Individuals’ IT-related Privacy Concerns: a Two-phase Cognitive Model

Abstract

Privacy is a highly dynamic concept and individuals with distinct life experiences and knowledge can perceive it differently. Despite the advances made by past IS research, little is still known about the antecedents of Privacy Concerns Related to IT (PCIT), their formation, and the relationship between general PCIT and PCIT regarding specific technologies. In an effort to address these knowledge gaps, the present study adopts the Elaboration Likelihood Model (ELM) as a theoretical lens to introduce three new constructs as key antecedents of general PCIT: privacy-related legal knowledge, privacy-related IT knowledge and general involvement with IT-related privacy. Based on ELM, the paper also proposes a two stage cognitive model that conceptualizes the relationship between general and technology-specific PCIT, and introduces a feature-based conceptualization of technology-specific PCIT.

Keywords: Privacy Concern, Technology-Specific Privacy Concern, Cognitive Model, User Characteristics
Introduction

The fast pace of technological advancements and competition among technology providers has facilitated information technology (IT) adoption by individuals and organizations. This has not only increased the amount and spread of digitalized personal information on the Internet, but it has also made IT accessible to those with malicious intent. A recent poll found privacy concerns related to IT (PCIT) to be the second most important privacy concern after financial privacy, with 66% of the respondents also being concerned about their privacy in general (Office of the Privacy Commissioner of Canada 2013). Another study found that 92% of Europeans were concerned about data collected by mobile apps and without their consent (European Commission 2014). The cross-disciplinary nature of the privacy concept (Smith et al. 2011) and the difficulties of providing a generally accepted and context-independent conceptualization of privacy (Xu et al. 2008; Pavlou 2011; Xu et al. 2011) have led Information Systems (IS) scholars to use privacy concerns as a proxy for assessing privacy in empirical research (Smith et al. 2011).

Despite the advances made by past PCIT research, the nature of IT-related privacy concerns varies across different studies. As noted by Hong and Thong (2013), some researchers have focused on perceptions of one’s concern for others’ behavior, while others have examined perceptions and/or expectations of others’ behavior. Both the dimensionality (Hong and Thong 2013) and the object toward which privacy concerns exist also varies. For example, while some studies have emphasized context-specific assessments of privacy concerns (e.g., Xu et al. 2011; Xu et al. 2012a; Jiang et al. 2013), others have focused on defining a general construct of privacy concerns related to IT (e.g., Hong and Thong 2013). Thus, the IS literature appears to have three variants of the privacy concerns construct: affective (perceptions of one’s concerns), behavioral (perceptions of others’ behavior) and normative (expectations of others’ behavior). Further, many IS researchers have examined the effects of privacy concerns on dependent variables that pertain to various behaviors, such as users’ willingness to provide information or their adoption of online transaction methods (Bélanger and Crossler 2011). To shed light on the nature and conceptualization of PCIT, some scholars have theorized about the formation of the PCIT construct and its antecedents (Table 1). A review of the literature on the formation of PCIT and its antecedents suggests that there also is a lack of research examining the relationship between general PCIT and technology-specific PCIT, as well as the role of privacy-related IT and legal knowledge in the formation of PCIT.

Interestingly, Li (2011) distinguished between general and specific concerns for information privacy by viewing general concern for information privacy as reflecting an individual’s “overall concern for information privacy across e-commerce contexts” (p. 466) and specific concern for information privacy as the individual’s privacy concern in “a given e-commerce context”. However, as the use of behavior-tracking software has extended the objects of individuals’ privacy concerns beyond information that is willingly shared with e-commerce websites, the present study adopts a broader view and defines general PCIT as individuals’ concerns regarding information and behavior privacy across IT contexts as a whole, and technology-specific PCIT as individuals’ concerns about privacy-related features of a specific technology (it is important to note that these two definitions do not categorize different IT contexts; they simply distinguish between concerns about IT in general as a whole and concerns about specific features of a specific IT, such as those of an organization’s ERP system). Then, after examining past conceptualizations and operationalizations of these constructs, the paper adopts the Elaboration Likelihood Model (Petty and Cacioppo 1986) as a theoretical lens to develop a feature-based conceptualization of technology-specific PCIT and proposes a two-phase cognitive model linking general and technology-specific PCIT.

