Journal of Business Ethics
https://doi.org/10.1007/s10551-019-04237-1

ORIGINAL PAPER

Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective

Weiyin Hong[1] · Frank K. Y. Chan[2] · James Y. L. Thong[1]

Received: 25 May 2018 / Accepted: 11 June 2019

Abstract
This paper investigates the drivers and inhibitors of Internet privacy concern. Applying the Multidimensional Development Theory to the online environment, we identify the important factors under four dimensions—i.e., environmental, individual, information management, and interaction management. We tested our model using data from an online survey of 2417 individuals in Hong Kong. The results show that the factors under all four dimensions are significant in the formation of Internet privacy concern. Specifically, familiarity with government legislation, Internet knowledge, benefit of information disclosure, privacy protection, and social presence reduce Internet privacy concern, while individuals' previous privacy invasion experience, risk avoidance personality, and sensitivity of information requested by websites increase Internet privacy concern. We conducted an analysis of unobserved heterogeneity to confirm the significance of these factors. A follow-up moderation analysis shows that the individual factors (i.e., previous privacy invasion experience, risk avoidance personality, and Internet knowledge) moderate the effects of the information management factor (i.e., information sensitivity) and the interaction management factors (i.e., privacy protection and social presence). The findings provide an integrated understanding of the formation of Internet privacy concern.

Keywords Internet privacy concern · Multidimensional development theory · Individual factors · Information management · Interaction management

Introduction

With the advances in Internet technologies, such as data mining tools, personalized marketing services, and ubiquitous electronic commerce applications, the collection and analysis of personal information are becoming rampant. Online consumers are increasingly concerned about their privacy, as their personal information and online activities are often automatically tracked and analyzed without their consent or knowledge (CIGI 2018; IDC 2017). Data breaches of large commercial databases, such as Facebook and Sony Pictures (Chaykowski 2018; Lewis 2014), also exacerbate consumers' privacy concerns. Such privacy concerns are further evident in the multimillion dollars lawsuits against Twitter (Roberts 2017), Facebook (Meyer 2017), and Google (Ruddick 2017). According to recent surveys, 91% of consumers agreed that they have lost control of their personal information and data (Rainie 2016), and 70% of consumers are more concerned about their privacy today than they were a few years ago (IDC 2017). The growing privacy concern has caused consumers to make serious changes in their behavior, such as closing social media accounts and making fewer online purchases (CIGI 2018). Hence, it is imperative for online companies to understand the drivers and inhibitors of individuals' privacy concerns so as to formulate strategies to alleviate such concerns.

Privacy concern has traditionally been a topic in business ethics research (e.g., Ashworth and Free 2006; Hajli and Lin 2016; Shaw 2003; Zhou and Piramuthu 2015). Specific to

✉ James Y. L. Thong
jthong@ust.hk

Weiyin Hong
whong@ust.hk

Frank K. Y. Chan
chanf@essec.edu

[1] Department of ISOM, School of Business and Management, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

[2] Department of Information Systems, Decision Sciences and Statistics, ESSEC Business School, 95021 Cergy Pontoise Cedex, France

Published online: 17 June 2019

the online context, Internet privacy concern (IPC) is defined as an individual's concern about possible loss of privacy due to voluntary or surreptitious information disclosure to websites (Dinev and Hart 2005). This definition of IPC is an extension of the traditional concept of information privacy concern, which refers to an individual's perception of fairness within the context of information privacy (Campbell 1997), to the online environment. In particular, IPC is viewed as a dyadic relationship between an individual and an online entity, which can either be a particular website or websites in general. Similar definitions have been adopted in prior research on IPC (e.g., Malhotra et al. 2004; Son and Kim 2008).

Although much research has been done on information privacy concerns in general and IPC in particular, most of the research has focused on the linkage between privacy concerns and outcomes, with little attention paid to the linkage between the antecedents[1] and privacy concerns (Smith et al. 2011). While some studies have examined factors that influence an individual's information privacy concern or IPC (e.g., Culnan and Bies 2003; Dinev and Hart 2004; Hann et al. 2007; Phelps et al. 2001; Ward et al. 2005), the goal of identifying the critical antecedents of IPC remains elusive due to the many external, internal, and situation-specific factors that can potentially influence IPC. For example, the legal and cultural environments can influence what an individual perceives as fair or not fair (Bellman et al. 2004; Caudill and Murphy 2000; Milberg et al. 2000). Meanwhile, an individual's perception of such external conditions can vary with personal characteristics (Chen et al. 2001; Phelps et al. 2000; Sheehan 2002) and past experience (Awad and Krishnan 2006). In summary, although previous studies have investigated the relationships between a number of antecedents and privacy concerns, these studies have usually been conducted in a disjointed manner (Smith et al. 2011). Therefore, there is a need for a comprehensive theoretical framework to guide a systematic identification and examination of the antecedents of IPC, which is a major stream of privacy research (Popovic et al. 2017).

Accordingly, our objective is to provide a comprehensive investigation of the drivers and inhibitors of IPC. First, we use the Multidimensional Development Theory (MDT; Laufer and Wolfe 1977) to guide our investigation. The MDT suggests that an individual's privacy concern is jointly determined by factors pertaining to four dimensions—i.e., environmental, individual, information management, and interaction management. The MDT was previously used to examine the conceptualization and measurement of IPC, particularly addressing the question of what IPC is (Hong and Thong 2013). We extend this line of research by using the MDT to study the antecedents of IPC, addressing the broader question of how IPC is formed or influenced by a variety of sources. We use the multidimensional conceptualization to guide our literature review and organize prior research findings on the antecedents of privacy concerns. Second, we formulate and empirically test a research model that incorporates key factors under each dimension of MDT. The results, based on a sample of 2417 respondents to an online survey conducted in Hong Kong, provide support for the significance of all four dimensions of MDT in affecting IPC. Finally, we validate our model by examining the unobserved heterogeneity in our sample (Becker et al. 2013; Esposito Vinzi et al. 2008). The analysis of unobserved heterogeneity confirms our findings and leads us to propose a refinement of the MDT by considering the interactions between the individual dimension and other dimensions. A follow-up moderation analysis confirms such interactions, thus providing a more nuanced and contextual understanding of the different drivers and inhibitors of IPC (Hong et al. 2014).

This study makes several contributions. Theoretically, this study demonstrates the utility of the MDT in understanding specific drivers and inhibitors of IPC, and it also refines the MDT by identifying its boundary conditions. Empirically, this study utilizes a large sample to validate the significance of the key antecedents of IPC, and it also illustrates the importance of incorporating unobserved heterogeneity into the analysis and validation. Practically, the findings will provide actionable and prescriptive advice to online companies regarding the management of users' IPC.

Theoretical Background

Literature Review

In a review of information privacy research, Smith et al. (2011) presented a macro level (APCO) model (Antecedents → Privacy Concerns → Outcomes) that considers a number of antecedents and outcomes associated with privacy concerns. They classified previously studied antecedents of privacy concerns into five dimensions: privacy experience, privacy awareness, personality differences, demographic differences, and culture/climate. They noted that past studies have investigated only the relationships between some selected antecedents and privacy concerns. Further, these relationships have not been confirmed through repeated studies and are thus tenuous.

To supplement Smith et al.'s (2011) APCO model, we conducted a more focused literature review of the antecedents of IPC and its closely related constructs—i.e., information privacy concern, consumer privacy concern, and

[1] In this paper, the term "antecedents" is used interchangeably with the terms "drivers" and "inhibitors".

employee privacy concern. As personal information of consumers and employees can be collected through the Internet, both consumers' and employees' perspectives are relevant to IPC and were included in our review. The reference disciplines covered in our literature review include information systems, marketing, public policy, management, and social science.

Our literature review reveals four major observations. Firstly, a variety of theories have been used in prior studies, such as utility maximization theory (Awad and Krishnan 2006; Hui et al. 2007), social contract theory (Martin 2016; Phelps et al. 2000; Singh and Hill 2003; Xu et al. 2005), justice theory (Ashworth and Free 2006), and protection motivation theory (Youn 2005). The majority of the theories are built upon the concept of "privacy calculus", which refers to the cost-benefit analysis that individuals perform when balancing the trade-offs between the cost of providing personal information and the benefit of information disclosure (Culnan and Armstrong 1999; Culnan and Bies 2003; Klopfer and Rubenstein 1977; Stone and Stone 1990). For example, the principle of the utility maximization theory (Awad and Krishnan 2006; Hui et al. 2007) is to maximize the total utility or satisfaction by an individual. The theory depicts the utility function of information disclosure as the difference between expected benefits (such as monetary incentive and personalized service) and expected costs (such as consumer privacy concerns and risks), and suggests an optimal point between the two, which determines the amount of information the individual is willing to disclose (Li 2012). Moreover, the privacy calculus (or cost-benefit analysis) is subject to further adjustment. The social contract theory suggests that the provision of personal information to an online merchant involves not only an economic exchange (i.e., purchasing goods and service) but also a social exchange (i.e., establishing relationships) (Li 2012). A social contract governs the information exchange and involves an implicit assessment of exchange fairness, i.e., the degree of fairness of information exchange involving whether the personal information is collected fairly and, will subsequently be used fairly (Li et al. 2011). An individual's understanding or implicit assessment of the fairness of information exchange will adjust the cost-benefit analysis (Culnan and Bies 2003). The justice theory suggests that fairness perceptions can have a positive effect on an individual's privacy decision making, which leads to a positive outcome of their privacy calculus and a greater willingness to disclose personal information (Xu et al. 2009). Despite its popularity in information privacy research, the privacy calculus framework does not account for the fact that privacy concern is developed over a long period of time as a result of interaction between the environment, the individual, and the social exchange situation (Laufer and Wolfe 1977; Marshall 1974; Weigel-Garrey et al. 1998). Some alternative theoretical perspectives, such as the protection motivation theory (Junglas et al. 2008),[2] have been adopted to study IPC from a set of factors that focus on users' perceived severity of privacy threats and their perceived ability to protect themselves from such threats. Given the multiple theories that focus on different aspects of IPC drivers and inhibitors, we suggest that a more comprehensive and complementary framework is necessary to gain a more complete understanding of the antecedents of IPC.

The second observation is much prior research has focused on conceptualizing and measuring information privacy concerns and IPC (e.g., Hong and Thong 2013; Liu et al. 2005; Malhotra et al. 2004; Smith et al. 1996; Son and Kim 2008; Stewart and Segars 2002), while there is a lack of general understanding of the antecedents of IPC. IPC has been conceptualized as a multi-facet construct that consists of multiple underlying dimensions (e.g., collection, secondary usage, errors, improper access, etc.) modeled using a variety of factor structures (i.e., first-, second-, or third-order; see Hong and Thong 2013 for a review). While previous studies have confirmed the predictive validity of IPC and reached a consensus on its effect on important dependent variables, such as trusting beliefs, risk beliefs, and complaining actions (e.g., Hong and Thong 2013; Malhotra et al. 2004; Son and Kim 2008), there is a lack of general understanding of the antecedents of IPC. Existing studies on the antecedents of IPC were done on a case-by-case basis (Smith et al. 2011), with some studies focusing on general factors, such as benefit of information disclosure, perceived vulnerability and perceived control (e.g., Ashworth and Free 2006; Dinev and Hart 2004; Hajli and Lin 2016), and some focusing on the context- or technology-specific factors, such as use of privacy protection tools, inclusion of privacy policy statement, provision of privacy enhancing features (e.g., Culnan and Bies 2003; Singh and Hill 2003; Son and Kim 2008; Xu et al. 2011a). While these disjointed findings provide useful insights, it is necessary to consolidate the findings and present an integrated framework to provide a general understanding of the key factors for managing privacy concerns.

