Influence of risks and privacy literacy on coping responses to privacy threats

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

The mass adoption of smartphones and their dedicated applications opens new opportunities for software vendors while presenting increased risks for software users. In order to understand the reaction of users facing privacy risks, this research presents an experiment measuring the influence of risks and privacy literacy on coping responses to privacy threats. Results show that risks literacy has the largest influence on the intention to install a potentially privacy-threatening application on a smartphone. These results could allow better targeting of actions developed to help users protect themselves against these new risks.

Keywords: *Privacy, smartphone, mobile application, protection motivation theory, partial least squares.*

Influence de la connaissance des risques et de la sensibilité à la sphère privée sur la réponse aux menaces concernant les données personnelles

Résumé

L'adoption massive des smartphones et des applications qui leurs sont dédiées ouvre de nouvelles opportunités pour les éditeurs de logiciels tout en présentant des risques accrus pour les possesseurs de ces appareils. Afin de comprendre la réponse des utilisateurs face aux dangers pesant sur leur sphère privée, cette recherche présente une expérience nous permettant de mesurer l'influence de la connaissance des risques et de la sensibilité aux atteintes à la sphère privée sur la réponse à ces dangers. Les résultats nous permettent de montrer que la connaissance des risques est l'élément le plus important dans la mesure de l'intention d'installer une application potentiellement dangereuse. Ces résultats vont permettre de mieux cibler les actions visant à aider les utilisateurs à se protéger face à ces nouveaux risques.

Mots-clés: *Vie privée, smartphone, application mobile, théorie de la motivation à se protéger, régression des moindres carrés partiels.*

1 Introduction

Smartphones are spreading around the world. They offer a convenient solution to make phone calls but they can also act as personal digital assistant, digital camera, media player or even as a GPS navigation unit. Furthermore, thanks to the hundreds of thousands of third-party applications, users can easily add new features to their devices. When installed on the same device that acts as a personal information repository, these applications can turn out to be a threat for 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 studies from online social networks are showing that users' intentions to use potentially privacy-threatening applications are influenced by the perceived benefits and risks resulting from their use. However, in the mobile applications context, users may not be aware of the privacy threats of an application that can access stored personal data without prompting the user to enter this information or specifically allowing access to it. Thus, we need to rethink how we assess the way people are interacting with these devices.

Third-party applications can be installed 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 software developers. The price of most applications is kept deliberately low, from free to two dollars on average. This encourages users to install multiple applications on their devices, based on their needs, interests or simply to entertain themselves. With such low prices, application developers are encouraged to use other ways to ensure sufficient revenues. Therefore, many applications incorporate, for example, third-party advertising. We can argue that people should nowadays be aware of these practices, since they are in widespread use on the Web.

However, there is a significant difference between using mobile applications and browsing the Web. We can assume that when people are browsing the Web, they are more conscious of the information they are providing to third parties. For example, users wanting to access a social network are required to provide personal information (such as a valid email address, gender, date of birth, etc.) and are generally informed, through terms and conditions, that this information can be stored by the owner of the website or resold to third parties. In the case of mobile applications, the mobile device already stores a lot of the user's personal information collected through the use of the smartphone. When installing new applications, the user is asked to grant access to specific smartphone functions such as network access, GPS location, stored personal information, etc. through a set of permissions. Thus, when installing an application, the user will grant, consciously or unconsciously, access to the personal information stored on the device. In this case, there is no further need for the user to manually provide specific information to the application. The application can access and collect the personal information it needs unnoticed.

Maddux and Rogers' (1983) protection motivation theory (PMT) postulates that attitude change is a function of the amount of protective motivation aroused by the cognitive appraisal processes. 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'. Previous research in the field shows that the intent to install a mobile application is in a significant proportion triggered by user's literacy in privacy risks and coping behaviours (De Santo and Gaspoz 2015). To understand a user’s decision-making when installing a mobile application, we need to further study how user privacy threats and coping behaviours literacy will influence the perceived benefits of using a specific application.