The PCIT Construct: Formation and Antecedents in the IS literature

In order to better understand what drives the diverse conceptualizations of PCIT and to uncover its less studied aspects, we reviewed IS research that operationalized it. To do so, we identified relevant studies from Hong and Thong (2013) and searched the IS basket of eight journals and all ICIS proceedings since 2004. We included research that either developed a measure (e.g., Smith et al. 1996; Malhotra et al. 2004; Chen and Rea 2004; Dinev and Hart 2004; Zviran 2008), or adapted past measures of PCIT (e.g., Pavlou et al. 2007; Hui et al. 2007; Sheng et al. 2008; Xu et al. 2012b, and Hong and Thong 2013), and for each study we noted a) the object of its privacy concern construct, b) the antecedents and consequences of the construct, and c) its technological context. This examination helped identify three areas in need of further
study. First, the *object toward which privacy concerns exist* varies in the literature. For example, while in Smith et al. (1996) this object is “organizational information privacy practices”, in Malhotra et al. (2004) it is individuals’ shopping preferences and financial information. Such differences partly stem from the different IT contexts studied by researchers: while some adopted a silo perspective toward IT by focusing on *specific technologies*, e.g., a specific website or a wearable technology for providing location-based services (e.g. Malhotra et al. 2004 and Sheng et al. 2008), others viewed technology from a general perspective to examine *general technology contexts*, such as E-business (e.g., Chen and Rea 2004) or the Internet (e.g., Dinev and Hart 2004). Yet, in the complex and interwoven ecosystem of today’s IT, many users may simultaneously hold both general, as well as technology-specific privacy concerns. The increasing connectedness of the IT infrastructure has also raised the importance of topics such as record linkage (e.g. Li and Sarkar 2010) in the privacy concerns literature, highlighting the importance of distinguishing between *general PCIT* and *technology-specific PCIT*, and examining their relationship.

Second, six of the ten studies that developed measures of PCIT (i.e. Smith et al. 1996; Chen and Rea 2004; Dinev and Hart 2004; Hui et al. 2007; Sheng et al. 2008; Zviran 2008) used respondent samples that were likely to have been previously exposed to privacy-related topics, which in turn might have influenced the extent to which the samples in question represented average technology users. For example, Smith et al.’s (1996) sample consisted of employees of financial organizations, IS managers, and graduate business students, all of whom are likely to have been already familiar with organizational information privacy issues when they participated in the study. Similarly, Chen and Rea’s (2004) respondents were students of a website architecture course who were likely to be knowledgeable about privacy vulnerabilities of websites. As such, the impact of individuals’ prior privacy-related knowledge on their perceptions of PCIT remains largely unexplored. Taking into account users’ privacy knowledge can help explain some of the mixed results that have been observed regarding the effect of privacy-assurance mechanisms, such as those concerning the influence of privacy seals on user behaviors (Tsai et al. 2010).