The third observation is prior empirical studies on the determinants of IPC may over-represent experienced Internet users, by soliciting subjects through emails (e.g., Bellman et al. 2004; Chen et al. 2001; Sheehan 2002), or targeting at students and IS professionals (e.g., Chen et al. 2001; Hui et al. 2007; Milberg et al. 1995). As a result, the privacy concerns of some population groups, such as less-experienced Internet users or non-students and non-IS professionals,

[2] Protection motivation theory proposes that individuals protect themselves based on their perceptions of: severity of, vulnerability to the threat, response efficacy (i.e., belief that implementing a behavioral response will reduce the threat), and self-efficacy (i.e., belief in one's ability to perform the behavioral response) (Li 2012).

have not been adequately studied. Some researchers have called for more balanced samples collected from the general population when studying IPC (Phelps et al. 2000; Ward et al. 2005). Further, the sample sizes in previous studies are typically around a few hundred, which limits the number of independent variables that can be simultaneously examined in a single study. There is a need for large-scale surveys which allow simultaneous investigation of a larger set of independent variables to determine and compare their impacts on IPC.

The fourth observation is most of the existing surveys were conducted on samples from western cultures, such as the US, Europe, and Australia (Rose 2006; Sheehan and Hoy 2000; Singh and Hill 2003). There are very few large-scale surveys published in peer-refereed journals using Asian samples (see Hong and Thong 2013). Prior literature suggests that cultural differences affect what people perceive as private and lead to different levels of privacy concern (Bellman et al. 2004; Harris et al. 2003; Milberg et al. 2000; Pavlou 2011). It is widely accepted among social scientists that the Asian culture differs from the western culture on many dimensions, including power distance, individualism, masculinity, and uncertainty avoidance (Hofstede et al. 2010). For example, as Asian cities are typically more crowded, people are used to others intruding into their personal space and being observed by others,[3] which may lead to lower levels of privacy concern perceptions (Westin 2003). The results of our study will help to validate prior findings from a western culture to an Asian culture with very different values.

Multidimensional Development Theory

The multidimensional development theory (MDT) proposed by Laufer and Wolfe (1977) provides a comprehensive description of multidimensional factors that influence an individual's perception of privacy and privacy invasion. According to the MDT, any privacy situation can be described in terms of four dimensions—i.e., environmental, individual, information management, and interaction management[4]—building on the recognition that an individual's privacy concern is a result of environmental influences, the individual's experience, and the interaction between the individual and other parties involved in the privacy situation. Thus, the MDT can provide a more comprehensive understanding of the antecedents of privacy concerns than other theories that are primarily based on the concept of privacy calculus (e.g., utility maximization theory). Next, we will elucidate the details of MDT and describe how it can be applied to the online setting together with a summary of relevant antecedents of IPC that have received theoretical or empirical support in the literature.

The environmental dimension refers to elements that act as boundaries of privacy meaning and experience. The environmental elements critically influence an individual's ability to perceive, have, and use available privacy options. For example, different government legislations provide different levels of privacy protection, and online privacy protection in particular (Caudill and Murphy 2000; Sarathy and Robertson 2003; Singh and Hill 2003; Westin 2003). These regulatory settings define, evoke, and sustain behaviors that are private. We summarized the environmental factors identified in prior studies as antecedents of IPC or its closely related constructs (see Table 4 of Appendix A). Government legislations, industry self-regulations, and culture values have been identified as three major environmental factors that affect an individual's perception of IPC. First, government legislations aimed at providing individuals with better control of their personal data can help to reduce privacy concern. For example, the Federal Trade Commission has implemented the Children's Online Privacy Protection Act to protect online privacy of children (Sarathy and Robertson 2003). Second, industries may develop rules and enforce procedures that protect consumers' privacy (Culnan and Bies 2003; Sarathy and Robertson 2003). Such industry self-regulations are typically provided by a particular company or an alliance of companies. Third, culture values such as individualism, uncertainty avoidance, and communication patterns have been found to be related to differences in privacy perceptions (e.g., Milberg et al. 2000; Miltgen and Peyrat-Guillard 2014).

The individual dimension refers to the influence of an individual's developmental process on his or her concept of privacy. The developmental experience of being capable of functioning independently adds a critical aspect to the relationship between the self and privacy. This dimension also reflects the fact that claims of privacy are shaped and asserted by each individual in daily life, as a function of one's education, past experience, and psychological makeup (Westin 2003). We summarized the individual factors identified in prior studies as antecedents of IPC or its closely related constructs (see Table 5 of Appendix A). Following Westin (2003), we classified the individual factors identified in prior literature into three categories. The first category

[3] Asians are used to high-density living conditions (e.g., small homes, crowded subways, etc.) and are more tolerant of noise and crowding than Westerners (Gillis et al. 1986). Thus, Asians may be more tolerant of being closely observed by others and lower privacy (e.g., Wang and Lau 2013).

[4] The individual dimension is an extension of the original self-ego dimension in the MDT. This dimension includes, in addition to an individual's experience, other individual-related factors suggested by Westin (2003), such as individual traits and demographics. Information management and interaction management are related dimensions that describe how an individual manages his or her interpersonal interaction with others.

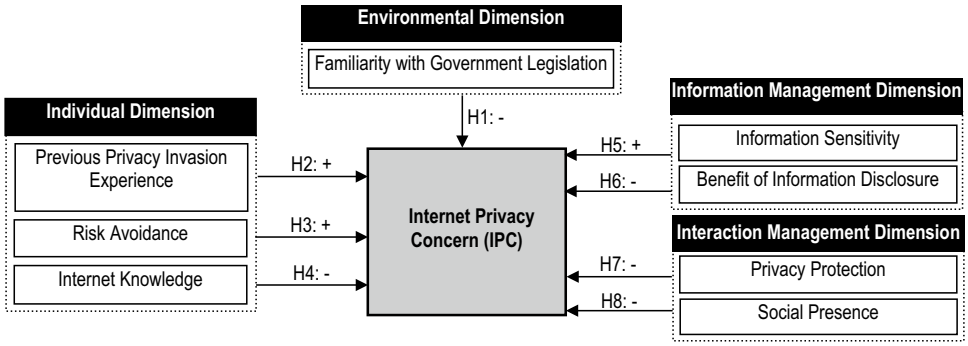

Fig. 1 Research model

represents past experience, such as previous privacy invasion experience (e.g., Awad and Krishnan 2006; Xu et al. 2012). The second category includes psychological and personality traits, such as risk avoidance, trust propensity, personality, etc. (e.g., Smith et al. 1996; Xu et al. 2005). The third category represents demographic variables, including age, gender, education, income, and Internet literacy (e.g., Chen et al. 2001; Sheehan 2002).

In addition, the MDT suggests that an individual's concept of privacy rights and rules is incrementally formed through interactions with other parties involved in privacy situations. All forms of privacy assume the existence of others and the possibility of a relationship with them. The acting out of this relationship has two elements: information management and interaction management (Laufer and Wolfe 1977). Information management refers to the management of information disclosure by balancing benefits and risks, whereas interaction management refers to the management of social interaction among individuals or between individuals and their socio-physical environment. We adapt these two concepts to the online environment. The information management dimension largely reflects the "privacy calculus" concept discussed earlier (Culnan and Armstrong 1999; Dinev and Hart 2006a). It refers to the recognition of the intrinsic tradeoff between the benefits derived from disclosing personal information to websites and the risks of privacy loss from the disclosure. We summarized the information management factors identified in prior studies as antecedents of IPC or its closely related constructs (see Table 6 of Appendix A). As expected, the benefit of information disclosure and the risk of information sensitivity have been extensively studied in prior literature (e.g., Andrade et al. 2002; Ashworth and Free 2006; Jiang et al. 2013; Miller and Weckert 2000; Phelps et al. 2000; Xu et al. 2011b); they represent the benefit and risk sides of an online information exchange respectively.

The interaction management dimension reflects the efforts of optimizing the exchange mechanism, so that individuals have more control of the information exchange situation and better ability to make the benefits-risks tradeoffs (Milne 2000). In the online environment, interaction management can be done through either the direct approach or the indirect approach. We summarized the interaction management factors and classified them into these two categories (see Table 7 of Appendix A). The direct approach refers to the technical implementations on websites with the observable purpose of reducing privacy concern, such as the use of privacy seals, authorization form for information release, inclusion of privacy statement, and provision of privacy enhancing features. (Culnan and Bies 2003; Singh and Hill 2003; Turner and Dasgupta 2003; Xu et al. 2011a). On the other hand, the indirect approach refers to the subtle measures that websites can adopt to reduce privacy concern, such as increasing the reputation of the website or the degree of human element (i.e., social presence) through the Web interface design (Eastlick et al. 2006; Pavlou et al. 2007; Xie et al. 2006).

Research Model

By applying the MDT in our literature review, we identified four dimensions that can impact individuals' IPC. As our primary objective is to test the utility of MDT in identifying the important antecedents of IPC, rather than to investigate all possible antecedents in a single study, we select the more prominent factor(s)[5] from each dimension of MDT to develop our research model (see Fig. 1).

Environmental Dimension

Under the environmental dimension of MDT, we identify familiarity with government legislation which has received the strongest theoretical and empirical support in prior research involving environmental factors. We exclude industry self-regulation and culture values as it is not the objective of this study to compare IPC across industries and countries.

[5] We also conducted a focus group discussion with seven Internet users to confirm the relevance of the selected factors.

Familiarity with Government Legislation refers to an individual's familiarity with government regulations and laws addressing privacy protection (Culnan and Bies 2003). Most governments have introduced privacy legislations and laws in order to protect privacy.[6] Prior research suggested that the implementation of privacy legislations provides individuals with control over their personal data, which can help to reduce privacy concern (Caudill and Murphy 2000; Culnan and Bies 2003; Sarathy and Robertson 2003; Xu and Teo 2004). When strict regulations are in place regarding personal information handling practices, individuals' level of privacy concern may relax due to the reduced number of privacy violations (Bennett 1992). Thus, we hypothesize that individuals who are familiar with government legislations are likely to have lower levels of IPC (H1).

Individual Dimension

Under the individual dimension of MDT, we identify one key antecedent from each of the three sub-dimensions. Specifically, previous privacy invasion experience is selected as a past experience factor as it best describes an individual's past experience that may raise privacy concern. Among the many personality factors, risk avoidance is selected as it has consistent empirical support from prior research. Similarly, Internet knowledge is selected as a prominent demographic factor as it has received more research attention and empirical support than the other demographic variables.

Previous Privacy Invasion Experience refers to previous personal experience of privacy invasion (Smith et al. 1996). Prior research showed that individuals vary in their concern for privacy based on life experiences (Culnan and Armstrong 1999; Singer et al. 1993). In particular, an individual's previous privacy invasion experience plays an important role in shaping the person's privacy concern (Culnan 1993; Smith et al. 1996; Stone and Stone 1990). If an individual had been a victim of privacy invasion before, the person is more likely to develop privacy concern due to the fear that the bad experience will recur. Prior research has found a positive relationship between past privacy invasion experience and IPC or reluctance to disclose personal information in the online environment (Bansal et al. 2010; Smith et al. 1996; Xu et al. 2012). Hence, we hypothesize that previous privacy invasion experience will increase IPC (H2).

Risk Avoidance is a personality characteristic that describes an individual's current tendency to take or avoid risks (Sitkin and Weingart 1995). The release of personal information is typically regarded as risky by individuals as they become vulnerable to a company's potential opportunistic behaviors (Laufer and Wolfe 1977; Milne and Gordon 1993). The provision of personal information for services and goods can be viewed as an exchange between individuals and websites. Individuals have little control over how their information will be processed by websites after the exchange. Thus, individuals with higher risk avoidance are more likely to develop stronger IPC as compared to individuals with lower risk avoidance due to the uncertainty and lack of control in online environment. Empirical evidence from prior research also supports the positive relationship between risk avoidance and IPC (Dinev and Hart 2005; Xu et al. 2005). Hence, we propose that risk avoidance has a positive effect on IPC (H3).

