *utilitarian benefits* provide instrumental and functional values, such as monetary rewards, personalization, or performance increase (Van der Heijden 2004).

According to the privacy calculus model, individuals make decisions based on a subjective assessment of perceived privacy risks and benefits associated with the behavior, such as information disclosure (Dinev and Hart 2006). The greater the perceived benefit of disclosure, the greater its likelihood. However, the value of benefits is discounted by perceived privacy risks. In this sense, individuals engage in decision making regarding disclosure based on a subjective risk-benefit assessment (Dinev and Hart 2006).

Individuals' decisions regarding privacy vary across different contexts (Petronio 2002). Individuals may perform different privacy behaviors in different settings based on both *hedonic* (e.g., social approval) and *utilitarian* (e.g., discount) benefits. However, when the context shifts to security, i.e., protecting information assets, the benefit structure changes to purely *utilitarian* form of benefits because in the information security context, actions do not result in *hedonic benefits*, such as satisfaction or enjoyment (Warkentin et al. 2016). Additionally, benefits and risks of privacy behaviors may be immediate, such as receiving a discount coupon in exchange of personal information. However, the benefits and risks associated with security behaviors may spread over time (e.g., identity theft) (Smith et al. 2011).

The privacy calculus model is suggested as a useful model for understanding users' privacy concerns and information disclosure behavior (Culnan and Bies 2003). The underlying assumption of this model is that individuals' disclosure behavior is performed based on a rational and evaluative decision making process. However, it is possible that individuals do not always make rational risk-benefit assessment (Min and Kim 2015). Instead, they may depend on mental shortcuts to assess privacy risks and attach subjective values to potential risks and benefits derived from privacy behaviors. Such mental shortcuts, also referred to heuristics, may *simplify* the decision-making processes (Carey and Burkell 2009).

Heuristics in Information Privacy and Security Decision-making

The way individuals perceive risks associated with their online behaviors influence their decision-making process. According to Carey and Burkell (2009), when individuals encounter complex situations regarding their privacy, they tend to take mental shortcuts to simplify the decision making processes. Such shortcuts influence how individuals perceive the potentials risks associated with violations of their privacy, as well as their subsequent privacy-protecting behavior (see Figure 1).

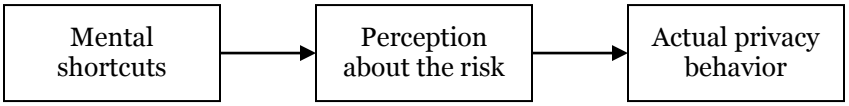

Figure 1. Heuristics and Privacy Behavior

In particular, three heuristics mechanisms influence individuals' decision making. *Affect heuristic* refers to the attitude and overall affective response towards the behavior (Carey and Burkell 2009). If individuals perceive the behavior favorably (with positive feelings), they tend to associate low risks with consequent related actions. One example is sharing personal information online. Individuals share highly personal information on social media profiles simply because they may like to do so (affect).

Representativeness heuristic refers to avoiding complex calculations by estimating likelihood of a privacy risks to occur based on stereotypes. For example, individuals may think that they may not be targeted by hackers because they do not have a credit card, are because they are poor or unimportant.

Availability heuristic refers to relying on past experiences and making decisions by retrieving similar examples from memories (Carey and Burkell 2009). For example, individuals might underestimate the risks associated with their privacy and may engage in risky behavior until they experience a personal information abuse (Smith et al. 1996). Individuals may also overestimate the risks if they have an acquaintance who had negative consequences of privacy invasion (Mutchler and Warkentin 2015)

Additionally, people tend to take mental shortcuts when they (1) lack the motivation to process the information due to its low personal relevance, and (2) have limited ability to process the information due

to their insufficient knowledge or the complexity of the given issue (Petty and Cacioppo 1984). Instead of a careful risk-benefit analysis, people take mental shortcuts or decisions based on factors such as credibility, appearance, and attractiveness. Performing an information security behavior (e.g., regular password change, security updates, and patches) depends on the knowledge and awareness of a given security issue (Schmidt et al. 2008). Such behaviors may be seen as a burden (Johnston and Warkentin 2010) and may be disregarded to save time or due to insufficient knowledge. Individuals may also overestimate their knowledge of performing security-related behaviors (Jensen et al. 2005).

Different heuristics mechanisms may explain individuals' decision-making processes regarding privacy and security related activities. For example, *affect heuristic* may be more salient in privacy behavior (e.g., self-disclosure of personal information), whereas, *availability heuristics* may be more salient in security behavior (e.g., use of stronger passwords after a recent hack). There may be other factors that can distinguish privacy and security behaviors besides heuristics. The following section elaborates on the *intrapersonal* and *interpersonal* factors and their relation to security and privacy related behaviors.

Influential Factors across Multiple Levels

Pedersen (1997) identified six types of individual privacy behaviors -- solitude, isolation, anonymity, reserve, intimacy with friends, and family. He found several common and unique factors across the six types of privacy. Behavior is a complex construct that is influenced by various factors from multiple levels (Glanz et al. 2008). According to socio-ecological model, these levels include *intrapersonal* (e.g., psychological factors, such as attitude), *interpersonal* (e.g., cultural factors, such as values and norms), *organizational* (e.g., educational institutions), *community* (e.g., religious groups), and *public policy* (e.g., federal or state laws and regulations) (Glanz et al. 2008). Behaviors related to information privacy and security may also be influenced by factors across multiple levels in different magnitude.