In order to understand the influence of the users’ literacy in privacy risks and coping behaviours on the intent to install a specific application, we set up an experiment in which we manipulated the users’ literacy in various aspects. This experiment showed that varying this literacy impacts the user’s intent to install a given application.

In the next section, we will review relevant research on protection motivation, privacy and coping behaviour. Section 3 presents the theoretical foundations of our study. The experimental design and the data collection methods are described in Section 4 and this is followed by a presentation of the statistical results in Section 5. We conclude by presenting the implications and limitations and make suggestions for future research in Section 6.

2 Literature review

Information privacy has become one of the core topics in information systems research (Pavlou 2011). Concerns over violation of user privacy are nowadays steadily growing. The widespread use of the Internet to communicate, share or exchange information, and advances in mobile computing have increased the interest in this topic. For our research, we use the Stone et al. (1983) definition of information privacy as ‘the ability (i.e. capacity) of the individual to control personally information about one’s self.’ We identified 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 privacy-threatening applications or technologies is presented in our leading journals and conferences. The applications studied include e-commerce (Malhotra, Kim, and Agarwal 2004), electronic health records (Angst and Agarwal 2009), direct marketing (Smith, Milberg and Burke 1996), radio frequency identification (Günther and Spiekermann 2005), home computing (Anderson and Agarwal 2010) and social networks (Bélanger and Crossler 2011). A recent review of information privacy research (Smith, Dinev and Xu 2011) 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 exploring this topic often rely on the theory of reasoned action, planned behaviour theory, general deterrence theory, rational choice theory, or theory of protection motivation. However, most of these studies hypothesized that users tend to underestimate the threat to their information security when they have to take a decision in these privacy risk contexts. However, the root cause of this failure has never been tested in order to correctly assess information security threats. A partial explanation of the fact that people can be concerned about their privacy but at the same time act incoherently by disclosing sensitive personal information, comes from Bennett (2011), 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’ (Smith, Dinev and Xu 2011). However, in the context of mobile applications, there is a gap between the valuation of information stored on the phone (for example in the 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) (Maddux & Rogers 1983) postulates that first information is received. Then this information initiates a cognitive mediating process. This process evaluates the response options towards the perceived situation. Finally, the result of these mediating processes, the threat appraisal and the coping appraisal, determines the reaction toward the situation. Previous research demonstrated the implicit influence of the PMT, privacy risk and coping behaviour literacies on users' intent to install a mobile application. In this research we want to go a step further and demonstrate the explicit influence of the privacy risk and coping behaviour literacies on PMT as well as the demographic antecedents of such literacies.

3 Development of hypotheses

In order to understand the process that results in the installation, or not, of a potentially privacy-threatening application on a smartphone, we will study the influences of the protection motivation process and the mobile application's characteristics on users' intentions. We seek to understand the effects of the protection motivation on the intention to use a particular smartphone application. Therefore, we postulate that the higher the protection behaviour, the lower the intent to install and use applications that could potentially put the user's privacy at risk. This also leads to the postulate that the intrinsic characteristics of a particular application will have some moderating effects on the intent to install and use it. Again, as the risk rises, the intention will decrease.

H1: Protection motivation will be negatively correlated to the intention to install and use an application

H2: An application's potential risks toward the user's privacy will be negatively correlated to the intention to install and use the application

As already stated, PMT describes how the sources of information and the effect of fear influence the development of protection behaviour. Information is used during two cognitive processes: threat appraisal and coping appraisal. In PMT, both processes are direct antecedents of protection behaviour. Environmental information includes verbal persuasion and observational learning. In the context of this study, we will only study observational learning. Part of the experiment's protocol will be to introduce the participants to the subject by telling them that our institution has the mandate to advise a tourist office in defining the specifications of a new mobile application for the promotion of a city. In order to determine the features and the risks that future users could accept from such an application, participants of the experiment have to take part in some sort of customer survey. Thus, given the experimental protocol used, we assume an equal effect on all participants. To operationalize observational learning, we differentiate coping behaviours 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. Moreover, we postulate that we can use both privacy literacy and coping behaviours literacy as antecedents to protection behaviour, as this behaviour is the direct result of the two appraisal processes.