Internet Knowledge refers to an individual's perception of their knowledge about the Internet and its related privacy issues (Harris et al. 2003). Individuals having more Internet knowledge are expected to have accurate privacy perceptions (Harris et al. 2003). Internet knowledge is often believed to have a significant impact on privacy concern. However, findings about this variable in the literature are mixed. On the one hand, Internet knowledgeable individuals may have less privacy concern because they are more skillful at protecting their online privacy. On the other hand, they may be more concerned because they are more aware of the potential threats posed by the Internet. The majority of prior studies have shown that Internet knowledge helps to reduce IPC (Dinev and Hart 2005; Harris et al. 2003; Miyazaki and Fernandez 2001; Rose 2006), but some studies found no significant correlation between Internet knowledge and privacy concern (e.g., Sheehan 2002; Ward et al. 2005), or even a positive relationship between Internet knowledge and privacy concern (e.g., Hoffman et al. 1999). In line with the majority of prior research, we propose that greater Internet knowledge helps to reduce IPC (H4).

Information Management Dimension

Under the information management dimension of MDT, information sensitivity and benefit of information disclosure are the two antecedents that have extensive theoretical and empirical support. They represent the risk and benefit sides of the "privacy calculus" concept respectively.

Information Sensitivity is defined as the level of privacy concern an individual feels for a type of data in a specific situation (Sheehan and Hoy 2000); it represents the "risk" side of the "privacy calculus" concept. Personal information can be classified into different categories, from less sensitive information, such as demographic data, lifestyle interests,

[6] In the U.S., some legislations, including the Privacy Act (1974), the Computer Matching and Privacy Act (1988), and the Telecommunications Act (1996), were introduced to restrict the collection, use, and dissemination of personal information. In Europe, the Council of Europe passed stricter rules that protect personal data from both the private and public sectors. In Asia, for example, Hong Kong has implemented privacy laws that are similar to that in Europe.

and media habits, to more sensitive information, such as personal identification data (i.e., name, address, phone number, and social security number) and financial data (Phelps et al. 2000). The more sensitive the data collected by companies, the higher the risk that individuals are exposed to in case the data are misused. Prior research has found that privacy concern increases as the sensitivity of personal information submitted to websites increases (Andrade et al. 2002; Ashworth and Free 2006; Dinev and Hart 2006b; Dinev et al. 2013; Rohm and Milne 2004; Ward et al. 2005). Hence, we hypothesize that information sensitivity has a positive effect on IPC (H5).

Benefit of Information Disclosure is defined as the benefits that individuals retain from information disclosure, such as monetary savings, time saving, self-enhancement, social adjustment, pleasure, novelty, and altruism (Hui et al. 2006). It represents the "benefit" side of the "privacy calculus" concept. Nowak and Phelps (1997) found that in traditional direct marketing situations, individuals often willingly supply personal information in expectation of future benefits, such as reduced prices, premiums, or other incentives. Similarly, Phelps et al. (2000) suggested that privacy concerns can be alleviated if marketers offer benefits in exchange for personal details, which is supported by the majority of empirical findings in prior research (Dinev et al. 2013; Hann et al. 2007; Ward et al. 2005; Xu et al. 2011b). Hence, we hypothesize that benefit of information disclosure helps to reduce IPC (H6).

Interaction Management Dimension

Under the interaction management dimension of MDT, we identify privacy protection as a salient direct approach, and social presence as an important indirect approach to interaction management of IPC. Although prior research has found reputation of the website to be also a salient factor, it is excluded due to practical relevance because it is less subject to manipulation through the Web interface design.

Privacy Protection refers to the technical solutions and practices that are adopted by websites to protect online users' privacy (Culnan and Bies 2003). In order to reduce individuals' privacy concern, websites have adopted many privacy protection practices and tools. These include seeking users' authorization before release of their personal information (Culnan and Bies 2003; Eastlick et al. 2006; Singh and Hill 2003), inclusion of privacy policy statements on the websites (Awad and Krishnan 2006; Hui et al. 2007; Pollach 2005; Resnick and Montania 2003; Tsai et al. 2011; Turner and Dasgupta 2003), utilization of privacy protection seals such as TRUSTe (Caudill and Murphy 2000; Etzioni 2019; Hui et al. 2007; Singh and Hill 2003; Xu et al. 2005), ensuring users' awareness of information collection (Culnan and Bies 2003; Sheehan 2002; Sheehan and Hoy 2000; Singh and Hill 2003), and removing identifiable personal information from databases (Garfinkel et al. 2007; Li and Sarkar 2006). In general, prior research has found that privacy protection is effective in reducing IPC (Xu et al. 2011a). Thus, we hypothesize that privacy protection can help to reduce IPC (H7).

Social Presence is defined as the extent to which a medium, e.g., a website, is perceived as truly conveying the presence of the communicating participants, e.g., the presence of a seller behind the website (Pavlou et al. 2007; Rice 1993; Short et al. 1976). One major disadvantage of e-commerce is the lack of face-to-face interaction. By creating an online environment that closely resembles a physical interaction with a seller, social presence helps to bring a website closer to its consumers (Choi et al. 2001). And closing the social distance between buyers and sellers may help to reduce IPC, which is partly a result of separation between online buyers and sellers. Thus, we hypothesize that social presence on websites has a negative effect on IPC (H8).

Methodology

Our research context was set in Hong Kong, which is one of the most connected cities in the world. According to the report by the Census and Statistics Department of Hong Kong (2018), 100% of population is covered by mobile cellular telephone network and public Internet access. 80.2% of households have personal computers (PCs) at home connected to the Internet and 88.6% of people aged 10 and above have smartphones. The majority of people in Hong Kong (89.4%) used the Internet during the last 12 months. Among these people, they used either PCs (88.3%) or smartphones (98.1%) to access the Internet.

In terms of culture, Hong Kong can be characterized using Hofstede et al. (2010)'s cultural dimensions, including power distance, individualism, masculinity, uncertainty avoidance, long-term orientation, and indulgence (Table 1). Hofstede Insights (2018) indicate that (1) Hong Kong people are willing to accept unequally distributed power in institutions and organizations (high score of 68 on power distance), (2) Hong Kong has a collectivist culture where people act in the interests of the group (low score of 25 on individualism), (3) Hong Kong is somewhat a masculine society that is success oriented and driven (moderate score of 57 on masculinity), (4) Hong Kong people are comfortable with ambiguity (low score of 29 on uncertainty avoidance), (5) Hong Kong has a pragmatic culture where people show an ability to adapt traditions easily to changed conditions (high score of 61 on long-term orientation), and (6) Hong Kong people are restrained and control the gratification of their desires (low score of 17 on indulgence). Overall, Hong Kong is notably different from western countries (e.g., United

Table 1 Hofstede's scores for selected countries (Hofstede Insights 2018)

Country	Power distance	Individualism	Masculinity	Uncertainty avoidance	Long-term orientation	Indulgence
Argentina	49	46	56	86	20	62
Brazil	69	38	49	76	44	59
China	80	20	66	30	87	24
France	68	71	43	86	63	48
Germany	38	67	66	65	83	40
Hong Kong	68	25	57	29	61	17
Indonesia	78	14	46	48	62	38
Italy	50	76	70	75	61	30
Japan	54	46	95	92	88	42
South Korea	60	18	39	85	100	29
Taiwan	58	17	45	69	93	49
Thailand	64	20	34	64	32	45
United Kingdom	35	89	66	35	51	69
United States	40	91	62	46	26	68
Vietnam	70	20	40	30	57	35

States, United Kingdom, Germany, and France) on many cultural dimensions, while it is quite comparable with other Asian countries (e.g., China, South Korea, Thailand, and Vietnam) (see Table 1).

In 2014, we posted a banner advertisement of our survey on a popular local website. At the time of the survey, this website allowed people to schedule appointments with government agencies and booking community services, such as recreational facilities. Hence, our sampling frame included both potential and existing users of the Internet, and also both experienced and novice Internet users. A lucky draw to win mobile phones that was restricted to those aged 18 years and above was used as an incentive to encourage participation in the survey. A total of 2417 valid responses were collected over a one-month period. Our final sample consisted of 43.3% males and 56.7% females. Their age ranged from 18 to 60 years. The majority of respondents had a bachelor degree (40.2%), a high school diploma (28.2%), or a vocational school certificate (16.5%). Their monthly income ranged from 0 (unemployed) to more than HK $30,000 with a mean income of HK$10,000. There was a wide spectrum of occupations, including senior management (5.3%), professionals (20.4%), clerical staff (21.5%), professional assistants (7.8%), sales assistants (6.4%), students (22.3%), and others (including factory workers, farmers, and fishermen). Their Internet experience ranged from less than 1 year to more than 11 years, with a mean of 7.5 years and a standard deviation of 2.3 years. Their average weekly Internet usage was 22.5 h, with the majority of the sample (47%) reporting their weekly usage under 15 h. Finally, 44.6% of respondents had previously provided personal information (e.g., name, email address, credit card number, etc.) to commercial websites (e.g., Amazon.com) for online shopping or payment. In summary, our sample is diverse in terms of respondents' demographic and Internet usage.[7]

We used established instruments whenever possible to measure the constructs (see Appendix B). A seven-point Likert scale with anchors ranging from 'strongly disagree' to 'strongly agree' was used for all constructs, except for previous privacy invasion experience which used a seven-point Likert scale with anchors ranging from "not at all" to "very much". IPC, the dependent variable, was conceptualized as a third-order construct with two second-order constructs (i.e., interaction management and information management) and six first-order constructs (i.e., collection, secondary usage, errors, improper access, control, and awareness), following Hong and Thong's (2013) conceptualization. We measured the six first-order constructs with three items each, adapted from Hong and Thong (2013). A sample item for collection is "It usually bothers me when websites ask me for personal information." A sample item for secondary usage is "I am concerned that when I give personal information to a website for some reason, the website would use the information for other reasons." A sample item for errors is "I am concerned that websites do not take enough steps to make sure that my personal information in their files is accurate." A sample

[7] We compared the demographics of our sample to the government census data of 2016 on Hong Kong's population. There was no significant difference in terms of gender (Chi-square, $p>0.05$), but our sample was relatively younger and more educated, and had lower income than the population average (Chi-square, $p<0.05$). Nevertheless, our sample was closely representative of the active adult Internet users in Hong Kong, who were aged between 25 and 44. 99% of users in this age group accessed the Internet every day (vs. the global median at 29%) (Statista 2016).

item for improper access is "I am concerned that databases that contain my personal information are not protected from unauthorized access." A sample item for control is "It usually bothers me when I do not have control of the personal information that I provide to websites." A sample item for awareness is "It usually bothers me when online privacy policy does not have a clear and conspicuous disclosure."