<table>
<thead>
<tr>
<th>Authors</th>
<th>PCIT measures</th>
<th>Antecedents of PCIT</th>
<th>Moderators, Mediators</th>
<th>Control var.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steward and Segars 2002</td>
<td>Smith et al. 1996</td>
<td>Computer anxiety</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Xu and Teo 2004 (Specific technology)</td>
<td>Combination of Smith et al. 1996 and Dinev and Hart’s 2004 measures</td>
<td>Control assurance mechanisms (technology, Industry self-regulation and legislation)</td>
<td>NA</td>
<td>General attitude toward technology, previous privacy experience, Innovativeness</td>
</tr>
<tr>
<td>Xu 2007 (Specific technology)</td>
<td>Smith et al. 1996</td>
<td>Control assurance mechanisms</td>
<td>Self-construal, perceived control</td>
<td>Experience with mobile applications, desire for information control, trust propensity, previous privacy experience</td>
</tr>
<tr>
<td>Dinev et al. 2008</td>
<td>Dinev and Hart 2004</td>
<td>Government intrusion concerns, perceived need for government surveillance</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Junglas et al. 2008</td>
<td>Smith et al. 1996</td>
<td>Agreeableness, conscientiousness, and openness to experience</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Xu et al. 2008 (Specific technology)</td>
<td>Smith et al. 1996</td>
<td>Individual’s disposition to privacy, perceived privacy risk, privacy control</td>
<td>Privacy intrusion</td>
<td>NA</td>
</tr>
<tr>
<td>Chen et al. 2009</td>
<td>Smith et al. 1996</td>
<td>Social network overlap, decisional control, information exclusivity</td>
<td>Decisional control</td>
<td>Disposition to value privacy, cookie setting, trust propensity, previous Invasion of privacy, SNS experience</td>
</tr>
<tr>
<td>Lowry et al. 2011</td>
<td>Smith et al. 1996</td>
<td>Masculinity, uncertainty avoidance, power distance, collectivism (cultural dimensions)</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Xu et al. 2012.a</td>
<td>Smith et al. 1996</td>
<td>Individual self-protection, industry self-regulation, government legislation</td>
<td>Perceived control over personal information</td>
<td>Desire for information control, privacy experience, trust propensity, prior experience with mobile &amp; LBS, fashion</td>
</tr>
<tr>
<td>Jiang et al. 2013</td>
<td>Malhotra et al. 2004</td>
<td>Perceived anonymity of self/others, perceived intrusiveness</td>
<td>NA</td>
<td>Gender, age, Internet experience, general chat room experience, chat room allocation, usage frequency, and misrepresentation beliefs</td>
</tr>
</tbody>
</table>

**Table 1. Formation of PCIT and its Antecedents in the IS literature**

Third, some IS studies have tried to improve perceptual measures by combining them with measures of a set of *privacy-related behaviors*, e.g., Hui et al.’ (2007) privacy concerns construct includes measures of
users’ cookie preferences. However, the IS privacy-concerns literature appears to have largely focused on understanding user behaviors following their exposure to traditional privacy enhancing mechanisms, such as privacy policy notifications and privacy seals (e.g. Hui et al. 2007; Tang et al. 2008). It is interesting to note that, recent advances in Privacy-Enhancing-Technologies (PET) provide opportunities for examining factors that can affect user adoption of new technologies, such as Encryption and Steganography Software, Blind Digital Signature (Seničar et al. 2003), anti-tracking (e.g. Ghostery.com, Disconnect.me) and anonymizer software (e.g. Tor project), as well as user perceptions of the persuasiveness and quality of traditional privacy enhancing mechanisms.

The antecedents of PCIT identified in the present literature review are summarized in Table 1. As can be seen in Table 1, these can be grouped into individual characteristics, legislative assurance mechanisms, social network characteristics in the context of social networking websites, and perceptions of government surveillance and intrusion. Further, many studies assessed PCIT based on Smith et al.’s (1996) operationalization. The individual antecedents of PCIT that have been studied include computer anxiety, personality traits, individual disposition to privacy, and perceived anonymity of self. Interestingly, existing knowledge regarding factors that can affect PCIT seems limited (Junglas et al. 2008). Despite controlling for some general technology- and internet-related experiences, IS research has also not yet examined prior privacy-related knowledge of the participants, such as their privacy-related IT and legal knowledge, as antecedents of their PCIT. Moreover, few studies have theorized about how individuals’ privacy concerns might be formed. An exception is Xu et al. (2008), who theorized the formation of individuals’ privacy concerns via a variance-based model that elaborated a cognitive process of PCIT formation. They conceptualized privacy awareness as reflecting users’ perceptions of the information they have about privacy news, privacy issues and privacy solutions, and hypothesized them as antecedents of individual disposition to privacy. The construct of privacy involvement (Larose and Rofin 2007) is similar to privacy awareness as it also captures user perceptions of their privacy-protection skills. It should also be noted that both studies have employed measures of user perceptions and subjective evaluations of their information and skills.

