The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors

Robert E. Crossler
Washington State University
rob.crossler@wsu.edu

France Bélanger
Virginia Tech
belanger@vt.edu

Abstract

Increasing collection of individuals' information has led to several security and privacy issues, such as identity theft and targeted marketing. These risks are further heightened in the mobile realm as data collection can occur continuously and ubiquitously. Most existing research considers threats to privacy and security as separate concerns, resulting in separate research streams. However, focusing on information privacy alone results in a lack of understanding of the security ramifications of individual information disclosure. Using the Information Motivation Behavioral (IMB) Skills Model as a theoretical foundation, we develop the Knowledge Gap Model of Security and Privacy Behavior. In the model, we propose that two knowledge gaps exist that affect how individuals enact security and privacy behaviors: the security-privacy knowledge gap, and the knowledge-belief gap. We use the model to develop a research agenda for future research.

1. Introduction

As multiple entities increasingly collect personal information about us, sensitive profiles are created that we often do not have control over. In fact, individuals often decide to disclose their personal information for the purpose of receiving some benefit [1-3]. However, the release of this information can result in security breaches for the individual because hackers target organizations' information repositories. As a result, individuals face a heightened risk of identity theft, targeted marketing, and reputational damage. If people who were subject to the security breaches of companies such as Ashley Madison, Adobe, or Sony would have viewed the disclosure of their information in terms of having their information stolen, odds are they would not have shared their information. These examples are manifested by disclosing information via a personal computer. However, with over 58% of all Americans owning a smartphone, including 83% of 18 to 29 year olds and 74% of 30 to 49 year olds [4], and many of them downloading large numbers of apps, even more information is being disclosed with little to no consideration or concern for the security of the information disclosed via these apps.

In the USA, 7% of the population accesses the Internet solely through their smartphone [5]. With the proliferation of these smart devices comes a unique set of challenges for organizations, individuals, and society at large [6], in particular with respect to information security and privacy as companies and governments continue to collect vast amounts of personal information from these smartphones [7], often without individuals' awareness. Issues identified in prior research with information privacy and security include default settings for pictures and videos having geo-tagging of location information [8, 9], malicious code attached to apps [10], and hidden data collection tools in apps [11]. The simplicity of data collection that occurs through the ubiquitous use of smartphones only increases this risk. By agreeing to download and use smartphone apps, users are implicitly giving permission to disclose sensitive information.

In this paper, we propose that there are two types of gaps that affect information privacy and security behaviors of individuals. The first gap is the privacy-security knowledge gap. This gap illustrates the different understanding of individuals regarding impacts of information being shared when presented with privacy or security-based decisions. The second gap is the knowledge-belief gap in which a person may believe they can do something but do not necessarily have the knowledge to do so. In the following sections, we describe these gaps and discuss how the Information-Motivation Behavioral (IMB) Skills Model can be a useful framework for exploring how these knowledge gaps affect behaviors, providing a bridge between information security and privacy research streams. Based on the model, we propose a research agenda that can help researchers understand of the reasons for the existence of these gaps and their consequences.

URI: http://hdl.handle.net/10125/41651
ISBN: 978-0-9981331-0-2

2. Background and theoretical foundations

A key premise of this research is that individuals have different levels of knowledge about mobile information security, information privacy, and technology, and that these differences create a knowledge gap and influence individuals' disclosure behaviors, putting their information at risk. Disclosure of information, even voluntary, is not only an information privacy issue but also an information security issue. Information security refers to individuals protecting themselves against threats to their information assets [12], while information privacy is viewed as an individual's ability to control information about themselves [e.g., 13, 14, 15]. Today's smartphones are typically set up with complex information security and privacy settings, with many default settings often set to give away most information. These settings often change over time with little to no notice provided to the user. In fact, today's "smartphone operating systems frequently fail to provide users with visibility into how third-party applications collect and share their private data" [16, p. 1]. As a result, many users are not aware nor knowledgeable enough to keep up with these changing settings. In fact, prior research has shown that individuals have limited awareness of how what they should do to protect their information privacy on mobile devices [17, 18]. Indeed, users often feel overwhelmed with how to control others' access to their personal information [19]. This is crucial because citizens' understanding of information security and privacy threats, and knowledge of the tools they can use to protect themselves, are necessary to provide a more secure society, particularly since individuals are the weakest link in security [12] and the last line of defense in information privacy [20].