As for the independent variables, familiarity with government legislations was measured by two newly-developed items. A sample item is "I am fully aware that the Hong Kong government has a Privacy Policy to protect my privacy." Previous privacy invasion experience was assessed by two items used in prior studies (Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2005). A sample item is "How often have you personally experienced incidents whereby your personal information was used by some website without your authorization?" We used three items from Xu et al. (2005) to measure the individual's risk avoidance. A sample item is "I would rather be safe than sorry." Internet knowledge was measured by two items adapted from Singh and Hill (2003). A sample item is "I am knowledgeable about the Internet and its related privacy issues." For the information and interaction management factors, in line with Hong and Thong's (2013) general conceptualization of IPC, we measured user perceptions towards websites in general, rather than towards a specific website. Information sensitivity and benefit of information disclosure were typically manipulated in prior studies (e.g., Malhotra et al. 2004; Phelps et al. 2000; Sheehan and Hoy 2000). We developed two items each for these two constructs by closely following their definitions. A sample item for information sensitivity is "Websites tend to ask me for sensitive personal information in order to obtain their services." A sample item for benefit of information disclosure is "I value the benefits that I can obtain by providing my personal information to websites." Popular privacy protection practices adopted by websites include seeking authorization before collecting personal information, provision of privacy protection tools, privacy statements, and informing individuals of personal information collection (Awad and Krishnan 2006; Hui et al. 2007; Singh and Hill 2003). Based on these popular practices, we created a four-item instrument for privacy protection. A sample item is "In general, websites would ask for my authorization before collecting my personal information." Finally, social presence was measured by three items taken from Pavlou et al. (2007). A sample item is "There is a sense of human contact in websites." The survey was delivered in Chinese, the main lingua franca in Hong Kong. The original measurement items (in English) were translated to Chinese and back-translated to English by professional translators. Minor wording discrepancies were discussed and resolved. The measurement scales were then pilot tested on 318 subjects drawn from the general population through an online survey. Analysis of the pilot test data confirmed that the scales were reliable and valid. We then proceeded with the main data collection.

Data Analysis

We used partial least squares (PLS), a component-based structural equation modeling (SEM) technique, to analyze our data. We chose PLS for multiple reasons. First, PLS can handle higher-order constructs and complex models with fewer restrictions than covariance-based techniques (Ringle et al. 2012; Ruiz-Palomino and Martinez-Cañas 2011). PLS is appropriate for testing our complex model with eight independent variables and one third-order dependent variable that consists of eight underlying dimensions (i.e., IPC). Second, PLS is suitable for studies that aim to examine the predictive power of the exogenous variables on the endogenous variables (Peng and Lai 2012). Given that the objective of our work is to consolidate previous disjointed findings and examine a comprehensive list of antecedents of IPC, PLS is an appropriate tool as it is prediction-oriented (Hair et al. 2011). Third, given our large sample, some spurious relationships may be found. PLS allows the use of some advanced analytical approaches to validate our results. In particular, we used the analysis of unobserved heterogeneity (Becker et al. 2013; Esposito Vinzi et al. 2008) to confirm the significance of our proposed factors. Finally, we acknowledge that there is a debate on the use of PLS. Previous simulation studies showed that the differences between PLS and covariance-based SEM (e.g., LISREL, AMOS) estimates are very small (e.g., Goodhue et al. 2012; Reinartz et al. 2009). The results of PLS and covariance-based SEM will be similar, provided that the sample size is large and a large number of indicator variables are used to measure the latent constructs (Hair et al. 2011), which is true in our case. To alleviate the concern of biased estimates, we also tested our model using LISREL. The LISREL results were consistent with the PLS results.

Table 2 presents descriptive statistics and correlations for all the constructs. For all constructs, both Cronbach's alpha and composite reliability were above 0.70, indicating the constructs had adequate reliability. The average variance extracted (AVE) for each construct was greater than the recommended 0.50 level, and the correlations between constructs were all below the square root of AVE of either construct. Also, we conducted a confirmatory factor analysis for all constructs. Appendix C showed that all factor loadings were above 0.7 and all cross-loadings were low, thus supporting convergent and discriminant validity of the scales (Fornell and Larcker 1981). Finally, we used the repeated indicators approach (Wetzels et al. 2009; Wijethilake et al. 2018) to model IPC as a third-order construct, following

Table 2 Descriptive statistics and correlations

Construct		Mean	SD	CA	CR	1	2	3	4	5	6	7	8	9
1	Familiarity with government legislation	4.08	1.08	0.75	0.89	(0.89)								
2	Previous privacy invasion experience	2.33	1.43	0.88	0.94	−0.02	(0.95)							
3	Risk avoidance	4.80	0.93	0.76	0.86	0.04*	0.04	(0.82)						
4	Internet knowledge	3.77	1.05	0.76	0.89	0.39***	0.01	0.06**	(0.88)					
5	Information sensitivity	4.21	1.04	0.92	0.96	0.09***	0.22***	0.19***	0.07***	(0.96)				
6	Benefit of information disclosure	3.57	1.01	0.90	0.95	0.20***	−0.18***	−0.12***	0.16***	−0.06**	(0.95)			
7	Privacy protection	4.89	0.90	0.80	0.87	0.24***	−0.32***	−0.01	0.13***	−0.07***	0.29***	(0.77)		
8	Social presence	3.28	1.03	0.84	0.91	0.23***	−0.11***	−0.06**	0.18***	−0.06**	0.39***	0.29***	(0.87)	
9	Internet privacy concern	4.94	1.00	0.96	0.97	−0.13***	0.34***	0.31***	−0.11**	0.41***	−0.35***	−0.25***	−0.35***	(0.79)

SD standard deviation, *CA* Cronbach's alpha, *CR* composite reliability, square root of average variance extracted (AVE) shown on diagonal

Hong and Thong's (2013) conceptualization. This helps to reduce the complexity of the structural equation model by reducing the number of relationships between IPC and its antecedents (Wijethilake et al. 2018). All loadings of the sub-constructs on the higher-order constructs exceeded 0.80 and were significant at $p < 0.001$. In summary, the measurement model demonstrated adequate reliability, convergent validity, and discriminant validity.

Figure 2 presents the results of the hypotheses testing.[8] Specifically, familiarity with government legislation reduced IPC ($\beta = -0.05$, $p < 0.05$), supporting H1. Both previous privacy invasion experience ($\beta = 0.20$, $p < 0.001$) and risk avoidance ($\beta = 0.22$, $p < 0.001$) increased IPC, supporting H2 and H3. Internet knowledge reduced IPC ($\beta = -0.07$, $p < 0.001$), supporting H4. Further, IPC was higher when individuals perceived the information required as more sensitive ($\beta = 0.31$, $p < 0.001$), and was lower when individuals perceived the benefit of information disclosure as high ($\beta = -0.16$, $p < 0.001$), supporting H5 and H6. Finally, both privacy protection ($\beta = -0.04$, $p < 0.05$) and social presence on websites ($\beta = -0.21$, $p < 0.001$) reduced IPC, supporting H7 and H8. The variance explained was 42%.

Prior research has noted that unobserved heterogeneity in structural equation models may pose a threat to the validity of findings and lead to misinterpretations and invalid conclusions (Becker et al. 2013; Esposito Vinzi et al. 2008). To validate our findings, we conducted an analysis of unobserved heterogeneity (see Appendix D). The results showed that, despite the existence of heterogeneous segments in our sample, all of the factors (except for Internet knowledge and privacy protection) had significant, consistent (either positive or negative) effects on IPC across the segments, thus providing support for the validity of our earlier model testing results (see Table 9 of Appendix D). Further, the results suggested that although the demographic variables (i.e., gender, age, education, income, and Internet experience) were not significantly different across the segments, the individual factors (i.e., previous privacy invasion experience, risk avoidance personality, and Internet knowledge) could

[8] In the first round of analysis, we controlled for the effects of gender, age, Internet experience, and weekly Internet usage on IPC, and found that none of the control variables was significant. Also, we conducted a series of split-group analyses based on these control variables and did not find any difference across subgroups. Thus, we proceeded to test the model with the main constructs only. Further, to alleviate the concern with common method bias (CMB), we employed the marker variable technique to validate our results. Following Malhotra et al. (2006), we used the smallest positive correlation among the latent constructs (i.e., 0.01) as an estimate of common method bias to produce a CMB-adjusted correlation matrix and re-estimate the path coefficients. The results showed that the CMB-adjusted path coefficients were consistent with those without the CMB adjustment. Hence, CMB was not deemed a threat to our results.

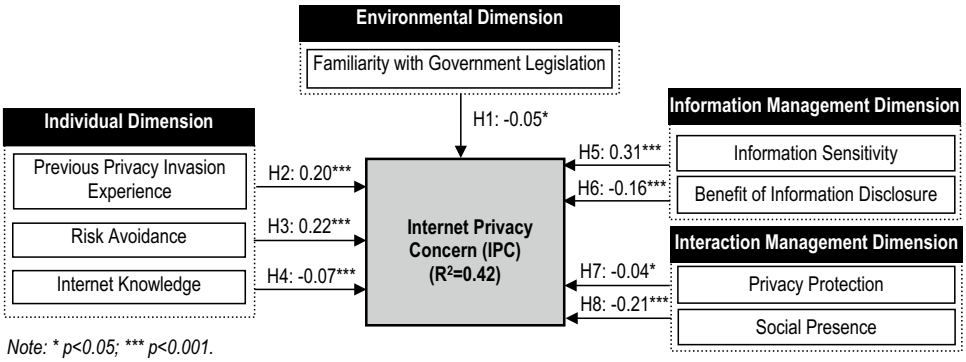

Fig. 2 Hypotheses testing results

Table 3 Results of moderation analysis

	Block 1	Block 2
Familiarity with government legislation (FAMLEG)	−0.05*	−0.05**
Previous privacy invasion experience (PREEXP)	0.20***	0.23***
Risk avoidance (RISK)	0.22***	0.22***
Internet knowledge (KNOW)	−0.07***	−0.08***
Information sensitivity (INFSEN)	0.31***	0.32***
Benefit of information disclosure (INFBEN)	−0.16***	−0.16***
Privacy protection (PROT)	−0.04*	−0.04*
Social presence (SOC)	−0.21***	−0.20***
PREEXP × FAMLEG		0.01
PREEXP × INFSEN		−0.05**
PREEXP × INFBEN		0.01
PREEXP × PROT		0.06***
PREEXP × SOC		0.00
RISK × FAMLEG		0.01
RISK × INFSEN		−0.05**
RISK × INFBEN		−0.02
RISK × PROT		−0.02
RISK × SOC		0.04*
KNOW × FAMLEG		−0.00
KNOW × INFSEN		0.06***
KNOW × INFBEN		−0.01
KNOW × PROT		−0.03
KNOW × SOC		−0.05**
R^2	0.42	0.44
Adjusted R^2	0.41	0.43
ΔR^2		0.02***

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

potentially account for the unobserved heterogeneity leading to the differential effects of the factors across segments (see Table 10 of Appendix D). The results of moderation analysis confirmed this conjecture and showed significant moderating effects of the individual factors (see Table 3).