The Formation of Individuals’ PCIT: A Two-Part Cognitive Model

To explain how individuals’ PCIT can form, we apply the Elaboration Likelihood Model (ELM) (Petty and Cacioppo 1986) as a cognitive theoretical lens. According to ELM, recipients exposed to new information are differentially influenced by the content of the message via either a central route or a peripheral route. The motivation to process a message and the ability to process a message are two key determinants of the route used in its processing. Individuals who have both the motivation and ability to process a message will analyze the quality of the arguments provided in the message in a more structured and objective manner, i.e., via the central route, than those who lack such motivation and/or ability. The latter will instead tend to rely on peripheral cues in analyzing the message, i.e., the peripheral route. Further, according to ELM, attitudes that are formed or changed through the central route are more enduring and can strongly predict behavior (Petty and Cacioppo 1986). To clarify the meaning of the attitude concept, Petty and Cacioppo (1986, p.5) noted that “attitudes can be based on a variety of behavioral, affective, and cognitive experiences and are capable of guiding behavioral, affective and cognitive processes”. As noted earlier in the Introduction, individuals’ privacy concerns can also be viewed as having affective, behavioral and normative aspects, which in turn suggests that PCIT can be viewed as a specific attitude whose formation and change can be explained via ELM. Moreover, a variety of empirical studies have strongly supported ELM’s predictive and explanatory powers (e.g., Cho 1999, Tam and Ho 2005), including several in IS. For example, Angst and Agarwal (2009) used ELM to study attitude change and opt-in behavior of electronic health-record system users and Bansal et al. (2008) used ELM to conceptualize the moderating role of privacy concerns on how privacy policy quality and peripheral cues affected users’ trust in a website. Thus, ELM provides a plausible theoretical explanation of the relationship between general PCIT and technology-specific PCIT, and a useful theoretical lens for incorporating users’ privacy-related knowledge as an important antecedent of their privacy concerns. The key role played by the central route of ELM is also suggested by the fact that many IS scholars have studied the effects of privacy concerns on different behaviors (Belanger and Crossler 2011), and as noted above, attitudes formed and changed through the central route of ELM tend to strongly affect such behaviors. Hence, the first phase of our model elaborates individuals’ formation of general PCIT, which in turn is hypothesized to influence their technology-specific PCIT when they encounter a new IT. As noted by Li (2011), studies that examined the
effect of individuals’ general knowledge about the Internet on privacy concerns have reported mixed results which suggests that “more efforts are needed to examine the nature of such knowledge and its impact on privacy concern” (p. 461). The present study answers this call by conceptualizing two specific types of knowledge, i.e., privacy-related IT knowledge and privacy-related legal knowledge, and by hypothesizing the effect of each on general PCIT. The next section describes the constructs of the research model and their relationships.

**Phase 1: General PCIT and Its Antecedents**

According to Clark (1999), personal privacy can be viewed along four dimensions: a person’s body, which is relevant to privacy concerns, such as for full body scanners at airports or for requiring bodily fluid samples, as well as personal data, behavior, and communication. Although the application of IT infrastructure and involvement of IT companies in projects that deal with bodily fluids (e.g. The Genographic Project 2014) has turned the privacy of a person’s body into a valid privacy concern, as all data from which such concerns originate are typically digitalized, they can be considered as personal information in the context of IT-related privacy concerns. Moreover, all communications that happen through IT can be viewed to constitute a special type of online behavior. Hence, based on Clark (1999), we conceptualize general PCIT as a formative second-order construct with two first-order dimensions: personal information concerns and e-behavior monitoring concerns. Further, as several IS studies have relied on Dinev and Hart’s (2004) measure of online behavior concerns to assess personal information concerns (e.g. Sheng et al. 2008), we suggest that general PCIT can be assessed via existing measures of these two constructs. The antecedents of general PCIT were conceptualized as follows.

**Privacy-Related IT Knowledge**

Privacy-Related IT knowledge is defined here as individuals’ knowledge of technical aspects of IT that can affect their privacy. In a recent survey, 56% of Canadians declared that they were not confident about their knowledge of how new technologies may influence their privacy (The Office of the Privacy Commissioner of Canada 2013). While measures of constructs such as computer self-efficacy (Compeau and Higgins 1995) and IT competence (Bassellier et al. 2001; Bassellier et al. 2003) are anchored on users’ subjective perceptions of their IT-related skills, the IS literature currently lacks a conceptualization and objective measure of users’ privacy-related IT knowledge. Further, operationalizations of this construct in fields outside IS have been largely based on one-dimensional single item measures (Park 2013). Two bodies of knowledge can be useful in the development and validation of a comprehensive and multidimensional measure of privacy-related IT knowledge: 1) The literature on computer literacy, IT literacy and digital literacy (e.g., Hargittai 2005, 2009), which has partly focused on developing standard tests of IT skills, and 2) Knowledge developed by privacy practitioners and scholars for privacy-related certifications, such as the body of knowledge for IT privacy certification proposed by the International Association of Privacy Professionals (2014).

