Influence of Users' Privacy Risks Literacy on the Intention to Install a Mobile Application

Alessio De Santo and Cédric Gaspoz

Information Systems and Management Institute, HES-SO // University of Applied Sciences Western Switzerland, HEG Arc, Neuchâtel, Switzerland
{alessio.desanto,cedric.gaspoz}@he-arc.ch

Abstract. While users are increasingly embracing smartphones worldwide, these devices, storing our most personal information, are repeatedly found to be leaking users' data. Despite various attempts to inform users of these privacy issues, they continue to adopt risky behaviors. In order to better protect users of these devices, we need to understand the antecedents of the decision to install potentially privacy-threatening applications on them. We ran a large experiment in order to determine the influence of privacy risks literacy on the intent to install a potentially privacy threatening application on a smartphone. Using partial least squares (PLS), we were able to find that more than the privacy risks literacy, it is the coping behavior literacy that influences the user's decision to install a mobile application. These findings are relevant to help determine a course of action in order to increase the user's privacy protection when using such devices.

Keywords: Privacy risk literacy, coping behavior, smartphone, protection motivation theory.

1 Introduction

More and more people are adopting smartphones worldwide. Agenda, address book, email reader, camera, versatile storage and GPS are all integrated in these devices. However, while conveniently storing our personal data, these devices can turn out to be silently leaking our private information. Stories of devices leaking personal information to third parties such as network operators, application developers, advertisers and device manufacturers appear frequently in the headlines. Recent results from online social networks show that users' intentions to install potentially privacy-invasive applications are influenced by the perceived benefits and risks resulting from their use, which are in turn moderated by the privacy controls provided to the user by the application. However, in the context of mobile device applications, the user may be unaware of the privacy invasiveness of an application that is able to access stored personal data for other purposes without the user's knowledge.

Due to the very nature of smartphone applications, we need to rethink how we assess the way people are interacting with them. When purchasing a smartphone, people not only buy a physical device, but they can then access hundreds of thousands

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_33

of applications through various online stores. The goal of these stores is to profit from enhancing the user experience on the device and to provide additional resources to device manufacturers or operating system developers. However, while selling applications with low price tags, application developers are encouraged to embed additional features in order to increase their revenues, mostly by reselling consumer profiles. One can argue that people are nowadays generally aware of these practices, since they are in widespread use on the mainstream Web.

However, a significant difference between using mobile applications and browsing the Web is that on the latter, people are more conscious of the information they are providing to third parties. When readers want to access newspaper websites, for example, they are required to provide personal information (for example a valid email address or some demographic information) and they are informed, for example through terms and conditions, that this information can be stored by the proprietor of the website or resold to third parties. In the case of mobile applications, the user already has a lot of personal information stored on the device for various purposes. When installing a new application, that application will request rights to access smartphone functions such as network access, access to stored personal information, access to capture devices, etc. Thus, by installing the application, the user is granting, consciously or unconsciously, access to the personal information stored on the device.

To understand user decision making in this context, we need to study how user privacy threats and coping behaviors literacy influences the perceived benefits of using a specific application. Protection motivation theory (PMT) postulates that attitude change is a function of the amount of protective motivation aroused by the cognitive appraisal processes [11]. Both threat and coping appraisal cognitive processes are triggered by information gathered from a variety of sources, which could be environmental or intrapersonal, and the threat appraisal process can also be initiated by a 'fear appeal'. We postulate that, in the context of choosing to install a mobile application, the principal source of information that triggers the cognitive appraisal processes is the users' literacy on privacy risks and coping behaviors. In order to understand the influence of the users' privacy risks and coping literacy on the intent to install a specific application, we set up an experiment in which we manipulated the users' privacy risk literacy. This experiment showed that varying this literacy impacts the users' intent to install a given application.

2 Privacy Protection

The advent of the information age, the widespread use of the Internet to communicate, share or exchange information, and advances in mobile computing have given rise to concerns over violation of user privacy. Consequently, information privacy has become one of the core topics in information systems (IS) research [14]. For our research, we use the Stone et al. (1983) [18] definition of information privacy as 'the ability (i.e. capacity) of the individual to control personally (vis-à-vis other individuals, groups, organizations, etc.) information about one's self.' This led us to

differentiate two ways of controlling personal information: (1) restricting the information we share and (2) restricting the way that information is shared.