Security-related behaviors may be derived from intrinsic motivations, whereas individuals may be extrinsically motivated to perform privacy-related behaviors. For example, the decision to use a stronger password may be self-determined, influenced by factors such as knowledge, awareness, and past experience. On the other hand, the willingness to be connected with others facilitates privacy-related behaviors by inspiring *interpersonal* behaviors that may challenge personal privacy, but which achieve self-presentation goals (e.g., impressing others or building social capital). Such goals extrinsically motivate individuals to carry out the behavior and serve as the external rewards that individuals expect to receive from performing a privacy behavior. Therefore, although both privacy and security behaviors are influenced by factors from all aforementioned levels, security behaviors may be influenced more by *intrapersonal* factors that can trigger intrinsic motivation, whereas, privacy behaviors may be influenced more by *interpersonal* factors that are associated with extrinsic motivation (Dincelli and Goel 2017).

Factors, in other levels, i.e., *organizational*, *community*, and *public policy*, may have distinct effects on privacy and security. For example, security requirements by employers may enforce individuals' actions regarding certain security issues (e.g., changing passwords regularly), whereas privacy policies may suggest desired behaviors without any sort of enforcement. Similarly, different countries and cultures might have different laws and norms regarding individual privacy. Therefore, cultural values and societal norms may cause distinct perceptions and attitudes towards privacy related issues. On the other hand, security is considered binary and security measures tend to be universal, not country or culture specific.

Conclusion

The distinction between information privacy and security has not yet been clearly defined in the IS literature. Although information privacy and security are conceptually related, we argue that they should be studied as separate constructs. This paper classifies nuances of privacy and security into three categories; namely, heuristics, benefit structure, and examining influential factors from multiple levels. We believe that these three approaches can be used to develop studies that examine the extent and type of variations between these two interrelated concepts. By examining the influences of various factors (e.g., benefit structure, heuristics, and various other multilevel determinants) on individuals' behaviors, perceptions, attitudes, beliefs, and concerns related to privacy and security, future studies can further shed light on the subtle differences between the two concepts. By doing so, more specific research questions can be formed in future studies about privacy and security, which lead to design and implementation of more effective interventions for information privacy and security related issues.

REFERENCES

Bansal, G. 2016. "Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation," *Journal of Computer Information Systems* (56), pp. 1-14.

Carey, R., and Burkell, J. 2009. "A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments," in *Lessons from the Identity Trail,* I. Kerr, V. Steeves and C. Lucock (eds.). Oxford University Press, pp. 65-82.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90-101.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.

Dincelli, E., and Goel, S. 2017. "Can Privacy and Security Be Friends? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks," in: *50th Hawaii International Conference on System Sciences (HICSS)*. Waikoloa, HI.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Glanz, K., Rimer, B. K., and Viswanath, K. 2008. *Health Behavior and Health Education: Theory, Research, and Practice*, (Fourth ed.). San Francisco, CA, USA: John Wiley & Sons.

Homans, G. C. 1958. "Social Behavior as Exchange," *American journal of sociology* (63:6), pp. 597-606.

James, T. L., Lowry, P. B., Wallace, L., and Warkentin, M. 2017. "The Effect of Belongingness on Obsessive-Compulsive Disorder in the Use of Online Social Networks," *Journal of Management Information Systems*, forthcoming.

Jensen, C., Potts, C., and Jensen, C. 2005. "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies* (63:1), pp. 203-227.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Emprical Study," *MIS Quarterly* (34:3), pp. 549-566.

Joinson, A., and Paine, C. B. 2007. "Self-Disclosure, Privacy and the Internet," in *The Oxford Handbook of Internet Psychology,* A. Joinson, K. McKenna, T. Postmes and U.-D. Reips (eds.). Oxford, United Kingdom: Oxford University Press, pp. 237-252.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Min, J., and Kim, B. 2015. "How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus between Benefit and Cost," *Journal of the Association for Information Science and Technology* (66:4), pp. 839-857.

Mutchler, L. A., and Warkentin, M. 2015. "How Direct and Vicarious Experience Promotes Security Hygiene," in: *10th Annual Symposium on Information Assurance (ASIA)*. Albany, NY: pp. 2-6.

Pedersen, D. M. 1997. "Psychological Functions of Privacy," *Journal of Environmental Psychology* (17:2), pp. 147-156.

Petronio, S. 2002. *Boundaries of Privacy*. Albany, NY: State University of New York Press.

Petty, R. E., and Cacioppo, J. T. 1984. "Source Factors and the Elaboration Likelihood Model of Persuasion," *Advances in Consumer Research* (11:1), pp. 668-672.

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., and Li, S. 2008. "A Cross-Cultural Comparison of U.S. And Chinese Computer Security Awareness," *Journal of Global Information Management* (16:2), pp. 91-103.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Van der Heijden, H. 2004. "User Acceptance of Hedonic Information Systems," *MIS Quarterly* (28:4), pp. 695-704.

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. "Continuance of Protective Security Behavior: A Longitudinal Study," *Decision Support Systems* (92), pp. 25-35.

Warren, S. D., and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), pp. 193-220.

Westin, A. F. 1967. *Privacy and Freedom*. Atheneum, NY: The Bodley Head.