The present study’s definition of general PCIT suggests a two-dimensional conceptualization of privacy-related IT knowledge: 1) general knowledge about IT infrastructure (e.g., the Internet, WLAN, IP addresses, cloud servers) and its characteristics that make unwillingly shared personal information identifiable and willingly shared personal information vulnerable to privacy intrusions. This dimension is related to personal information concerns; 2) general knowledge about privacy-intruding software agents, such as cookies, beacons and other behavior-tracking software, which relates to e-behavior monitoring concerns. Individuals’ IT knowledge about privacy-related technical topics, such as the traceability of IP addresses and online behaviors, the technical abilities of ISPs and governments for Internet surveillance, the extreme connectivity of the IT ecosystem, and the possibility of retrieving deleted data from “unsanitized” hard drives (Kissel et al. 2006) can increase individuals’ general PCIT. Thus, we suggest that privacy-related IT knowledge will positively influence general PCIT (H1).

**Privacy-Related Legal Knowledge**

Privacy-Related legal knowledge is defined here as individuals’ knowledge of IT-related legal aspects that can affect their privacy. Although some IS studies (e.g., Xu and Teo 2004) have found a negative relationship between the “mere existence of privacy protection law” and privacy concerns, none of the studies reviewed here conceptualized privacy-related legal knowledge as an antecedent of PCIT. Hence, an objective of the present study is to also develop a valid measure of individuals' privacy-related legal
knowledge. Despite the presence of privacy legislation in many countries, e.g., two federal laws of Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada (Privacy Legislations in Canada 2014), the Data Protection Directive in the European Union legislation (Data Protection Directive 2014), and the Electronic Communication Privacy Act of 1986 in the United States, many IT users remain poorly informed about their existence, as well as their potential vulnerabilities and shortcomings. For example, following the recently proposed changes to the Canadian Digital Privacy Act (i.e., Bill-S4), “organizations will be permitted to disclose personal information without consent (and without a court order) to any organization that is investigating a contractual breach or possible violation of any law” (Geist 2014). Fraser (2005) also noted two other vulnerabilities of privacy-related legislation in Canada: “Canadian PIPEDA cannot be applied to non-commercial operations of charities and the “MUSH” sector, meaning municipalities, universities, schools and hospitals...[and] the question of whether PIPEDA applies to commercial activities that take place outside Canada’s borders remains.” (p. 1). Moreover, the pace of amendments and modifications to privacy-related legislations are sluggish and much slower than the pace of technological advancements (European Commission 2012). The multinational nature of the Internet also adds to legal complexities of privacy-related issues since the physical location of a specific online company determines the privacy law it is subjected to, as well as the privacy rights of its users. Being knowledgeable about such legal issues, complexities and uncertainties in privacy-related legislations is likely to increase the IT-related privacy concerns of people who are aware of privacy as a fundamental human right. Hence, we suggest that privacy-related legal knowledge will positively influence general PCIT (H2).

**General Involvement with IT-Related Privacy**

This construct is defined here as individuals’ attentiveness to IT-related privacy issues. Some IS researchers (e.g., Zviran 2008) have theorized individuals’ previous privacy-invasion experience as an antecedent of PCIT. Smith et al. (1996) went further by including an item for measuring individuals’ awareness of others’ privacy invasion experiences. Existing measures of this construct mainly rely on individual perceptions even though the majority of IT users do not have a “coherent view of what information is worth defending and how to defend it” (Keller 2013). That is, unless individuals have personally experienced major negative consequences due to the invasion of their privacy (e.g., financial loss, identity theft), they do not seem to grasp the privacy invasiveness potential of many situations, which raises concerns regarding the validity of perceptual measures. To address this shortcoming and to meet the theoretical prerequisites of ELM’s central route, which requires strong motivation and ability to process a message, the present study intends to operationalize this construct by asking individuals whether they follow privacy-related news and question them on their attentiveness and objective understanding of recent local and/or global privacy invasion cases. Such an approach can enable a comprehensive assessment of their involvement with IT-related privacy. For example, knowing that the Privacy Commissioner of Canada, the main advocate of Canadian privacy rights, has recently lost an unencrypted hard drive that contains salary information of their 800 current and former employees (CBC News 2014) can make Canadians objectively more concerned about their privacy. Hence, consistent with other IS scholars (e.g., Smith et al. 1996, Xu et al. 2012b), we suggest that general involvement with IT-related privacy will positively influence general PCIT (H3).