Research into users' intent to install applications or technologies that may carry privacy risks is presented in the leading IS journals and conferences. The applications studied include electronic health records [2], e-commerce [12], direct marketing [17], home computing [1], radio frequency identification [9] and social networks [3]. A recent review of information privacy research [16] reviewed all publications on privacy in management information systems and concluded that 'positivist empirical studies will add the greatest value if they focus on antecedents to privacy concerns and on actual outcomes'. They found that few researchers studied both the antecedents and the outcomes of privacy concerns; most publications study either the effects of antecedents on privacy concern or the effects of privacy concerns on outcome.

Studies addressing this topic often rely on the theory of planned behavior, the theory of reasoned action, rational choice theory, general deterrence theory or the theory of protection motivation. However, the majority of these studies made some assumptions as to the ability of the user to make an informed decision in these privacy risk contexts and found that users tended to underestimate the threat to their information security. However, none of the research tests the root cause of this failure to correctly assess information security threats. A partial explanation of the fact that people can be concerned about their privacy and at the same time readily hand over sensitive personal information, comes from Bennett (2011) [4] who conceptualized the notion of privacy as a commodity. 'Under the commodity view, privacy is still an individual and societal value, but it is not absolute, as it can be assigned an economic value and be considered in a cost–benefit calculation at both individual and societal levels' [16]. However, in the context of mobile applications, there is a gap between the valuation of information stored on the phone (for example in case of theft or loss of the device) and users' perceived valuation of the privacy risks associated with those applications. This gap can therefore not be fully explained by the commodity view; further explanation could include the cognitive process itself, the lack of information available to application users or simply by the users' overconfidence in their own capabilities.

The protection motivation theory (PMT) [11] postulates that first information is received. Then this information initiates a cognitive mediating process. This process evaluates the response options toward the perceived situation. Finally, the result of these mediating processes, the threat appraisal and the coping appraisal, determines the reaction toward the situation. In this theory, information sources are the input variables of the model and are categorized as environmental and intrapersonal. Environmental sources being composed by verbal persuasion and observational learning. The intrapersonal information sources include personality characteristics and prior experience. Thus, by studying information sources, we can understand the user behavior when confronted with the intention to install a new application on a smartphone.

3 Hypotheses Development

In order to study the intention to install an application on a smartphone, we will study the influences of the protection motivation process and the mobile application's characteristics on users' decisions. We seek to understand the effect of the protection motivation on the intention to install a particular smartphone application. In this context, we postulate that the higher the protection behavior, the lower is the intent to install the applications that could potentially be privacy threatening. We also postulate that the intrinsic characteristics of a particular application will have some moderating effects on the intent to install it. Again, as the risk rises, the intention will decrease.

- **H1**: *Users' privacy risk literacy will be negatively correlated to the intention to install an application*
- **H2**: *Users' coping behavior literacy will be positively correlated to the intention to install an application*
- **H3**: *Application's potential risks toward the users' privacy will be negatively correlated to the intention to install an application*

As stated above, PMT describes how the sources of information and the fear appeal influence the development of protection behavior. The information is used during two cognitive processes: threat appraisal and coping appraisal. In PMT, both processes are direct antecedents of the protection behavior. Environmental information includes verbal persuasion and observational learning. In the context of this study, we will only study observational learning. We postulate that verbal persuasion will be part of the experiment, given that participants are told that, in order to support the development of mobile applications, they will have to decide which application will have the best chances on the markets. Thus, given the experimental protocol used, we assume an equal effect on all participants. To operationalize observational learning, we differentiate coping behaviors and privacy risks literacy. These two constructs summarize the extent of literacy in both domains. As PMT makes the difference between threat and coping appraisal, we will measure each one independently.