While existing research treats information security and information privacy threats mostly separately, we argue that research on information privacy alone results in a lack of understanding of the security ramifications of information disclosure for individuals. For example, Figure 1 suggests that when individuals face a choice that may impact their privacy (e.g. sharing personal information to access a social networking site), they often decide to disclose the information. This view is supported by privacy paradox research [e.g., 21, 22, 23], which suggests that even when individuals are concerned they will still share their information if there are some benefits for doing so. However, if individuals believe the information that is shared can be accessed fraudulently (e.g. sharing credit card information with a questionable website), then they may refrain from sharing this information [24]. In other words, individuals may decide not to perform behaviors that would affect the security of their information, but they may share this same information without much thought when they benefit from such sharing (e.g., convenience, reduced costs, etc.). This suggests that citizens may not fully understand the difference between protecting the security of their smartphone information and protecting the privacy of the information shared with others via the same smartphone. We refer to this as the security-privacy knowledge gap.

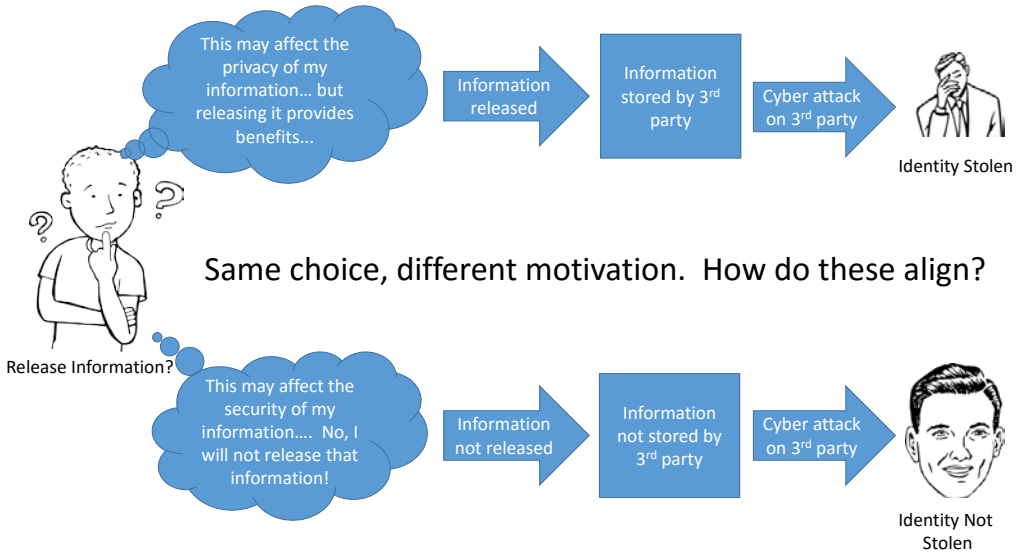

Figure 1. The Information Security-Privacy Knowledge Gap

In this research, we focus on the knowledge gap in the mobile environment since in today's society many individuals use smartphones for numerous everyday tasks, and often use their smartphone as their main device for all interactions. In this context, threats are growing more rapidly than in the traditional online environment. For example, users download apps without trying them, relying on descriptions of the apps, reviews and ratings [25]. Yet, apps are executable files that can be used for mischievous acts since information security is often weakly implemented in smartphones [26] and there is generally a weaker mobile regulatory framework for privacy [26]. In fact, the average user has over 200 apps on their smartphone, with several possibly unsafe ones [27]. Some apps allow app developers to collect individuals personal information for any purpose they chose to [28]. Research shows that in the mobile context individuals may not even know they are giving away such information [17, 18, 29]. Furthermore, this information is often mingled with data collected via other computers and stored in organizational databases. Therefore, with the proliferation of smartphones, the mobile platform has become a new target-rich environment for hackers [30]; this context provides a uniquely rich contextual source to study the security-privacy knowledge gap.

2.1. The Information-Motivation Behavioral (IMB) skills model

Most of the research on mobile information security and privacy has been conducted either without strong theoretical foundations or uses the privacy calculus [e.g., 2, 3, 31, 32-34], privacy paradox [e.g., 22, 23, 35], or protection motivation theory [36-39]. However, since this research has not focused on actual knowledge, we turn to a theoretical foundation that specifically addresses the need to recognize knowledge or skills in affecting individual behaviors: the Information Motivation Behavioral (IMB) Skills Model.

The Information-Motivation Behavioral (IMB) Skills Model [40-43], presented in Figure 2, has been mostly used in the behavioral health and social psychology literatures. Examples of its applicability include prediction of self-examination for breast cancer [44], risk-reduction behaviors related to HIV [40-42, 45], or condom usage [46]. In most of these studies, the IMB Skills Model is used to predict actual behaviors whereas factors associated with other theories, such as the Theory of Planned Behavior [47-49] tend to focus on intentions. The model has not been used in the contexts of information security or privacy, although most of the information security research discusses skills in the form of perceived ability (self-efficacy) [36, 37, 50-52]. Contrarily to that research, we argue researchers need to measure actual skills and the resulting behaviors. While protection of one's information is different from protection related to one's health, the IMB Skills Model offers an avenue to better understand individual behaviors related to information security and privacy. There are some studies outside the realms of behavioral health that have used the model, such as a study of young adults' voting behaviors [53].