Following Aiken and West (1991), we plotted the significant interactions (see Fig. 3) and performed simple slope tests. First, previous privacy invasion experience moderated the effects of information sensitivity and privacy protection. The positive effect of information sensitivity on IPC was stronger for individuals who had low previous privacy invasion experience ($\beta = 0.35$, $p < 0.001$) than for those who had high previous privacy invasion experience ($\beta = 0.27$, $p < 0.001$). The effect of privacy protection on IPC was significant and negative for individuals who had low previous privacy invasion experience ($\beta = -0.10$, $p < 0.001$), but was non-significant for those who had high previous privacy invasion experience ($\beta = 0.01$, p>0.05). Second, risk avoidance

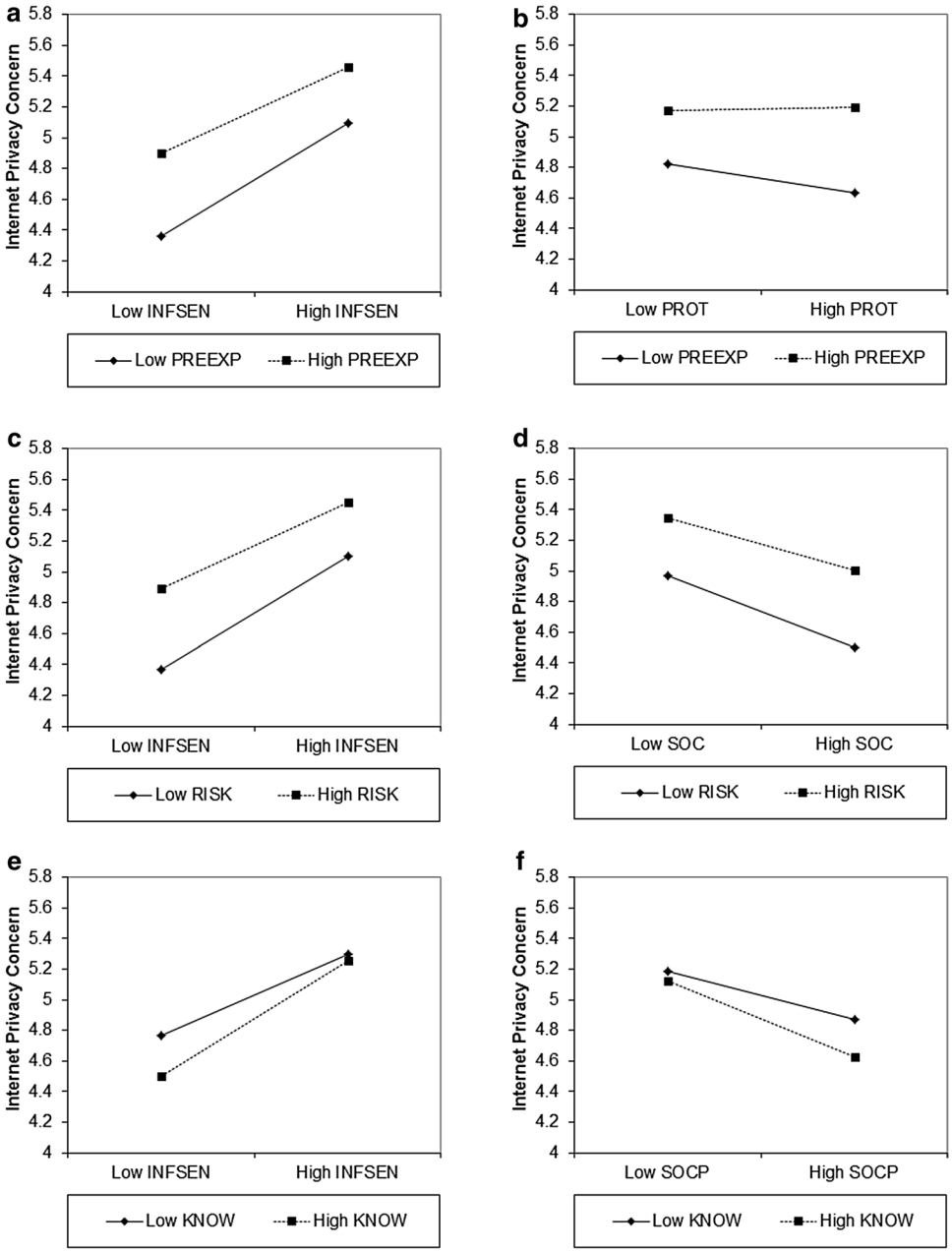

Fig. 3 **a** Previous Privacy Invasion Experience (PREEXP) × Information Sensitivity (INFSEN). **b** Previous Privacy Invasion Experience (PREEXP) × Privacy Protection (PROT). **c** Risk Avoidance (RISK) × Information Sensitivity (INFSEN). **d** Risk Avoidance (RISK) × Social Presence (SOC). **e** Internet Knowledge (KNOW) × Information Sensitivity (INFSEN). **f** Internet Knowledge (KNOW) × Social Presence (SOC)

moderated the effects of information sensitivity and social presence. The positive effect of information sensitivity on IPC was stronger for individuals who had low risk avoidance ($\beta = 0.35$, $p < 0.001$) than for those who had high risk avoidance ($\beta = 0.27$, $p < 0.001$). The negative effect of social presence on IPC was stronger for individuals who had low risk avoidance ($\beta = -0.22$, $p < 0.001$) than for those who had high risk avoidance ($\beta = -0.16$, $p < 0.001$). Finally, Internet knowledge moderated the effects of information sensitivity and social presence. The positive effect of information sensitivity on IPC was stronger for individuals who had high Internet knowledge ($\beta = 0.36$, $p < 0.001$) than for those who had low Internet knowledge ($\beta = 0.26$, $p < 0.001$). The negative effect of social presence on IPC was stronger for individuals who had high Internet knowledge ($\beta = -0.24$, $p < 0.001$) than for those who had low Internet knowledge ($\beta = -0.15$, $p < 0.001$).

Discussion

Compared with prior research, this study provides a more nuanced understanding of the drivers and inhibitors of IPC. The results show that the four dimensions of the MDT have both direct and interaction effects on individuals' IPC. First, the information management dimension plays an important role in determining IPC. On the one hand, the sensitivity of

information solicited on websites has the strongest positive effect on IPC among all independent variables. In particular, for individuals who have greater Internet knowledge, the positive effect of information sensitivity on IPC will be stronger; and interestingly, for individuals who are more risk-averse and who have more previous privacy invasion experience, their IPC will not increase as much as expected along with the increase in information sensitivity, possibly due to the already relatively high level of their IPC. On the other hand, if websites offer benefits in return for information disclosure, individuals' IPC will be reduced.

Second, the interaction management dimension is critical in shaping IPC. Social presence was found to be the strongest inhibitor of IPC among all independent variables. In particular, for individuals who have greater Internet knowledge, the negative effect of social presence on IPC will be stronger; and interestingly, for individuals who are more risk-averse, they will be less responsive to social presence, possibly due to their already high IPC. Next, contrary to the common belief that adopting privacy protection practices automatically reduces privacy concern, we found that these practices are effective only for individuals with little previous privacy invasion experience.

Third, the individual dimension also has a role to play in affecting IPC. Specifically, individuals who had experienced privacy invasion previously are likely to have higher IPC, as such experience will cause individuals to be more cautious about providing personal information to websites. In addition, individuals who are risk-averse will be more concerned about the potential negative consequences of privacy invasion, and thus, have higher IPC. On the contrary, knowledgeable Internet users are likely to be more skillful at protecting their online privacy, and thus, have lower IPC.

Last but not least, the environment dimension also plays a significant role in determining IPC. Individuals who are familiar with government legislations are less concerned about their online privacy.

Theoretical Implications

This paper makes multiple theoretical contributions. First, we have used the MDT as a guiding theoretical lens to advance our understanding of the antecedents of individuals' privacy concerns. The MDT was previously used to examine the conceptualization and measurement of IPC (Hong and Thong 2013), focusing on website practices related to the dimensions of information management and interaction management only. However, the MDT has not been used to investigate the factors that influence an individual's formation of IPC. We extend this line of research by using the complete set of dimensions in the MDT to study the antecedents of IPC. MDT provides a comprehensive and multidimensional framework which takes into account multiple sources of factors that together affect an individual's privacy perception. It provides a good supplement to the risk-benefit paradigm of privacy investigation (such as the social contract theory), and emphasizes the importance of environmental, individual, information management, and interaction management factors in shaping IPC. By considering the multiple dimensions of MDT, researchers can develop a more complete view of the formation of an individual's IPC. Our post hoc analysis further identifies the boundary conditions of MDT and illustrates a refinement of MDT by considering the interaction between the individual dimension and the other three dimensions. Overall, our work demonstrates the utility in applying MDT to examine the drivers and inhibitors of IPC. In particular, our focus on an individual's IPC towards websites in general, rather than IPC towards a specific website (e.g., Facebook) or IPC formed under a particular circumstance (e.g., the Cambridge Analytica scandal), enables researchers to better understand the formation of IPC in spite of temporary fluctuations due to discrete incidents. Such IPC may help to explain why different individuals react differently to the same privacy situation (e.g., some Facebook users may choose to close their account after the Cambridge Analytica scandal, while others may not care much.)

Second, we have conducted a comprehensive review of antecedents of IPC and other relevant types of privacy concerns by using MDT as the guiding framework. Our review supplements existing work on information privacy (e.g., Bélanger and Crossler 2011; Pavlou 2011; Smith et al. 2011), with a particular focus on antecedents of IPC. We found that prior studies have collectively examined factors pertaining to the four dimensions of MDT, highlighting the relevance and utility of MDT in understanding antecedents of IPC. However, prior research has not examined the factors pertaining to multiple dimensions of MDT in the same study, resulting in a disjointed consideration of potentially relevant factors. Also, we observed mixed findings for some of the factors identified in our review. These observations highlight the fragmented nature of extant research in this domain and suggest the need to consolidate and validate previous findings.

Third, based on the literature review, we have incorporated salient factors under each dimension of MDT to formulate an integrated model. The resulting model synthesizes previous findings and provides a foundation to guide future research on understanding and managing online privacy, which is currently inadequate in the business ethics literature (e.g., Ashworth and Free 2006; Martin 2016; Sarathy and Robertson 2003). By simultaneously including factors from multiple dimensions of MDT, our work sheds light on the relative impacts of different dimensions on IPC. Our results show that all dimensions of MDT have significant impacts on IPC. This indicates the need to consider factors from various dimensions jointly in investigating the factors shaping individuals' IPC.

Fourth, our post hoc analysis provides a more nuanced evaluation of the effects of the various antecedents on IPC. The results of the analysis for unobserved heterogeneity show that while most of the antecedents have significant, consistent effects on IPC, certain antecedents could have differential effects on IPC across the heterogeneous segments in a sample (see Table 9 of Appendix D). Further, the results of moderation analysis show that the individual factors (i.e., previous privacy invasion experience, risk avoidance personality, and Internet knowledge) significantly moderated the effects of the factors pertaining to the information management dimension (i.e., information sensitivity) and interaction management dimension (i.e., privacy protection or social presence) (see Table 3; Fig. 3). This finding is consistent with Laufer and Wolfe's (1977) claim that the meaning and experience of privacy in any specific situation can be circumscribed by the interaction of the dimensions of MDT and the elements within them. In summary, the relationships between IPC and its antecedents may be more intricate. Future research could consider alternative ways to model IPC and its antecedents to yield new insights and contextual understanding of the formation of IPC (Hong et al. 2014).

Finally, our study helps to extend and validate prior findings on the antecedents of IPC in an Asian context. In general, our results show that the identified antecedents appear to be significant and consistent across western and Asian contexts. However, it should be noted that some of the antecedents may be prone to cultural variation, as reflected by Hofstede et al. (2010)'s cultural dimensions. For example, the effect of familiarity with government legislation is relatively weak in our sample. This could be because people in Hong Kong are comfortable with ambiguity (a very low score on uncertainty avoidance) and their adherence to laws and rules may be flexible to suit the actual situation (Hofstede et al. 2010). Thus, the presence and enforcement of legislations may not play a major role in their privacy decision making. Relatedly, despite the very low score on uncertainty avoidance, risk avoidance has a strong effect in our sample. This finding suggests that individual traits play a more prominent role in affecting individual privacy decision making, as compared to the country-level cultural values that may not apply to every case. In addition, information sensitivity is the strongest predictor of IPC in our sample. This could be attributed to the restrained culture in Hong Kong (a very low score on indulgence), where people have a tendency toward cynicism and pessimism (Hofstede et al. 2010) and thus be more cautious about the negative consequences of disclosing sensitive information. Also, the strong effect of social presence in our sample could be attributed to the collectivist culture of Hong Kong (a low score on individualism), where people place a high value on personal relationships. In sum, cultural differences could potentially influence an individual's perceptions of IPC and its antecedents, which warrants further research.

Practical Implications

There are practical implications for governments, individuals, and website designers. First, government legislation is an important baseline protection of individuals' information privacy. Our results showed that not only it is important to have government legislations in place, but also individuals have to be aware and familiar with these legislations. Similar to other government programs where awareness is key (Yap and Thong 1997; Yap et al. 1994), governments need to educate their citizens about privacy regulations and laws, so that their citizens would know what privacy rights are protected by law. In addition, it is important to enforce compliance by websites through legislations.