The second type of source of information is the intrapersonal one. This source comprises personality aspects, as well as prior experience with related situations. In order to measure intrapersonal information, we use the reflective global information privacy concern (GIPC) construct. This allows us to measure the user's past experience with the transmission of privacy related information. This construct will directly influence the attitude of the user, the privacy risk literacy and the coping behavior. A higher concern about information privacy should influence negatively the intention to install a privacy threatening application and should reflect a better literacy in both risks and coping behaviors.

- **H4**: *Global information privacy concern will be positively correlated to the privacy risks literacy*
- **H5**: *Global information privacy concern will be negatively correlated to the intention to install an application*
- **H6**: *Global information privacy concern will be positively correlated to the coping behaviors literacy*

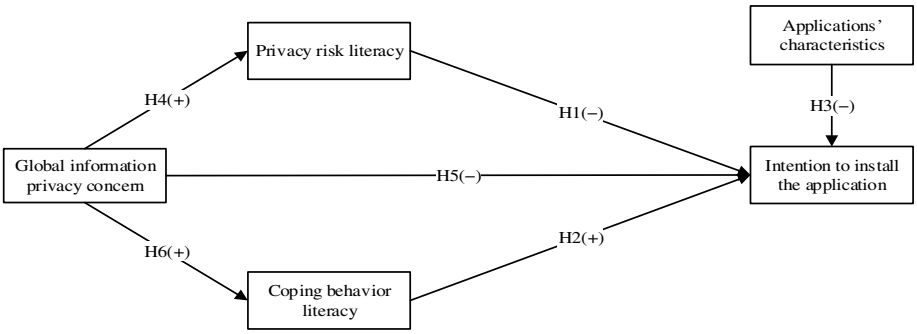

Fig. 1. Proposed research model

The final research model (Figure 1) clearly represents the antecedents of the intention to install and use smartphone applications. This intention depends on the application characteristics, users' privacy risks literacy, users' coping behaviors literacy and users' global information privacy concern.

4 Methodology

In order to explore our model (Figure 1), we conducted an experiment during which users' privacy risks literacy and applications' characteristics were variable. The experiments consisted of a height sections survey subjected to 1200 people. The survey was introduced as a preliminary project to determine the criteria of adoption of a fictive mobile tourist application. The first section was a basic demographic survey including questions concerning the use of smartphones. Section 2 measured the GIPC of the respondents. To measure the GIPC, we used an existing and approved scale [17]. In section 3, the respondents' privacy risk literacy was measured, followed by the coping behavior literacy in section 4. Section 5 presented two possible scenarios of our application, a low privacy threatening scenario and a high privacy threatening scenario. Each scenario was characterized by expected features and required permissions. The respondents had to rate their intention to install the application on a five-point Likert scale. In section 6, the respondents' privacy risk literacy was manipulated. A recent article from a reputable newspaper was presented to the respondent. In the article, the author presented the privacy risks of applications' permissions acceptance and illustrated it with the very popular Facebook Messenger application. In order to test their understanding of the texts, we asked each subject three comprehension questions about the text they had just read. After the manipulation, the subject was then again asked to read the descriptions of two mobile applications scenarios (one application presenting high privacy risks and the other presenting low privacy risks) and to decide if they would install them on their mobile

device. Finally, in section 8 we measured the respondents' privacy risk literacy again, with the same measurement items as in section 4 but shuffled. The respondents were remunerated for their work.

To measure the impact of the manipulation, 307 surveys were allocated to a control group. In this group, the manipulation text was replaced by a simple and non-manipulating article relating the success story of a similar tourism application in a European country.

4.1.1 Users' Privacy Risk Literacy Measurement

Based on the Google Android developer documentation, we retrieved all the existing mobile application permissions. Permissions accessing to private data were selected and categorized in seven different groups of data. Tests of correlation were used to ensure these categories were mutually exclusive. Finally corresponding privacy questions (Q1 to Q7 in Table 1) were formulated to measure the users' privacy risk literacy.