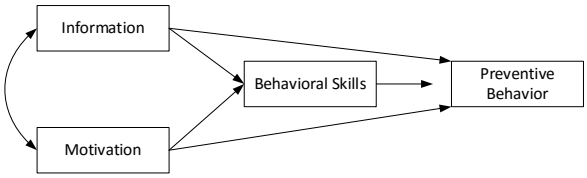

Figure 2. The Information Motivation Behavior Skills Model [43]

As seen in Figure 2, there are three key components that lead to individual behaviors: information, motivation, and skills related to the behavior. According to the IMB Skills model, information is a pre-requisite for behaviors to be enacted. Information relates to the individuals' understanding of the concepts related to the behavior of interest and of the means necessary to achieve the behavioral change. In behavioral health, this would include knowing about the risks related to HIV or cancer. In the context of mobile information security and privacy, this would suggest that individuals need to be aware of the risks related to their use of the mobile device. This is consistent with research on information security and privacy, although this research often relates awareness to behavioral intentions to protect oneself. For example, individuals who are aware of information security in general have a more positive attitude towards information security, with positive attitudes ultimately leading to compliance intentions [54]. Similarly, as users become aware of privacy threats online, they become more willing to change their online behaviors [55]. These studies, and others [e.g., 56], demonstrate that the nature of people's choice to perform information security and privacy related practices is driven by their awareness of the issues surrounding mobile environments. What is not known from prior research, however, is the link between the information (awareness) that individuals have and the development of their knowledge or skills. IMB Skills Model suggests that such a link exists. It would suggest that the more familiar a person is with the

information security and privacy issues that can arise from their use of mobile devices, the more likely they are to learn the skills that are needed to protect themselves.

The IMB Skills model suggests that motivation is required for behaviors to occur, and that such motivation include both personal motivation and social motivation. Personal motivation is related to individual affect and attitudes (personal attitude and reasons for performing the behavior), while social motivation deals with social support systems that can reinforce one's motivation (perception of support to engage in the behavior). Motivation is related to information as an individual needs to understand the concepts (e.g. the risks of smoking) to be motivated to enact a behavior (e.g., stop smoking). In the context of mobile information security and privacy, personal motivation can occur when one wants to protect oneself. Prior research suggests that a key motivator here can be a prior security or privacy invasion experience [23, 57]. For example, one bad experience of information privacy violation can change a consumer's perception of all companies in the marketplace [57] while people who have more favorable experiences have higher trust in Internet stores [58]. With a prior security or privacy invasion experience, the loss of personal information will likely lead to an increased motivation to protect oneself in the future. One prior study found that when information was collected covertly or without the mobile device user knowing about it [23], individuals perceived increased risks of using mobile devices. Other studies confirm that prior security or privacy invasion experiences increase individuals' concerns [59, 60].

In terms of social motivation, there is abundant research that suggests social norm influences individual technology related behaviors. In fact, several information security studies have used social influence concepts as determinants of information security behavioral intention [e.g., 50, 51]. A variety of concepts are inter-mixed, with some researchers using subjective norm [e.g., 61], overall social influence [62], or other forms of norms such as group norm or social norm [63, 64]. In the context of information security and privacy, we turn to more a more recent definition of social norm to reflect the social motivation of individuals in protecting themselves. Cialdini and Trost define social norm as "Rules and standards that are understood by members of a group, and that guide and/or constrain social behavior without the force of laws" [65 p. 152]. If one's important others believe they should protect their information on their mobile devices, individuals may be more willing to learn how to enact these protections, and to actually perform them. Just like the information component of the model, however, information privacy and security research has not yet tested the link between motivation and skills as proposed in the IMB Skills model.

The final component of the IMB Skills model is behavioral skills. The model suggests that both actual and perceived skills are necessary for individuals to be able to enact the behavior. Knowing about something and wanting to protect oneself is not sufficient if the individuals do not have the skills necessary to perform the required behavior. In this regard, adaptations of the IMB model vary, with some suggesting that self-efficacy is sufficient, while others emphasize the need to learn the actual skills necessary to enact the behavior. Self-efficacy is "the conviction that one can successfully execute the behavior required to produce outcomes" [66]. Since its initial conceptualization, a number of studies have applied the concept of self-efficacy to explain individual computer usage performance [e.g. 67, 68, 69]. As research has emerged in the information security literature, self-efficacy has also regularly been found to influence people's security behaviors [e.g. 36, 37, 50, 51, 52]. In the information privacy literature, self-efficacy has not been as regularly included but has been shown to influence intentions to follow a privacy policy [70] and to protect oneself on the Internet [71].