**Phase 2: Technology-Specific PCIT and the Cognitive Carry Over of General PCIT**

The second phase of the proposed research model explains the formation of technology-specific PCIT that occurs when individuals encounter a specific IT. Many IS studies that assessed technology-specific privacy concerns have incorporated the label of the specific IT they examined into their measures of general IT-related privacy concerns (e.g., Smith et al. 1996, Dinev and Hart 2004). For example, Xu et al. (2012b) replaced “companies” in Smith et al.’s (1996) measure with the term “mobile apps” and Jiang et al. (2013) used “chat room” and “my chat partner” to replace the wording in Malhotra et al.’s (2004) measure. However, the social and technological advancements of IT, such as the emergence of third-party assurance mechanisms, mandating privacy policy statements from websites and the prevalence of PET, allow the use of more pragmatic and feature-based measures to operationalize Technology-Specific PCIT proposed here. For example, to assess the privacy-friendliness of a specific website, individuals can adopt anti-tracking software and monitor all invisible cookies and beacons which track their e-behavior without their consent. Further, to examine the relationship between general PCIT and technology-specific PCIT,
Cognitive model of IT-related privacy concerns

using the same wording for both general and technology-specific PCIT items can confuse respondents and/or lead to method bias.

Comparing general and context-specific concerns for privacy, Xu et al. (2012a) suggested that the latter are based on “individuals’ assessment of privacy concerns” regarding a specific context. In the research model of Figure 1, this context can be any specific IT that possesses at least one of three privacy-related features that one can assess, including the IT-provider’s privacy policy, the privacy seals of a third-party, and PET analyses of the IT’s privacy-friendliness. It is important to note that only individuals who have cognitively formed a certain level of general PCIT might be able to form a technology-specific PCIT. This is mainly due to the unfamiliarity and inattentiveness of those who have low general PCIT levels to privacy-related features of a technology and their inability to analyze them. Technology-specific PCIT is defined here as individuals’ concerns about privacy-related features of a specific IT and conceptualized as a formative second-order construct that consists of the three following first-order constructs.

![Figure 1. A Two-Phase Cognitive Model of Individual PCIT](image)

**Concerns About the Reliability of the Specific IT Provider’s Privacy Policy**

This construct captures individuals’ concerns about the ambiguity, comprehensiveness and trustworthiness of the IT provider’s privacy policy. According to Turow et al. (2005), 75% of the American consumers they studied misunderstood the existence of a privacy policy statement and thought that their data would not be shared with a third-party and did not critically analyze the content of the privacy statement. Individuals with higher levels of general PCIT will be more likely to pay attention to the IT provider’s privacy policy and be more concerned about its reliability. So far, no study has yet conceptualized such a construct, and the cognitive carry-over from general PCIT is reflected in Figure 1 with the hypothesis that general PCIT will positively influence concerns about the reliability of the IT provider’s privacy policy (H4).