Second, individuals need to educate themselves about the latest privacy protection technologies, including privacy statements, tools, seals, etc., available on the Internet. With adequate knowledge in place, they will be in a better position to judge whether a particular website is trustworthy in terms of handling their personal information. As a result, they can be more proactive in ensuring their personal information in the online environment are protected and manage their levels of IPC.

Third, our results provide useful advice to website designers. It is critical for websites to carefully balance the sensitivity of the information they ask for and the products/services/benefits provided in return. Websites should not ask for sensitive personal information unless absolutely necessary. If they do, they should explain why this information is requested, so that individuals can evaluate the benefits from providing this information. Further, websites should take appropriate actions to protect the information provided by individuals and use them only for the purpose agreed. By doing so, these individuals will have lower IPC and be more willing to provide personal information to websites.

Fourth, websites typically rely on technical measures to reduce individuals' privacy concerns, including privacy statements, providing third-party seals, and so on. While these technical measures are effective, websites can more effectively lower individuals' IPC by increasing their social presence through making their interface design appear more 'human'. For example, by including a picture of a sales person or mimicking the layout of a physical store online, websites can induce potential online consumers to feel closer to them (by providing a similar experience as shopping in a physical store), which results in lowered privacy concern.

Finally, the significant interactions involving the individual dimension highlight the challenges in mitigating privacy

concerns for different individuals. Our results suggest that for individuals who have previous privacy invasion experience and who are highly risk-averse, they have relatively higher IPC and are less likely to be subject to manipulation by information sensitivity, privacy protection, and social presence. This finding underscores the importance of not raising unnecessary privacy concerns in the first place and the need for more effective mitigation measures that can be tailored to users' privacy requirement, such as customized privacy protection (e.g., Zhou and Piramuthu 2015).

Conclusion

This study used MDT as a framework to organize the many antecedents of IPC identified in our literature review. We then tested the utility of MDT by examining the effects of selected antecedents from its various dimensions on individuals' IPC. The results support the utility of MDT for understanding and predicting individuals' IPC. All four dimensions of MDT have significant impact on individuals' IPC, and there are also significant interactions among the dimensions. The MDT framework can serve as a foundation for future research investigating the antecedents of IPC.

Appendix A: Summary of Antecedents of Internet Privacy Concerns

See Tables 4, 5, 6, and 7.

Table 4 Environmental dimension of multidimensional development theory

	Environmental factors				
	Culture values	Government legislations and laws	Industry self-regulation	Media exposure	Social citizenship
Bellman et al. (2004)	X	X			
Benamati et al. (2017)				X	
Caudill and Murphy 2000)		X	X		
Chen et al. (2001)		X			
Culnan and Bies (2003)		X	X		
Dinev et al. (2006)	X				
Dinev et al. (2013)		X			
Flaherty (1989)		X			
Harris et al. (2003)	X				
LaRose and Rifon (2006)			X		
Lowry et al. (2011)	X				
Metzger and Docter (2003)		X	X		
Milberg et al. (1995)	X	X			
Milberg et al. (2000)	X	X			
Miltgen and Peyrat-Guillard (2014)	X				
Ozdemir et al. (2017)				X	
Sarathy and Robertson (2003)		X	X		
Singh and Hill (2003)		X			X
Smith (1994)		X			
Smith et al. (1996)				X	
Turner and Dasgupta (2003)		X	X		
Ward et al. (2005)	X				
Xu and Teo (2004)		X	X		
Xu et al. (2009)		X	X		
Xu et al. (2011a)			X		
Xu et al. (2012)		X	X		

Table 5 Individual dimension of multidimensional development theory

	Individual factors												
	Past experience	Psychological and personality traits						Demographics					
	Previous privacy invasion experience	Trust propensity	Risk avoidance	Personality	Paranoia	Social criticism	Social awareness	Age	Gender	Education	Income	Internet literacy/ knowledge
Awad and Krishnan (2006)	X												
Bansal et al. (2010, 2016)	X			X									
Belanger and Crossler (2019)	X												
Bellman et al. (2004)													X
Benamati et al. (2017)	X							X	X				
Chen et al. (2001)								X	X	X	X	X	
Culnan and Armstrong (1999)	X												
Dinev and Hart (2005)							X						X
Dinev and Hart (2006a)			X										
Graeff and Harmon (2002)								X	X		X		
Hajli and Lin (2016)									X				
Hann et al. (2007)		X		X					X				
Harris et al. (2003)													X
Hoffman et al. (1999)													X
Junglas et al. (2008)				X									
Li (2014)		X											
Miltgen and Peyrat-Guillard (2014)								X					
Miyazaki and Fernandez (2001)													X
Ozdemir et al. (2017)	X												
Phelps et al. (2000)								X	X	X			
Rose (2006)								X					X
Singh and Hill (2003)													X
Sheehan (2002)								X		X			X
Smith et al. (1996)	X	X			X	X							
Stewart and Segars (2002)													X
Ward et al. (2005)				X									X
Xu and Teo (2004)	X												
Xu et al. (2005)	X	X	X										
Xu et al. (2011a)	X							X	X				
Xu et al. (2011b)	X												
Xu et al. (2012)	X	X						X	X	X			

Table 6 Information management dimension of multidimensional development theory

	Informational management factors				
	Information sensitivity	Benefit of information disclosure	Purpose/usage of the information	Perceived vulnerability	Perceived ability to control information
Andrade et al. (2002)	X	X			
Ashworth and Free (2006)	X	X	X		
Culnan and Bies (2003)		X			
Dinev and Hart (2004)				X	X
Dinev and Hart (2006b)	X				
Dinev et al. (2013)	X	X	X	X	X
Hajli and Lin (2016)				X	X
Hann et al. (2007)		X			
Jiang et al. (2013)		X			
Li et al. (2011)	X				
Miller and Weckert (2000)		X	X		
Phelps et al. (2000)	X	X			X
Phelps et al. (2001)	X				
Rohm and Milne (2004)	X				
Sheehan (2002)	X	X			
Sheehan and Hoy (2000)	X	X	X		
Singh and Hill (2003)		X	X		
Ward et al. (2005)	X	X			
Warkentin et al. (2017)					X
White (2004)	X	X			
Xie et al. (2006)		X			
Xu et al. (2009)		X		X	
Xu et al. (2011a)				X	X
Xu et al. (2011b)		X		X	
Xu et al. (2012)					X

Table 7 Interaction management dimension of multidimensional development theory

	Interaction management factors									
	Direct approaches								Indirect approaches	
	Use of privacy protection tools/seals	Awareness of information collection	Authorization of information release	Inclusion/completeness of privacy policy statement	Procedure fairness	Provision of privacy enhancing features	Consumer privacy empowerment	Website informativeness	Reputation of the website	Social presence
Andrade et al. (2002)				X					X	
Ashworth and Free (2006)		X			X					
Awad and Krishnan (2006)				X						
Belanger and Crossler (2019)		X								
Culnan and Armstrong (1999)					X					
Culnan and Bies (2003)		X	X	X	X	X				
Eastlick et al. (2006)			X						X	
Hoehle et al. (2019)								X		
Li (2014)									X	
Pavlou et al. (2007)								X		X
Resnick and Montania (2003)				X						
Sheehan (2002)		X								
Sheehan and Hoy (2000)		X								
Singh and Hill (2003)	X	X	X	X						
Son and Kim (2008)	X								X	
Turner and Dasgupta (2003)	X			X		X				
Van Dyke et al. (2007)							X			
Xie et al. (2006)				X					X	
Xu and Teo (2004)						X				

Table 7 (continued)

	Interaction management factors										
	Direct approaches							Indirect approaches			
	Use of privacy protection tools/seals	Awareness of information collection	Authorization of information release	Inclusion/completeness of privacy policy statement	Procedure fairness	Provision of privacy enhancing features	Consumer privacy empowerment	Website informativeness	Reputation of the website	Social presence
Xu et al. (2005)	X					X				
Xu et al. (2011a)				X						
Xu et al. (2012)							X			

Appendix B: Measurement Scales

Internet Privacy Concern (Collection) (Adapted from Hong and Thong 2013)

COL1 It usually bothers me when websites ask me for personal information

COL2 When websites ask me for personal information, I sometimes think twice before providing it

COL3 I am concerned that websites are collecting too much personal information about me

Internet Privacy Concern (Secondary Usage) (Adapted from Hong and Thong 2013)

SEC1 I am concerned that when I give personal information to a website for some reason, the website would use the information for other reasons

SEC2 I am concerned that websites would sell my personal information in their computer database to other companies

SEC3 I am concerned that websites would share my personal information with other companies without my authorization

Internet Privacy Concern (Errors) (Adapted from Hong and Thong 2013)

ERR1 I am concerned that websites do not take enough steps to make sure that my personal information in their files is accurate

ERR2 I am concerned that websites do not have adequate procedures to correct errors in my personal information

ERR3 I am concerned that websites do not devote enough time and effort to verifying the accuracy of my personal information in their databases

Internet Privacy Concern (Improper Access) (Adapted from Hong and Thong 2013)

ACC1 I am concerned that databases that contain my personal information are not protected from unauthorized access

ACC2 I am concerned that websites do not devote enough time and effort to preventing unauthorized access to my personal information

ACC3 I am concerned that websites do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers

Internet Privacy Concern (Control) (Adapted from Hong and Thong 2013)

CON1 It usually bothers me when I do not have control of the personal information that I provide to websites
CON2 It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by websites
CON3 I am concerned when control is lost or unwillingly reduced as a result of a marketing transaction with websites

Internet Privacy Concern (Awareness) (Adapted from Hong and Thong 2013)

AWA1 It usually bothers me when online privacy policy does not have a clear and conspicuous disclosure
AWA2 It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by websites
AWA3 It usually bothers me when websites seeking my information online do not disclose the way the data are collected, processed, and used

Familiarity with Government Legislations (Self-developed Based on the Definition of the Construct)

FAMLEG1 I am fully aware that the Hong Kong government has a Privacy Policy to protect my privacy
FAMLEG2 I am familiar with the Privacy Policy issued by the Hong Kong government

Previous Privacy Invasion Experience (Adapted from Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2005)

PREEXP1 How often have you personally experienced incidents whereby your personal information was used by some websites without your authorization?

PREEXP2 How often have you personally been the victim of what you felt was an improper invasion of privacy by websites?

Risk Avoidance (Adapted from Xu et al. 2005)

RISK1 I would rather be safe than sorry
RISK2 I am cautious in trying new or different things
RISK3 I avoid risky things

Internet Knowledge (Adapted from Singh and Hill 2003)

KNOW1 I am knowledgeable about the Internet and its related privacy issues
KNOW2 I am knowledgeable about latest developments that address Internet privacy issues

Information Sensitivity (Self-developed Based on the Definition of the Construct)

INFSEN1 When I am required to provide personal information to websites in exchange of their services, the information that they ask for are usually very sensitive personal information
INFSEN2 Websites tend to ask me for sensitive personal information in order to obtain their services

Benefit of Information Disclosure (Self-developed Based on the Definition of the Construct)

INFBEN1 The benefits that I can obtain by providing my personal information to websites are usually significant
INFBEN2 I value the benefits that I can obtain by providing my personal information to websites

Privacy Protection (Self-developed Based on the Definition of the Construct and Popular Practices)

PROT1 In general, websites would ask for my authorization before collecting my personal information
PROT2 In general, websites would use privacy protection tools (such as third-party seals from TRUSTe or BBBOnline)

PROT3 In general, websites would include a privacy policy statement on their websites
PROT4 In general, websites would let me aware the purpose of collecting my personal information

Social Presence (Adapted from Pavlou et al. 2007)

SOC1 There is a sense of human contact in websites
SOC2 There is a sense of personalness in websites
SOC3 There is a sense of human warmth (or sensitivity) in websites

Appendix C

See Table 8.