2.2. Knowledge-belief gap

While the IMB Skills model suggests that both perceived an actual abilities are necessary to enact a preventive behavior (Figure 2), most prior research on information security and privacy has focused mostly on measuring self-efficacy (a perceived ability) to evaluate knowledge [e.g., 37, 70, 72, 73]. Self-efficacy deals with one's perceived confidence at performing a behavior, such as utilizing a technology. Not surprisingly, there have been conflicting findings as to the role of self-efficacy in affecting security and/or privacy behaviors. Research suggests that a limiting factor to people performing protective behaviors is their lack of knowledge of technical tools to do so [74]. Likewise, we propose that actual knowledge is necessary to be able to mitigate information security and privacy issues. A survey conducted on behalf of the Privacy Commissioner of Canada suggests that over time individuals have been feeling less and less confident that they have the knowledge needed about how new technologies affect their personal privacy [75]. Further supporting the argument that knowledge is necessary to mitigate information security and privacy issues is a recent study in which knowledge of security actions via organizational policies was found to be different between organizations and led to differences in the performance of security actions [76].

Information security and privacy knowledge is likely to vary across different populations. Prior research suggests that older adults are less likely to be comfortable and knowledgeable about new technologies [77], suggesting that "the use of privacy tools on social network sites is not randomly distributed among users," and "some individuals' information and reputations may be more at risk than others" (p. 1650). Similarly, Li, Gupta, Zhang and Sarathy [78] suggest that some age groups are better able to take advantage of privacy tools to protect their privacy than others. Age may therefore impact privacy concerns and the resulting interest that individuals may have in protecting themselves. The information privacy literature has often examined how a set of determinants impact information privacy concerns, and the related behavioral intentions to share information, transact with a website, or protect oneself. Some studies have included covariates to reflect the thought that the digital divide may impact individuals' privacy or security protection intentions or practices. For example, individual characteristics found to impact willingness to share information include education [33] and age [78]. Age and education have also been found to affect concern for information privacy [26]. All of those prior studies did not examine the possible impacts of the differences within the samples beyond using demographics as covariates. While it would be valuable to understand why demographic variables impact security and privacy behaviors, prior research does not typically address this question, although there are exceptions [77].

In summary, we argue that in the context of information security and privacy, actual knowledge is necessary in addition to perceived abilities for individuals to understand the threats and to know how to use the mobile device settings to protect themselves from both information security and privacy threats. Therefore, we expand the IMB Skills model to include both self-efficacy and actual knowledge in the model. However, we suggest that a gap exists between the actual knowledge of an individual and that individual's perceived abilities. In other words, what an individual thinks he can do may be different from what the individual's actual knowledge is. Since there is limited research in this domain, we propose several research questions in the next section to explore this gap in future research.

3. The mobile privacy-security knowledge gap model

Based on the IMB Skills model discussed above, we propose the Mobile Privacy-Security Knowledge Gap Model presented in Figure 3. As illustrated in the Figure, there are three parts to framework, consistent with IMB – information and motivation, behavioral skills, and behaviors. The model illustrates the relationships between each of these sections within the information privacy and security contexts, as well as the gaps that exist between privacy and security, as well as between knowledge and beliefs. Resulting from this model is a research agenda, presented in the next sub-section.

The ultimate dependent variables in the proposed model are information privacy and security behaviors. In the mobile environment, protecting an individual's information security and/or privacy requires an actual behavior to be enacted. Prior research has suggested that intending to protect one's information privacy or security is not sufficient; one needs to actually use information protection practices to be protected [12] [76]. These information security and privacy protection practices should be holistic (limiting the amount of information provided via location-based information, browsing habits, and other settings; using a passcode; encrypting one's mobile device; etc.), as enacting only one protection is not sufficient [24].

3.1. Research agenda

The Mobile Privacy-Security Knowledge Gap Model extends the IMB Skills model in several ways. First, it provides a contextualization of the IMB Skills model to the mobile information privacy and security contexts. Second, the proposed model explicitly differentiates between actual knowledge and beliefs as behavioral skills. Finally, the model breaks down behavioral skills into technology, security and privacy knowledge and beliefs. Each of these areas lead to numerous research questions that can be explored in future research.