Table 1. Users' privacy risk literacy measurement items

Privacy risk issues	*Category*	*Android Permissions*
(Q1) It is likely that your movements are recorded and relayed	Location	access_coarse_location, access_fine_location, access_location_extra_command, access_mock_location,
(Q2) It is likely that your smartphone's settings and status are relayed	System settings and status	access_wifi_state, battery_stats get_tasks, read_phone_state, read_sync_settings, read_sync_stats
(Q3) It is likely that an application retrieves the entire list of your contacts	Profile and contacts	get_accounts, read_contacts, read_call_log,
(Q4) It is likely that your messages and social streams are browsed, to extract potential confidential information	Messages and social	read_sms, read_social_stream, read_user_dictionary
(Q5) It is likely that your user profile and interests are analyzed and relayed	User profile and interests	read_profile, subscribed_feeds_read, read_history_bookmarks,
(Q6) It is likely that the content of your smartphone's agenda is relayed	Calendar	read_calendar
(Q7) It is likely that the publisher of the application accesses the pictures and videos stored on your smartphone	Audio, photo and video	record_audio, camera, read_external_storage

4.1.2 Coping Behavior Literacy Measurement

Based on the privacy risk literacy measurement item, we developed the coping behavior literacy measurement items.

Table 2. Users' coping behavior measurement items

Coping behavior	*Privacy risks*
(Q8) It is effective to block communication networks to prevent data transfers	Q1–Q7
(Q9) ... to paste a sticker on my camera so it does not capture photos / videos without my knowledge	Q7
(Q10) ... to control my bills in order to detect anomalies	Q1–Q7
(Q11) ... to encrypt my data to make it unreadable to malicious persons	Q4, Q6, Q7
(Q12) ... to deny access to the data stored on my phone	Q1–Q7
(Q13) ... to control the transfer of data over Internet	Q1–Q7

4.1.3 Applications' Characteristics

In order to determine low and high privacy threatening permissions, we conducted an experiment involving a common application scenario and several sets of permissions associated. The sets of permissions were mostly elaborated in regard to the application features but also including some unrelated and therefore privacy threatening permissions (from Table 1). The experiment came up with two sets of permissions that were generally considered to be 'low' privacy threatening and two others that were generally perceived as 'high' privacy threatening.

The experiment consisted of asking participants to rank eleven sets of permissions developed, on a three-level scale going from totally acceptable to totally unacceptable. In order to avoid any bias due to systematic reflection, the order of the permissions in the different sets was shuffled. No logical structure or sequence of permission could therefore have been detected. Moreover, all of the statement sets contained similar numbers of words, with four or five permission statements in each. The authors then ranked these eleven sets based on their level of threat (low, middle, high) having reached agreement on the content.

For each set of permissions presented, we measured the behavioral intent, prediction and plan to install the application on a five-point Likert scale, from 'strongly agree' to 'strongly disagree'. The question on planning to install the application was inverted, that is, measuring the intent to not install, in order to check the validity of the survey [10].

5 Data Analysis

We used various techniques to clean the collected data. The first one eliminated all the respondents who completed the survey in less than 4 minutes; this was considered the minimum time to comprehend the experiment. The second filter consisted of a reverse record check [13] on the four applications' installation proposals. We then used the comprehension questions asked at the end of section 6 to eliminate further

records. The last filter retained only people who owned a Google Android smartphone, in order to ensure understanding of the problem by the respondents. After this cleaning process, 426 records remained exploitable.

The final demographic data of the participants are shown in Table 3. The majority of them are male undergraduates between 26 and 35. Almost all the participants (93.9%) had at least six months' experience with a smartphone. All the participants currently own a Google Android smartphone (due to the data cleaning process).

Table 3. Demographic information

	# of participants	*Percentage (%)*
Gender		
Male	301	70.65
Female	125	29.34
Age		
18–25	93	21.83
26–35	156	36.62
36–45	127	29.81
46–55	32	7.51
older than 56	18	4.23
Education		
Primary School Degree	12	2.82
High School Degree	135	31.69
Certificate / Diploma Degree	96	22.54
Bachelor Degree	131	30.75
Master Degree	48	11.27
Doctorate	4	0.94
Global experience with a smartphone		
Less than 6 months	26	6.10
From 6 to12 months	43	10.09
From 1 to 2 years	80	18.78
From 2 to 3 years	86	20.19
More than 3 years	191	44.84

Partial least squares (PLS) [6], a variance-based structural equation modelling (SEM) analysis technique [5], was used for assessing our model and hypothesis. Since the aim of our research was to predict an intention and not to confirm a theory or a phenomenon, the use of PLS–SEM was suitable [15]. Users' risks privacy literacy, users' coping behavior literacy, demographic information and applications characteristics were each conceptualized as first-order formative constructs. Users' GIPC and intention to install the application were conceptualized as first-order reflective constructs.