Table 8 Results of confirmatory factor analysis

	FAMLEG	PREEXP	RISK	KNOW	INFSEN	INFBEN	PROT	SOC	AWA	COL	SEC	CON	ERR	ACC
FAMLEG1	**0.85**	−0.06	0.06	0.27	0.07	0.15	0.28	0.15	−0.01	−0.07	−0.07	−0.11	−0.12	−0.07
FAMLEG2	**0.93**	0.02	0.03	0.41	0.09	0.20	0.17	0.24	−0.10	−0.10	−0.09	−0.11	−0.12	−0.14
PREEXP1	−0.01	**0.96**	0.05	0.01	0.22	−0.19	−0.30	−0.11	0.18	0.32	0.40	0.33	0.26	0.26
PREEXP2	−0.02	**0.93**	0.01	0.02	0.19	−0.14	−0.29	−0.09	0.14	0.26	0.32	0.27	0.23	0.20
RISK1	0.03	0.05	**0.83**	0.05	0.18	−0.11	−0.06	−0.04	0.21	0.26	0.22	0.21	0.20	0.20
RISK2	0.06	0.01	**0.80**	0.05	0.15	−0.09	0.08	−0.07	0.30	0.24	0.22	0.19	0.22	0.25
RISK3	0.01	0.03	**0.84**	0.05	0.14	−0.08	−0.03	−0.02	0.19	0.23	0.18	0.19	0.18	0.18
KNOW1	0.25	−0.01	0.05	**0.81**	0.05	0.09	0.11	0.09	−0.04	−0.09	−0.03	−0.05	−0.05	−0.04
KNOW2	0.42	0.02	0.06	**0.96**	0.08	0.17	0.13	0.20	−0.11	−0.11	−0.09	−0.08	−0.10	−0.13
INFSEN1	0.10	0.21	0.18	0.07	**0.96**	−0.05	−0.05	−0.05	0.32	0.34	0.35	0.35	0.29	0.33
INFSEN2	0.08	0.22	0.18	0.07	**0.96**	−0.06	−0.07	−0.06	0.31	0.34	0.36	0.37	0.29	0.33
INFBEN1	0.21	−0.15	−0.10	0.15	−0.02	**0.95**	0.26	0.36	−0.24	−0.30	−0.30	−0.26	−0.25	−0.24
INFBEN2	0.18	−0.18	−0.13	0.15	−0.09	**0.96**	0.28	0.38	−0.26	−0.34	−0.33	−0.30	−0.27	−0.27
PROT1	0.16	−0.24	0.02	0.08	−0.03	0.18	**0.73**	0.17	0.01	−0.10	−0.14	−0.15	−0.11	−0.07
PROT2	0.19	−0.24	0.01	0.15	−0.04	0.20	**0.80**	0.22	−0.08	−0.16	−0.21	−0.18	−0.17	−0.14
PROT3	0.21	−0.19	0.04	0.08	−0.01	0.13	**0.70**	0.09	0.06	−0.07	−0.10	−0.09	−0.09	−0.03
PROT4	0.20	−0.28	−0.02	0.10	−0.07	0.29	**0.87**	0.29	−0.13	−0.24	−0.28	−0.26	−0.23	−0.20
SOC1	0.21	−0.07	−0.02	0.15	−0.04	0.31	0.27	**0.88**	−0.24	−0.26	−0.25	−0.23	−0.22	−0.25
SOC2	0.18	−0.10	−0.02	0.13	−0.03	0.31	0.26	**0.82**	−0.20	−0.23	−0.21	−0.19	−0.20	−0.18
SOC3	0.21	−0.10	−0.09	0.17	−0.07	0.38	0.23	**0.91**	−0.33	−0.34	−0.32	−0.27	−0.29	−0.33
AWA1	−0.05	0.16	0.26	−0.08	0.30	−0.24	−0.08	−0.27	**0.92**	0.56	0.54	0.54	0.57	0.64
AWA2	−0.08	0.16	0.28	−0.10	0.31	−0.25	−0.08	−0.29	**0.95**	0.57	0.55	0.53	0.56	0.66
AWA3	−0.07	0.16	0.27	−0.09	0.31	−0.23	−0.09	−0.29	**0.93**	0.55	0.54	0.55	0.56	0.66
COL1	−0.10	0.33	0.26	−0.12	0.34	−0.31	−0.25	−0.32	0.52	**0.89**	0.66	0.61	0.53	0.53
COL2	−0.06	0.24	0.29	−0.11	0.31	−0.31	−0.14	−0.28	0.54	**0.91**	0.65	0.58	0.52	0.53
COL3	−0.09	0.29	0.27	−0.10	0.33	−0.31	−0.21	−0.30	0.58	**0.93**	0.74	0.67	0.59	0.58
SEC1	−0.07	0.35	0.24	−0.08	0.34	−0.30	−0.24	−0.29	0.57	0.73	**0.93**	0.72	0.59	0.61
SEC2	−0.08	0.41	0.23	−0.07	0.36	−0.31	−0.28	−0.27	0.50	0.69	**0.93**	0.70	0.57	0.59
SEC3	−0.11	0.32	0.24	−0.09	0.33	−0.30	−0.25	−0.30	0.56	0.68	**0.93**	0.74	0.60	0.63
CON1	−0.11	0.30	0.23	−0.08	0.36	−0.28	−0.23	−0.27	0.56	0.66	0.76	**0.96**	0.60	0.60
CON2	−0.11	0.30	0.24	−0.07	0.35	−0.29	−0.23	−0.26	0.56	0.66	0.74	**0.97**	0.61	0.61
CON3	−0.12	0.32	0.23	−0.08	0.36	−0.28	−0.25	−0.26	0.54	0.65	0.73	**0.96**	0.61	0.59
ERR1	−0.13	0.26	0.24	−0.09	0.30	−0.27	−0.20	−0.27	0.57	0.59	0.62	0.61	**0.92**	0.69
ERR2	−0.12	0.24	0.22	−0.07	0.26	−0.25	−0.20	−0.25	0.54	0.53	0.57	0.57	**0.94**	0.64
ERR3	−0.13	0.23	0.23	−0.10	0.28	−0.25	−0.21	−0.25	0.56	0.55	0.57	0.58	**0.93**	0.69
ACC1	−0.10	0.22	0.25	−0.10	0.34	−0.25	−0.16	−0.29	0.69	0.58	0.64	0.60	0.68	**0.94**
ACC2	−0.13	0.24	0.24	−0.11	0.32	−0.27	−0.18	−0.28	0.65	0.57	0.61	0.59	0.71	**0.96**
ACC3	−0.12	0.24	0.25	−0.11	0.33	−0.26	−0.16	−0.29	0.66	0.56	0.62	0.60	0.69	**0.96**

The bold values are used to highlight the factor loadings of the items for their corresponding constructs

Appendix D: Results of Analysis of Unobserved Heterogeneity

We conducted an analysis of unobserved heterogeneity in our sample using the REBUS-PLS method (Esposito Vinzi et al. 2008). The REBUS-PLS method aims to detect sources of heterogeneity in both the structural and the outer model for all exogenous and endogenous latent variables. Unlike other similar methods such as FIMIX-PLS and PLS-POS, REBUS-PLS does not require specifying a priori the number of segments to be extracted from a sample and is able to identify the appropriate number of segments based on a hierarchical classification on the residuals of all units from the overall structural model (see Becker et al. 2013 for a review).

The REBUS-PLS analysis identified three segments from our sample. We assessed the measurement model for each segment before we interpreted the results. For all segments, the measurement models possessed adequate reliability, convergent validity, and discriminant validity. Table 9 presents the results of the REBUS-PLS analysis. The results showed that compared with the model of the full sample, the models of the three identified segments explained a greater amount of variance in IPC and had a better goodness of fit. This suggests that unobserved heterogeneity existed in our sample and the respondents in different segments may value the factors differently in forming their IPC, as confirmed by the pairwise tests for path differences. Despite the significant differences in some paths, the results showed that all of the factors had significant, consistent (either positive or negative) effects on IPC across segments, except for Internet knowledge and privacy protection in Segment 2. Overall, the results provided support for the validity of the main model testing results.

Following the guidelines of Esposito Vinzi et al. (2008) and Becker et al. (2013), we characterized the identified segments and attempted to account for the unobserved heterogeneity by incorporating potential moderators into the model. First, we compared the demographic variables (gender, age, education, income, and Internet experience) across the three segments. However, the results of pairwise comparison showed that there was no significant difference for all demographic variables. Second, we compared the mean values of the latent constructs in the model. The results of pairwise comparison showed that some significant differences existed across the segments (see Table 10). In particular, the respondents in Segment 2 reported the highest mean values for risk avoidance, information sensitivity, and Internet privacy concern among the segments. The respondents in Segment 2 also reported a higher mean value for familiarity with government legislation than those in Segment 1, a lower mean value for Internet knowledge than those in Segment 3, and a lower mean value for benefit of information disclosure than those in Segment 1. Given the relatively high mean value for risk avoidance and low mean value for Internet knowledge for Segment 2, we expected individual factors to be the potential variables that could account for the unobserved heterogeneity leading to the differential effects of the factors across segments.

Table 9 Results of REBUS-PLS analysis

	Full $N=2417$ (100%)	Segment 1 $N=694$ (28.7%)	Segment 2 $N=860$ (35.6%)	Segment 3 $N=863$ (35.7%)	p_{12}	p_{13}	p_{23}
R^2	0.42	0.72	0.57	0.89			
Goodness of Fit index	0.54	0.69	0.57	0.72			
Familiarity with government legislation	−0.05*	−0.15***	−0.11***	−0.18***	0.190	0.325	0.012
Previous privacy invasion experience	0.20***	0.36***	0.26***	0.38***	0.002	0.433	0.000
Risk avoidance	0.22***	0.18***	0.23***	0.25***	0.143	0.006	0.504
Internet knowledge	−0.07***	−0.09***	0.03	−0.03*	0.006	0.022	0.161
Information sensitivity	0.31***	0.31***	0.39***	0.39***	0.007	0.003	0.862
Benefit of information disclosure	−0.16***	−0.15***	−0.26***	−0.16***	0.001	0.547	0.001
Privacy protection	−0.04*	−0.07**	−0.02	−0.05***	0.207	0.612	0.247
Social presence	−0.21***	−0.24***	−0.28***	−0.36***	0.209	0.000	0.020

p_{12}: p value for multi-group comparison test for path differences between Segment 1 and Segment 2. p_{13}: p value for multi-group comparison test for path differences between Segment 1 and Segment 3. p_{23}: p value for multi-group comparison test for path differences between Segment 2 and Segment 3

*$p<0.05$, **$p<0.01$, ***$p<0.001$

Table 10 Results of mean-difference tests

	Segment 1 $N=694$ (28.7%)	Segment 2 $N=860$ (35.6%)	Segment 3 $N=863$ (35.7%)	p_{12}	p_{13}	p_{23}
Familiarity with government legislation	3.99	4.16	4.05	0.002	0.258	0.040
Previous privacy invasion experience	2.37	2.31	2.31	0.399	0.364	0.933
Risk avoidance	4.67	4.96	4.75	0.000	0.101	0.000
Internet knowledge	3.74	3.71	3.86	0.548	0.022	0.003
Information sensitivity	4.08	4.34	4.17	0.000	0.111	0.000
Benefit of information disclosure	3.63	3.50	3.59	0.010	0.328	0.072
Privacy protection	4.88	4.89	4.88	0.854	0.991	0.831
Social presence	3.33	3.25	3.27	0.141	0.199	0.805
Internet privacy concern	3.98	5.78	4.91	0.000	0.000	0.000

p_{12}: p value for mean-difference test between Segment 1 and Segment 2. p_{13}: p value for mean-difference test between Segment 1 and Segment 3. p_{23}: p value for mean-difference test between Segment 2 and Segment 3

Funding This research was funded by a Grant RPC11BM17 from the authors' institution.