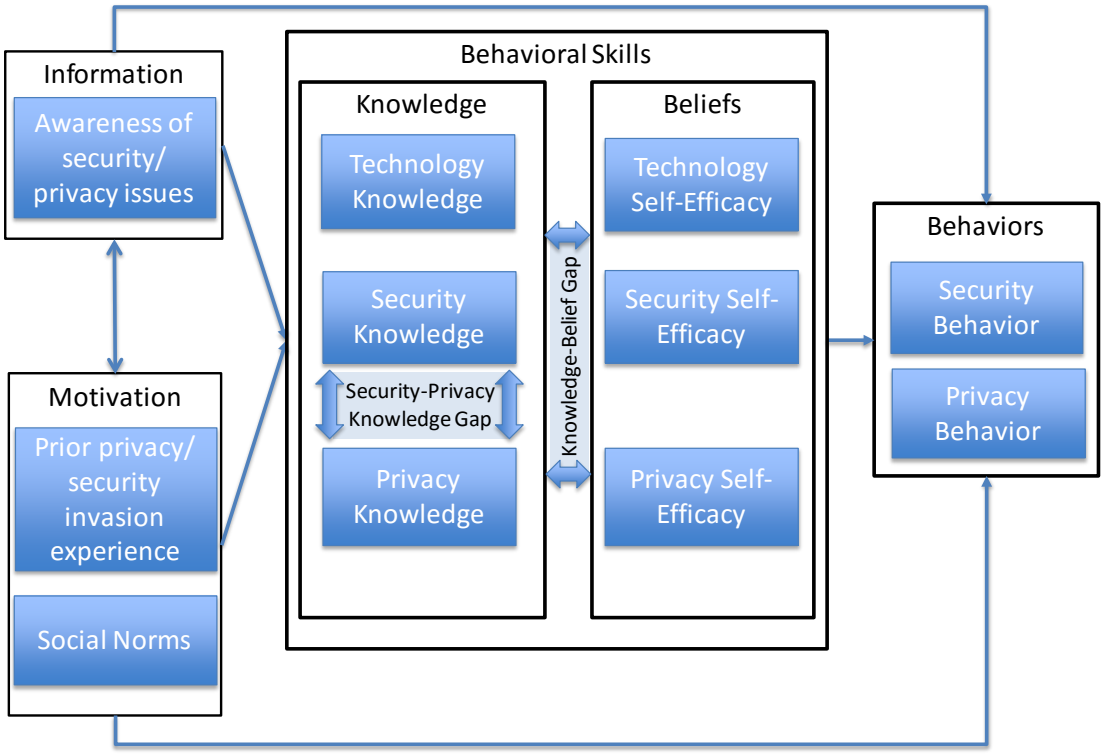

Figure 3. The Mobile Privacy-Security Knowledge Gap Model

3.1.1. Exploring the security-privacy knowledge gap. The prior discussion based on information security and privacy research shows that individuals might have different understandings of the use of their personal information when the context of study is a security threat as opposed to a privacy threat. This needs further testing, answering questions such as: how are individuals' information sharing decisions impacted by the security/privacy framing of a disclosure decision? What is the relative importance of the level of knowledge about information security and the level of knowledge about information privacy in affecting behaviors? These studies could be designed using experimental or quasi-experimental settings where actual knowledge can be tested and framing of disclosure of information as security or privacy could be manipulated.

3.1.2. Exploring the knowledge-belief gap. The IMB skills model suggests that knowing how to do something and believing you know what to do are important in enabling behaviors. However, this relationship has not yet been tested within information privacy or security contexts. Researchers could determine whether knowledge or beliefs is more important within this context. Furthermore, as knowledge is put into a nomological net of understanding privacy and security behaviors, future research could help to identify factors that lead to an increased level of knowledge.

3.1.3. Identifying determinants of knowledge. The IMB Skills model highlight the roles of having information and having motivation in determining both the skills and the ultimate protection behavior. While several studies have explored the roles of information factors such as awareness on information privacy or security behaviors [e.g., 54, 79], studies have typically not considered the effect of these on behavioral skills, whether self-efficacy or actual knowledge. Numerous studies can be conducted to answer questions such as: What factors besides awareness affect individual knowledge? What factors besides awareness affect individual self-efficacy and other behavioral skills beliefs? How are information factor sand motivation factors related in the contexts of information security and privacy? What is the relative effect of social norms in affecting knowledge, behavioral beliefs skills, and behaviors?

3.1.4. Developing artifacts to bridge the knowledge gaps. The Mobile Privacy-Security Knowledge Gap model identifies to key gaps that may affect how individuals protect their information privacy and security. While it is important to have research that provides an undertaking of the issues leading to these knowledge gaps and the consequences of these

knowledge gaps, it is also crucial to develop IT artifacts that can help improve privacy [14] and security behaviors. Such artifacts could target reducing the gap in knowledge between privacy and security, such as educational websites, apps, or other tools. Furthermore, IT artifacts can help reduce the knowledge-belief gap by providing hands-on training and self-evaluation.

4. Conclusion

The Mobile Privacy-Security Knowledge Gap model can serve as a foundation for future research to explore factors that lead individuals to perform desirable mobile information security and privacy protection practices. Given the global growth of mobile computing, and the related security and privacy risks, it is important to understand what will lead to such proactive behaviors. Since knowledge is not likely to be equally distributed [18], researchers need a better understanding of the effects mobile technologies have on the privacy and security of vulnerable individuals.