Composite reliability scores of the reflective constructs were all above 0.70, confirming the validity of these. The Applications' Characteristics being a single-item construct, the conventional reliability and convergent validity assessments were inappropriate.

Table 4. Formative constructs before/after manipulation

Group	*Items*	*Mean*	*S.D.*	*Weight*	*Group Mean*	*Group S.D.*
Users' risk privacy literacy from 1 (very unlikely) to 5 (very likely)	Q1	3.23/3.54	1.28/1.34	–0.10/0.66	3.36/ 3.59	1.32/ 1.37
	Q2	3.53/3.58	1.35/1.44	0.61/1.48		
	Q3	3.65/3.80	1.21/1.26	0.20/0.42		
	Q4	3.40/3.63	1.32/1.40	–1.26/–0.57		
	Q5	3.23/3.42	1.38/1.42	0.15/-0.65		
	Q6	3.03/3.40	1.43/1.46	1.25/0.67		
	Q7	3.48/3.74	1.23/1.24	–0.28/–1.46		
Users' coping behavior literacy from 1 (very ineffective) to 5 (very effective)	Q8	3.42	1.06	0.10/0.45	3.57	1.15
	Q9	3.15	1.45	0.24/–0.11		
	Q10	3.56	1.16	–0.51/–1.11		
	Q11	3.89	1.13	0.88/0.47		
	Q12	3.70	1.06	0.46/0.19		
	Q13	3.71	1.05	–0.16/0.12		

5.1 Effects of the Manipulation

Before any manipulation, we predicted that the likelihood of a subject intending to install an application was 17.3%, based on the coping behavior literacy, the users' privacy risk literacy, the GIPC and the applications' characteristics. The users' coping behavior literacy was the most influential construct, exerting a positive influence of 24.2% versus the negative influence of 5.4%, 18.7% and 22.0% of the applications' characteristics, the users' privacy risk literacy and GIPC. It was also interesting to note that the GIPC determined 14.1% of the users' privacy risk literacy, with 37.6% of influence.

T-statistics were used to test the proposed hypotheses for the standardized path coefficients, by specifying the same number of cases that existed in the dataset and bootstrapping 500 re-samples. The model fit was determined through strong path coefficients significant at $p<0.01$. One-tailed t-tests were used, as the hypotheses were all direction specific.