Compliance with Ethical Standards

Conflict of interest The authors have no conflicts of interest.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the authors' institutional Human Participants Research Panel. Informed consent was obtained from all individual participants whereby they had to click a consent button before they can participate in the online survey.

References

Aiken, L. S., & West, S. C. (1991). *Multiple regression testing and interpreting interactions*. Newbury Park, CA: Sage.

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research, 29*(1), 350–353.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21.

Becker, J. M., Rai, A., Ringle, C. M., & Völckner, F. (2013). Discovering unobserved heterogeneity in structural equation models to avert validity threats. *MIS Quarterly, 37*(3), 665–694.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041.

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems, 28*(1), 34–49.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313–324.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents-Privacy Concerns–Outcomes model. *Journal of Information Science, 43*(5), 583–600.

Bennett, C. J. (1992). *Regulating privacy*. Ithaca, NY: Cornell University Press.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing, 11*(3), 44–57.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7–19.

Census and Statistics Department of Hong Kong. (2018). Hong Kong as an Information Society. Retrieved October 12, 2018 from https://www.censtatd.gov.hk/hkstat/sub/sp120.jsp?productCode=B1110006.

Centre for International Governance Innovation (CIGI). (2018). 2018 CIGI-ipsos global survey on internet security and trust. Retrieved October 12, 2018 from https://www.cigionline.org/internet-survey-2018.

Chaykowski, K. (2018). Facebook says data on 87 million people may have been shared in Cambridge Analytica leak. Forbes. Retrieved April 4, 2018 from http://www.forbes.com/sites/kathleench

aykowski/2018/04/04/facebook-says-data-on-87-million-people-may-have-been-shared-in-cambridge-analytica-leak/.
Chen, J. C., Zhang, Y., & Heath, R. (2001). An exploratory investigation of the relationships between consumer characteristics and information privacy. *Marketing Management Journal, 11*(1), 73–81.
Choi, Y. K., Miracle, G. E., & Biocca, F. (2001). The effects of anthropomorphic agents on advertising effectiveness and the mediating role of presence. *Journal of Interactive Advertising, 2*(1), 19–32.
Culnan, M. J. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341–363.
Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedure fairness, and impersonal trust: An empirical investigation. *Organizational Science, 10*(1), 104–115.
Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.
Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – A study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389–402.
Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents: Measurement validity and a regression model. *Behavior & Information Technology, 23*(6), 413–422.
Dinev, T. & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29.
Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.
Dinev, T., & Hart, P. (2006b). Privacy concerns and levels of information exchange: An empirical investigation of intended eservices use. *eService Journal, 4*(3), 25–59.
Dinev, T., Xu, H., Smith, H. J., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316.
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.
Esposito Vinzi, V., Trinchera, L., Squillacciotti, S., & Tenenhaus, M. (2008). REBUS-PLS: A response-based procedure for detecting unit segments in PLS path modelling. *Applied Stochastic Models in Business & Industry, 24*(5), 439–458.
Etzioni, A. (2019). Cyber trust. *Journal of Business Ethics, 156*(1), 1–13.
Flaherty, D. H. (1989). *Protecting privacy in surveillance societies*. Chapel Hill, NC: University of North Carolina Press.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.
Garfinkel, R., Gopal, R., & Thompson, S. (2007). Releasing individually identifiable microdata with privacy protection against stochastic threat: An application to health information. *Information Systems Research, 18*(1), 23–41.
Gillis, A. R., Richard, M. A., & Hagan, J. (1986). Ethnic susceptibility to crowding: An empirical analysis. *Environment and Behavior, 18*(6), 683–706.
Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Comparing PLS to regression and LISREL: A response to Marcoulides, Chin, and Saunders. *MIS Quarterly, 36*(3), 703–716.
Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4/5), 302–318.
Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139–152.
Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111–123.
Hann, I. H., Hui, K. L., Lee, S. Y., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13–42.
Harris, M. M., Hoye, G. V., & Lievens, F. (2003). Privacy and attitudes towards Internet-based selection systems: A cross-cultural comparison. *International Journal of Selection and Assessment, 11*(2/3), 230–236.
Hoehle, H., Aloysius, J. A., Goodarzi, S., & Venkatesh, V. (2019). A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency. *European Journal of Information Systems, 28*(1), 91–113.
Hoffman, D. L., Novak, T., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85.
Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: software of the mind*. Columbus, OH: McGraw Hill.
Hofstede Insights. (2018). Country comparison. Retrieved October 12, 2018 from https://www.hofstede-insights.com/country-comparison/.
Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111–136.
Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298.
Hui, K. L., Tan, B. C. Y., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology, 6*(4), 415–441.
Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.
International Data Corporation (IDC). (2017). IDC special report: measuring U.S. Privacy Sentiment (IDC #US42238617).
Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579–595.
Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387–402.
Klopfer, P. H., & Rubenstein, D. L. (1977). The concept privacy and its biological basis. *Journal of Social Issues, 33*(3), 52–65.
LaRose, R., & Rifon, N. (2006). Your privacy is assured—of being disturbed: Comparing Web Sites with and without privacy seals. *New Media and Society, 8*(6), 1009–1029.
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional development theory. *Journal of Social Issues, 33*(3), 22–42.
Lewis, D. (2014). Sony pictures: The data breach and how the criminals won. Forbes. Retrieved December 18, 2014 from http://www.forbes.com/sites/davelewis/2014/12/17/sony-pictures-how-the-criminal-hackers-won/.
Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481.
Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57,* 343–354.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' willingness to disclose personal information. *Decision Support Systems, 51*(3), 434–445.

Li, X. B., & Sarkar, S. (2006). Privacy protection in data mining: A perturbation approach for categorical data. *Information Systems Research, 17*(3), 254–270.

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*(1), 289–304.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200.

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.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science, 52*(12), 1865–1883.

Marshall, N. J. (1974). Dimensions of privacy preferences. *Multivariate Behavioral Research, 9*(3), 255–271.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569.

Metzger, M. J., & Docter, S. (2003). Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting and Electronic Media, 47*(3), 350–374.

Meyer, D. (2017). Here's why Facebook got a $1.4 million privacy fine in Spain. Fortune. Retrieved September 11, 2017 from http://fortune.com/2017/09/11/facebook-privacy-fine-spain/.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65–74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57.

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the Internet. *Journal of Business Ethics, 28*(3), 255–265.

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing, 19*(1), 1–6.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 12*(2), 206–215.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103–125.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs, 35*(1), 27–44.

Nowak, G., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when 'privacy' matters. *Journal of Direct Marketing, 11*(4), 94–108.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642–660.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?". *MIS Quarterly, 35*(4), 977–988.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online environments: An agency theory perspective. *MIS Quarterly, 31*(1), 105–136.

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management, 30*(6), 467–480.

Phelps, J. P., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2–17.

Phelps, J. P., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27–41.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*(3), 221–235.

Popovic, A., Smith, H. J., Thong, J. Y. L., & Wattal, S. (2017). Information privacy. In: A. Bush & A. Rai (Eds.), *MIS quarterly research curations*. Retrieved April 30, 2017 from http://misq.org/research-curations.

Rainie, L. (2016). The state of privacy in post-Snowden America. Pew Research Center. Retrieved September 21, 2016 from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332–344.

Resnick, M. L., & Montania, R. (2003). Perceptions of consumer service, information privacy, and product quality from semiotic design features in an online Web store. *International Journal of Human-Computer Interaction, 16*(2), 211–234.

Rice, R. (1993). Using social presence theory to compare traditional and new organizational media. *Human Communication Research, 19*(4), 451–484.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1), iii–xiv.

Roberts, J. J. (2017). Instagram, Twitter and others could pay users $5.3 million in app privacy settlement. Fortune. Retrieved April 4, 2017 from http://fortune.com/2017/04/04/find-friends-privacy-instagram-twitter/.

Rohm, A., & Milne, G. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research, 57*(9), 1000–1011.

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management, 43*(3), 322–335.

Ruddick, G. (2017). UK class action accuses Google of unlawfully harvesting personal data. The Guardian. Retrieved November 30, 2017 from http://www.theguardian.com/uk-news/2017/nov/30/uk-class-action-accuses-google-of-unlawfully-harvesting-personal-data.

Ruiz-Palomino, P., & Martinez-Cañas, R. (2011). Supervisor role modeling, ethics-related organizational policies, and employee ethical intention: The moderating impact of moral ideology. *Journal of Business Ethics, 102*(4), 653–668.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics, 46*(2), 111–126.

Shaw, T. R. (2003). The moral intensity of privacy: An empirical study of webmaster' attitudes. *Journal of Business Ethics, 46*(4), 301–318.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society, 18*(1), 21–32.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62–73.

Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. London: Wiley.

Singer, E., Mathiowetz, N. A., & Couper, M. P. (1993). The impact of privacy and confidentiality concerns on survey participation: The case of the 1990 US census. *Public Opinion Quarterly, 57*(4), 465–482.

Singh, T., & Hill, M. E. (2003). Consumer privacy and the Internet in Europe: A view from Germany. *Journal of Consumer Marketing, 20*(7), 634–651.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal, 38*(6), 1573–1592.

Smith, H. J. (1994). *Managing privacy: Information technology and corporate America*. Chapel Hill, NC: University of North Carolina Press.

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

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

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

Statista. (2016). Daily internet usage rate in Hong Kong in 2016, by age group. Retrieved October 12, 2018 from https://www.statista.com/statistics/347959/daily-internet-usage-age-group-hong-kong/.

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

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349–411.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.

Turner, E. C., & Dasgupta, S. (2003). Privacy on the Web: An examination of user concerns, technology, and implications for business organizations and individuals. *Information Systems Management, 20*(1), 8–19.

Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets, 17*(1), 68–81.

Wang, J., & Lau, S. S. (2013). Hierarchical production of privacy: Gating in compact living in Hong Kong. *Current Urban Studies, 1*(2), 11–18.

Ward, S., Bridges, K., & Chitty, B. (2005). Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications, 11*(1), 21–40.

Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: What determines smart meter technology adoption? *Journal of the Association for Information Systems, 18*(11), 758–786.

Weigel-Garrey, C. J., Cook, C. C., & Brotherson, M. J. (1998). Children and Privacy. *Journal of Family Issues, 19*(1), 43–64.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431–453.

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33*(1), 177–195.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology, 14*(1/2), 41–51.

Wijethilake, C., Munir, R., & Appuhami, R. (2018). Environmental innovation strategy and organizational performance: Enabling and controlling uses of management control systems. *Journal of Business Ethics, 151*(4), 1139–1160.

Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters, 17*(1), 61–74.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011a). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 518–546.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011b). The personalization privacy paradox: A study of privacy decision making process for location-awareness marketing. *Decision Support Systems, 51*(1), 42–52.

Xu, H. & Teo, H. H. (2004). Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. In: *Proceedings of the 25th international conference on information systems* (pp. 793–806). Washington, DC, 2004.

Xu, H., Teo, H. H., & Tan, B. C. Y. (2005). Predicting the adoption of location-based services: The role of trust and perceived privacy risk. In: *Proceedings of the 26th international conference on information systems* (pp. 897–910). Las Vegas, NV, 2005.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push–pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 137–176.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342–1363.

Yap, C. S., & Thong, J. Y. L. (1997). Programme evaluation of a government information technology programme for small businesses. *Journal of Information Technology, 12*(2), 107–120.

Yap, C. S., Thong, J. Y. L., & Raman, K. S. (1994). Effect of government incentives on computerization in small business. *European Journal of Information Systems, 3*(3), 191–206.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110.

Zhou, W., & Piramuthu, S. (2015). Information relevance model of customized privacy for IoT. *Journal of Business Ethics, 131*(1), 19–30.