5. References

[1] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C., "Privacy Calculus Model in E-Commerce - a Study of Italy and the United States", European Journal of Information Systems, 15(4), 2006, pp. 389-402.

[2] Dinev, T., and Hart, P., "An Extended Privacy Calculus Model for E-Commerce Transactions", Information Systems Research, 17(1), 2006, pp. 61-80,100.

[3] Xu, H., Teo, H., Tan, B.C., and Agarwal, R., "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", Journal of Management Information Systems, 26(3), 2009-10, pp. 135-174.

[4] Pew Research Center, "Mobile Technology Fact Sheet", http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/, accessed June 6, 2016.

[5] Weise, E., "For 7% of Americans, Smartphone Is Only Link to Internet", http://www.usatoday.com/story/tech/2015/04/01/smartphone-dependent-7-pew/70672728/, accessed April 2, 2015.

[6] Duggan, M., and Rainie, L., "Cell Phone Activities 2012", http://www.pewinternet.org/2012/11/25/cell-phone-activities-2012/, accessed June 6, 2016.

[7] Lyon, D., "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique", Big Data & Society, 1(2), 2014, pp. 1-13.

[8] Molok, A., Nuha, N., Chang, S., and Ahmad, A., "Disclosure of Organizational Information on Social Media: Perspectives from Security Managers", Pacific Asia Conference on Information Systems (PACIS) 2013, 2013

[9] Kuzma, J.M., "Children and Geotagged Images: Quantitative Analysis for Security Risk Assessment", International Journal of Electronic Security and Digital Forensics, 4(1), 2012, pp. 54-64.

[10] Hern, A., "Apple Removes Malicious Programs after First Major Attack on App Store", http://www.theguardian.com/technology/2015/sep/21/apple-removes-malicious-programs-after-first-major-attack-on-app-store, accessed October 28, 2015.

[11] McCarthy, C., "ACLU Chapter Flags Facebook App Privacy", http://news.cnet.com/8301-13577_3-10318842-36.html, accessed December 23, 2013.

[12] Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R., "Future Directions for Behavioral Information Security Research", Computers & Security, 32(1), 2013, pp. 90–101.

[13] Bélanger, F., Hiller, J., and Smith, W.J., "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes", Journal of Strategic Information Systems, 11(3/4), 2002, pp. 245-270.

[14] Bélanger, F., and Crossler, R.E., "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", MIS Quarterly, 35(4), 2011, pp. 1017-1041.

[15] Smith, H.J., Dinev, T., and Xu, H., "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 35(4), 2011, pp. 989-1015.

[16] Enck, W., Gilbert, P., Seungyeop, H.A.N., Tendulkar, V., Byung-Gon, C., Cox, L.P., Jaeyeon, J., McDaniel, P., and Sheth, A.N., "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones", ACM Transactions on Computer Systems, 32(2), 2014, pp. 5:1-5:29.

[17] Bélanger, F., and Crossler, R.E., "Research in Progress: The Privacy Helper ©2013: A Tool for Mobile Privacy", Workshop for Information Technology and Systems (WITS), 2013

[18] Crossler, R.E., and Bélanger, F., "Mobile Information Privacy Protection Practices (MIP3)", IFIP WG8.11/11.13 Dewald Roode Workshop on Information Security, 2013

[19] Madden, M., "Public Perceptions of Privacy and Security in the Post-Snowden Era", http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/, accessed June 6, 2016.

[20] Bélanger, F., and Xu, H., "The Role of Information Systems Research in Shaping the Future of Information Privacy", Information Systems Journal, 26(6), 2015, pp. In Press.

[21] Norberg, P.A., Horne, D.R., and Horne, D.A., "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors", Journal of Consumer Affairs, 41(1), 2007, pp. 100-126.

[22] Sutanto, J., Palme, E., Tan, C.H., and Phang, C.W., "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users", MIS Quarterly, 37(4), 2013, pp. 1141-1164.

[23] Xu, H., Luo, X.R., Carroll, J.M., and Rosson, M.B., "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing", Decision Support Systems, 51(1), 2011, pp. 42-52.

[24] Crossler, R.E., and Bélanger, F., "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument", The Data Base for Advances In Information Systems, 45(4), 2014, pp. 51-71.

[25] Franko, O.I., and Tirrell, T.F., "Smartphone App Use among Medical Providers in ACGME Training Programs", Journal of Medical Systems, 36(2012, pp. 3135-3139.

[26] Zhang, R., Chen, J.Q., and Lee, C.J., "Mobile Commerce and Consumer Privacy Concerns", Journal of Computer Information Systems, 53(4), 2013, pp. 31-38.