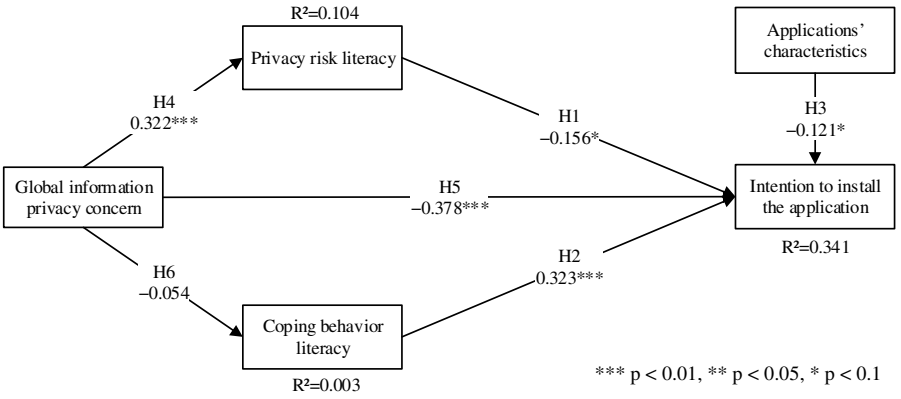

Fig. 2. Model results after manipulation

After the users' privacy risk literacy manipulation, the intention to install an application was predicted at 34.1% by the coping behavior literacy, the users' privacy risk literacy, the GIPC and the applications' characteristics. In other words, we almost doubled the prediction of the intention to install the application, and the elements were 16.9% more predictive than before the manipulation. In that assertion, the GIPC was the most influencing construct with a negative influence of 37.8%, followed by the users' coping behavior literacy with a positive influence of 32.3%, the users' privacy risk literacy with a negative influence of 15.6% and finally the applications' characteristics with a negative influence of 12.1%. The GIPC influences significantly the users' privacy risk literacy but not the users' coping behavior literacy, which suggests that something else influences the users' coping behavior literacy, it could certainly be the behavioral experience, but this is beyond the scope of this study. The weight of each item demonstrated the item's contribution to the construct. We retained non-significant indicators to preserve content validity [5].

Table 5. Descriptive statistics, psychometric measurement validation and correlations for reflective measures

	Indicator	*Indicator Reliability*	*AVE*	*Composite Reliability*	*Discriminant Validity*
GIPC	gipc_1	0.67	0.78	0.91	Yes
	gipc_2	0.81			
	gipc_3	0.86			
Intention to install the application	install_1	0.97	0.97	0.99*	Yes
	install_2	0.98			
	install_3inv	0.96			

As explained above, we had two reflective constructs: GIPC and the intention to install the application. The reliability and validity of the reflective measures were achieved (composite reliability (CR) > 0.70); average variance extracted (AVE) > 0.50) (see Table 5). The square root of the AVE for each construct was greater than the correlations with other factors, which means that the satisfactory discriminant validity was also achieved (see Table 5), and the cross-loadings show each item loading higher on its own factor than on others (see Table 6).

Table 6. Loadings and cross-loadings for reflective measures

Indicators	***GIPC***	***Intention to install an application***
gipc_1	**0.820**	–0.318
gipc_2	**0.901**	–0.366
gipc_3	**0.929**	–0.469
install_1	–0.442	**0.986**
install_2	–0.428	**0.988**
install_3inv	–0.442	**0.982**

6 Discussion

For the first time, a study examines the antecedents of the intention to install an application on smartphones. Results are interesting, given that we are able to predict more than 34% of the intention with our constructs. Following our intuition, **H1**, **H2** and **H3** are all verified. This allows, for the first time, to use PMT in order to enlighten the tradeoffs between privacy risks and intention to install an application. Past researchers have examined this question through the lens of privacy calculus theory [7], which includes information disclosure as a tradeoff of benefits and risks. Here we are able to use objective information in order to predict the intention. Indeed, benefits and risks, especially with sensitive information, are very difficult to assess. How valuable is my email address, my mobile phone number, or my current localization? It is very difficult to make an objective evaluation of the value of this information. It is also challenging to estimate the expected benefits from the use of a given application. Therefore, by using objective evaluations of one's literacy in privacy risks and coping behavior we have a much more appropriate prediction of one's intention to use a mobile application. Moreover, by predicting more than 34% of the intention, our model opens new opportunities to develop programs and policies to increase the protection of smartphone users.

The second assumption that we made in our model is that protection motivation and, ultimately, intention to use an application are user dependent. We cannot expect all users to have the same sensitivity regarding their personal information. Some are happy to share it in exchange for some sort of service while other will probably never trade it. Our hypotheses **H4**, **H5** and **H6** validate that GIPCs have a direct influence on the privacy risks literacy, the intention to install an application and on the coping behavior literacy. Given that all three hypotheses are verified, we can validate our global approach in prediction users' intention in this context.

The results of our study provide evidence that as the level of users' privacy risk literacy increases, the protection motivation report increases and directly impacts on the willingness to install or use an application. Our findings also suggest that increases in users' privacy risk literacy increases the influence of the characteristics of the application. Simply stated, users who are more conscious of the privacy risks are less prone to install an application independently of the characteristics of the application. Therefore, to protect users from confidential data loss, it would be effective to act on their privacy risk literacy.