**Concerns About the Reliability of Third-Party Privacy Assurance**

Different certifying organizations, such as TRUSTe and BBBOnline, provide privacy seals for various IT, such as mobile applications, websites, and cloud services. This construct reflects individuals’ concerns about the transparency of the certification procedure and its criteria, as well as the accountability of the certifying organization. Individuals who have higher levels of general PCIT are likely to more readily recognize privacy seals and be more concerned about the reliability of third-party privacy assurance. Hence, it is hypothesized that general PCIT will positively influence concerns about the reliability of privacy seals (H5).
Concerns About the Reliability of PET

Rather than relying only on privacy assurance mechanisms that are out of their control, IT users have recently begun to adopt PET. Since 2007 the European Commission has been trying to increase individuals’ awareness of PET and their potential benefits (European Commission 2007). These efforts have resulted in PETs, such as ghostery and disconnect anti-monitoring software, which reveal certain privacy-related features of an IT, including invisible cookies, web bugs, beacons and all invisible information collection and behavior tracking mechanisms of a website. It is reasonable to think that individuals with higher levels of general PCIT will be more likely to adopt PET to analyze the privacy-friendliness of IT, such as websites. Yet, PETs themselves are a specific type of IT and may have their own privacy issues and performance errors. Hence, we suggest that general PCIT will positively influence concerns about the reliability of PET (H6).

Methodology

The present study’s conceptualization of the formation of technology-specific PCIT and its research model can be tested by applying a variety of research methods. As noted earlier, the constructs of the proposed model are new, except for e-behavior monitoring concerns and personal information concerns. To operationalize privacy-related IT knowledge, we intend to first interview IT scholars and practitioners who work in the privacy domain. To develop measures of privacy-related legal knowledge we plan to interview law scholars and practitioners whose interests cover IT, IT law, and privacy. The interview data will be analyzed to identify elements that can enable assessments of privacy-related IT and technology users’ legal knowledge as objectively as possible. We also intend to operationalize general involvement with IT-related privacy by closely monitoring various local and global IT-related privacy news and issues publicized in mass media and blogs with a view to developing an appropriate measure. These measures will then be refined and validated via interviews with a different set of practitioners and scholars. This will be followed by a pre-test survey to assess the validity of the developed measures and to further purify them. The three other constructs of the research model, i.e., concerns about the reliability of privacy policy, concerns about the reliability of third-party assurance mechanism and concerns about PET will be pre-tested and purified based on data gathered in a survey. Next, the revised measures will be administered to the participants of an experimental study designed to validate the second phase of the research model, as well as the cognitive carry-over effect of general ITC to the second phase. Before the experimental sessions, participants will be asked to respond to a survey that will assess the constructs of the first phase. Participants with both high and low general ITC will then be asked to execute a set of pre-defined tasks which will require them to use an IT. Their privacy-related behaviors, such as their level of attention to the privacy policy statement, to the privacy seal and their adoption of PET, will be closely monitored and analyzed. At the end of the experiment participants will be asked to respond to survey questions that will assess their concerns about the reliability of the privacy policy, third-party assurance mechanism and their concerns about PET. The collected data will then be used to test the study hypotheses, as well as to compare the behavior of participants with high and low levels of general ITC. The nomological validity of the proposed conceptualization of technology-specific PCIT will be further assessed by examining its relationship with several theoretically-related constructs, such as the participants’ behavior of sharing personal information.

Conclusion

Our review of the IS literature regarding 1) existing conceptualizations Privacy Concerns related to IT (PCIT) and 2) their antecedents suggests that, despite the advances made in past research, we still know little about PCIT’s antecedents (Junglas et al. 2008), formation, the relationship between general and technology-specific PCIT. In an effort to address these knowledge gaps, the present study adopted the Elaboration Likelihood Model (ELM) (Petty and Cacioppo 1986) as a theoretical lens to introduce three new constructs as key antecedents of general PCIT: privacy-related legal knowledge, privacy-related IT knowledge and general involvement with IT-related privacy. Relying on ELM’s theoretical explanations, the proposed research model helps explain the cognitive formation of technology-specific PCIT and sheds light on the potential relationship between general and technology-specific PCIT. An additional contribution is provided by the study’s feature-based conceptualization of technology-specific PCIT. Privacy is a highly dynamic concept (Solove 2002) and individuals with distinct life experiences and
knowledge can perceive it differently. As such, we hope that the present study can provide a useful first step in better understanding this complex concept, its antecedents, and its theoretical structure.
References


International Association of Privacy Professionals. 2014. “Outline of the body of knowledge for the certified information privacy professional/ information technology,” (https://www.privacyassociation.org/media/pdf/certification/CIPPIT_BOK_v.2.0.0.3.pdf)

Cognitive model of IT-related privacy concerns