[27] Wilson, T., "Researchers: Mobile Applications Pose Rapidly Growing Threat to Enterprises", http://www.darkreading.com/researchers-mobile-applications-pose-rapidly-growing-threat-to-enterprises/d/d-id/1269361, accessed June 8, 2016.

[28] Perez, S., "After Getting Booted from Apple's App Store, Mobile Privacy App Clueful Returns on Android", http://techcrunch.com/2013/05/21/after-getting-booted-from-apples-app-store-mobile-privacy-app-clueful-returns-on-android/, accessed June 7, 2016.

[29] Conger, S., Pratt, J.H., and Loch, K.D., "Personal Information Privacy and Emerging Technologies", Information Systems Journal, 23(5), 2013, pp. 401-417.

[30] Thompson, C., "Cybercriminals Are Coming after Your Mobile Apps: Experts", http://www.cnbc.com/id/100755795, accessed June 6, 2016.

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

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

[33] Anderson, C.L., and Agarwal, R., "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information", Information Systems Research, 22(3), 2011, pp. 469-490.

[34] Jiang, Z., Heng, C.S., and Choi, B.C.F., "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions", Information Systems Research, 24(3), 2013, pp. 579-595.

[35] Sheng, H., Nah, F.F.-H., and Siau, K., "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns", Journal of the Association for Information Systems, 9(6), 2008, pp. 344-376.

[36] Crossler, R.E., "Protection Motivation Theory: Understanding Determinants to Backing up Personal Data", 43rd Hawaii International Conference on System Sciences (HICSS), 2010, pp. 1-10.

[37] Herath, T., and Rao, H., "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", European Journal of Information Systems, 18(2), 2009, pp. 106-125.

[38] Rogers, R.W., "A Protection Motivation Theory of Fear Appeals and Attitude Change", Journal of Psychology: Interdisciplinary and Applied, 91(1), 1975, pp. 93-114.

[39] Rogers, R.W., Prentice-Dunn, S., and Gochman, D.S., "Protection Motivation Theory": Handbook of Health Behavior Research 1: Personal and Social Determinants., Plenum Press, 1997, pp. 113-132.

[40] Fisher, J.D., and Fisher, W.A., "Changing Aids Risk Behavior", Psychological Bulletin, 111(3), 1992, pp. 455-474.

[41] Fisher, J.D., and Fisher, W.A., "The Information-Motivation- Behavioral Skills Model of Aids Risk Behavior Change: Empirical Support and Applications", in (Oskamp, S., and Thompson, S., 'eds.'): Understanding and Preventing Hiv Risk Behavior: Safer Sex and Drug Use, Sage, Thousand Oaks, CA, 1996, pp. 100-127.

[42] Fisher, J.D., and Fisher, W.A., "Theoretical Approaches to Individuallevel Change in Hiv-Risk Behavior", in (Peterson, J., and Diclemente, R., 'eds.'): The Hiv Prevention Handbook, Plenum, New York, NY, 2000, pp. 3-55.

[43] Fisher, J.D., Fisher, W.A., Williams, S.S., and Malloy, T.E., "Empirical Tests of an Information-Motivation-Behavioral Skills Model of Aids-Preventive Behavior with

Gay Men and Heterosexual University Students", Health Psychology, 13(3), 1994, pp. 238-250.

[44] Misovich, S.J., Fisher, J.D., Martinez, T., Bryan, A., and Catapano, N., "Predicting Breast Self-Examination: A Test of the Inforamtion-Motivation-Behavioral Skills Model", Journal of Applied Social Psychology, 33(4), 2003, pp. 775-790.

[45] Boldero, J., Sanitioso, R., and Brain, B., "Gay Asian Australians' Safer-Sex Behavior and Behavioral Skills: The Predictive Utility of the Theory of Planned Behavior and Cultural Factors", Journal of Applied Social Psychology, 29(10), 1999, pp. 2143-2163.

[46] Anderson, E.S., Wagstaff, D.A., Heckman, T.G., Winett, R.A., Roffman, R.A., Solomon, L.J., Cargill, V., Kelly, J.A., and Sikkema, K.J., "Information-Motivation-Behavioral Skills (IMB) Model: Testing Direct and Mediated Treatment Effects on Condom Use among Women in Low-Income Housing", Annals of Behavioral Medicine, 31(1), 2006 pp. 70-79.

[47] Ajzen, I., "The Theory of Planned Behavior", Organizational behavior and human decision processes, 50(2), 1991, pp. 179-211.

[48] Ajzen, I., and Fishbein, M., "Attitudes and Normative Beliefs as Factors Influencing Intentions", Journal of Personality and Social Psychology, 21(1), 1972, pp. 1-9.

[49] Ajzen, I., and Fishbein, M., Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ, 1980.