These results are very interesting as they validate our assumption that, in the context of mobile applications, the privacy as a commodity view [4] could no longer hold, as the users are no longer aware of the magnitude of private information that they share with application editors. Thus, we need to further study the implications of users' literacy on their decisions to install and use mobile applications, in order to better protect smartphone users against unintentional leakage of private information. Moreover, this could also assist OS editors in developing some sort of risk training in their software in order to increase the privacy risks literacy for their user base.

There are many opportunities to further explore this subject. It seems that very often the awareness context [8] of the user in deciding to install a mobile application

is very low. This is not because the risk information is unavailable, but because most users do not bother to consult it, or they simply do not want to know about it. We need to further study the awareness context of the users, as well as the antecedents to a move from one context to the other. Using the awareness context theory in future research on privacy risks with mobile applications should help researchers to understand how users are evaluating their trust in application developers. This should then help policymakers in designing public awareness campaigns on mobile applications' privacy risks.

7 Conclusion

This study presents a new model to predict the user's intention to install a smartphone application based on PMT. Validated by a large experiment, our model uses objective measures of the privacy risks literacy and the coping behavior literacy in order to predict the intention to install an application with specific characteristics. This model voluntarily departs from the traditional risks/benefits explanation of these behaviors, given that first, users are unable to assess the value of both risks and benefits, and second, that the risk may occur long after the installation of the application.

We suggest that this model can be used to develop more effective ways to help users of these devices to protect their privacy. This is a necessary advance, given the increased amount of information that is stored on smartphones. With the evolution of the technology, more and more people are storing medical records captured by external sensors or financial transactions carried out through mobile payment services that have a high value for resellers of personal profiles. By showing the antecedents of the intention, our model will assist policymakers and developers in protecting smartphone users from increased attempts to access their personal information.

References

1. Anderson, C.L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q 34(3), 613–643 (2010)
2. Angst, C.M., Agarwal, R.: Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. MIS Q 33(2), 339–370 (2009)
3. Bélanger, F., Crossler, R.E.: Privacy in the digital age: a review of information privacy research in information systems. MIS Q 35(4), 1017–1042 (2011)
4. Bennett, C.: In defense of privacy: the concept and the regime. Surveill 8(4), 485–496 (2011)
5. Bollen, K., Lennox, R.: Conventional wisdom on measurement: A structural equation perspective. Psychol. Bull. 110(2), 305–314 (1991)
6. Chin, W.W.: Commentary: Issues and Opinion on Structural Equation Modeling. Manag. Inf. Syst. Q. 22(1), vii–xvi (1998)
7. Dinev, T., Hart, P.: An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res. 17(1), 61–80 (2006)

8. Glaser, B.G., Strauss, A.L.: Awareness Contexts and Social Interaction. Am. Sociol. Rev. 29(5), 669–679 (1964)
9. Günther, O., Spiekermann, S.: RFID and the perception of control. Commun. ACM. 48(9), 73–76 (2005)
10. Johnston, A.C., Warkentin, M.: Fear appeals and information security behaviors: an empirical study. MIS Q 34(3), 549–566 (2010)
11. Maddux, J.E., Rogers, R.W.: Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19(5), 469–479 (1983)
12. Malhotra, N.K., et al.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Inf. Syst. Res. 15(4), 336–355 (2004)
13. Öztaş Ayhan, H., Işiksal, S.: Memory recall errors in retrospective surveys: A reverse record check study. Qual. Quant. 38(5), 475–493 (2005)
14. Pavlou, P.A.: State of the information privacy literature: where are we now and where should we go? MIS Q 35(4), 977–988 (2011)
15. Ringle, C.M., et al.: Editor's comments: a critical look at the use of PLS-SEM in MIS quarterly. MIS Q. 36(1), iii–xiv (2012)
16. Smith, H.J. et al.: Information Privacy Research: An Interdisciplinary Review. MIS Q. 35(4), 989–1015 (2011)
17. Smith, H.J. et al.: Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Q. 20(2), 167–196 (1996)
18. Stone, E.F., et al.: A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. J. Appl. Psychol. 68(3), 459–468 (1983)