[50] Johnston, A.C., and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS Quarterly, 34(3), 2010, pp. 548-566.

[51] Liang, H., and Xue, Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", Journal of the Association for Information Systems, 11(7), 2010, pp. 394-413.

[52] Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R., "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security", European Journal of Information Systems, 18(2), 2009, pp. 151-164.

[53] Glasford, D.E., "Predicting Voting Behavior of Young Adults: The Importance of Information, Motivation, and Behavioral Skills", Journal of Applied Social Psychology, 38(11), 2008, pp. 2648-2672.

[54] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS Quarterly, 34(3), 2010, pp. 523-548.

[55] Malandrino, D., Scarano, V., and Spinelli, R., "Impact of Privacy Awareness on Attitudes and Behaviors Online", Science, 2(2), 2013, pp. 65-82.

[56] Sheehan, K.B., and Hoy, M.G., "Dimensions of Privacy Concern among Online Consumers", Journal of Public Policy & Marketing, 19(1), 2000, pp. 62-73.

[57] Pavlou, P.A., and Gefen, D., "Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role", Information Systems Research, 16(4), 2005, pp. 372-399.

[58] Liping, L., Chan, L., and Dan, Z., "A New Approach to Testing Nomological Validity and Its Application to a Second-Order Measurement Model of Trust", Journal of the Association for Information Systems, 13(12), 2012, pp. 950-975.

[59] Xu, H., Gupta, S., Rosson, M.B., and Carroll, J.M., "Measuring Mobile Users' Concerns for Information Privacy", Thirty Third International Conference on Information Systems (ICIS), 2012

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

[61] Johnston, A.C., and Warkentin, M., "Fear Appeals and Informaiton Security Behaviors: An Empirical Study", MIS Quarterly, 34(3), 2010, pp. 548-566.

[62] Venkatesh, V., Morris, M., Davis, G.B., and Davis, F.D., "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly, 27(3), 2003, pp. 425-478.

[63] Sherif, M., The Psychology of Social Norms, Harper & Row, New York, NY, 1936.

[64] Turner, J.C., Social Influence, Brooks/Cole Publishing Company, Pacific Grove, CA, 1991.

[65] Cialdini, R.B., and Trost, M.R., "Social Influence: Social Norms, Conformity and Compliance", in (Gilbert, D.T., Fiske, S.T., and Lindzey, G., 'eds.'): The Handbook of Social Psychology, 4th Edition, McGraw-Hill, Boston, MA, 1998, pp. 151-192.

[66] Bandura, A., "Self-Efficacy: Toward a Unifying Theory of Behavioral Change", Psychological Review, 84(2), 1977, pp. 191-215.

[67] Compeau, D., Higgins, C.A., and Huff, S., "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study", MIS Quarterly, 23(2), 1999, pp. 145-158.

[68] Compeau, D.R., and Higgins, C.A., "Application of Social Cognitive Theory to Training for Computer Skills", Information Systems Research, 6(2), 1995, pp. 118-143.

[69] Johnson, R.D., and Marakas, G.M., "Research Report: The Role of Behavioral Modeling in Computer Skills Acquisition - toward Refinement of the Model", Information Systems Research, 11(4), 2000, pp. 402-417.

[70] Warkentin, M., Johnston, A.C., and Shropshire, J., "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention", European Journal of Information Systems, 20(3), 2011, pp. 267-284.

[71] Sangmi, C., Bagchi-Sen, S., Morrell, C., Rao, H.R., and Upadhyaya, S.J., "Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens", IEEE Transactions on Professional Communication, 52(2), 2009, pp. 167-182.

[72] Anderson, C.L., and Agarwal, R., "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions", MIS Quarterly, 34(3), 2010, pp. 613-643.

[73] Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., and Greer, C., "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior", International Journal of Human-Computer Studies, 71(12), 2013, pp. 1163-1173.

[74] Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S., "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security", Symposium on Usable Privacy and Security (SOUPS), 2015

[75] Phoenix Strategy Perspectives, "Survey of Canadians on Privacy-Related Issues", https://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.pdf, accessed June 8, 2016.

[76] Blythe, J.M., Coventry, L., and Little, L., "Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors", Symposium on Usable Privacy and Security (SOUPS), 2015

[77] Litt, E., "Understanding Social Network Site Users' Privacy Tool Use", Computers in Human Behavior, 29(4), 2013, pp. 1649-1656.

[78] Li, H., Gupta, A., Zhang, J., and Sarathy, R., "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract", Decision Support Systems, 57(January), 2014, pp. 376-386.

[79] Hu, Q., Hart, P., and Cooke, D., "The Role of External and Internal Influences on Information Systems Security - a Neo-Institutional Perspective", The Journal of Strategic Information Systems, 16(2), 2007, pp. 153-172.