H3: Risks literacy will be positively correlated to protection motivation

H4: Coping behaviours literacy will be negatively correlated to protection motivation

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. GIPC reflects the user's level of information privacy concerns in general. Based on this concern, we postulate that the attitude of the user toward risks and coping behaviour will be directly influenced by past experiences and concerns with privacy-threatening situations. Thus, a higher concern about information privacy should be reflected in a better literacy in both risks and coping behaviours.

H5: Global information privacy concern will be positively correlated to the privacy risks literacy

H6: Global information privacy concern will be positively correlated to the coping behaviours literacy

Finally, to totally cover intrapersonal sources of information, we need to measure the user's prior experience with smartphones (prior experience) as well as generic demographic aspects (personality variables). We choose to use prior experience and demographics as antecedents of GIPC, privacy risks and coping behaviours. In fact, the experience and demographic variables will determine how the user will behave in similar situations and thus will directly influence the user's literacy. Moreover, in this exploratory study we are mainly interested in the independent effects of demographic variables, more than on the global effect. To understand if there are specific demographics that influence the GIPC and the literacy in risks and coping behaviour, we investigate various factors such as gender, academic discipline, age and experience with smartphones.

H7: Demographics will be correlated to the risks literacy

H8: Demographics will be correlated to the coping behaviours literacy

H9: Demographics will be correlated to the coping behaviour literacy

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 and the protection motivation of the user, which in turn depend on the user literacy in privacy risks and coping behaviours.

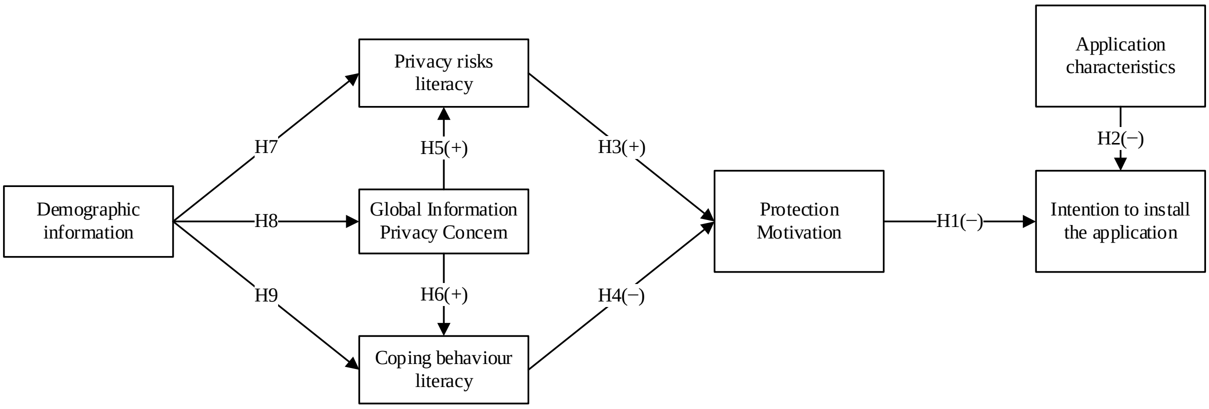
Application characteristics
Privacy risks literacy
H7
H5(+)
H3(+)
H2(−)
Demographic information
H8
Global Information Privacy Concern
Protection Motivation
H1(−)
Intention to install the application
H9
H6(+)
H4(−)
Coping behaviour literacy

Figure 1. Proposed research model

4 Research method

In order to explore our model (Figure 1), we conducted two experiments. In the first we manipulate the user's privacy risks literacy, while in the second we manipulate the user's coping behaviours literacy. Both experiments followed the same protocol.

4.1 Development of measurement items

In order to conduct our experiment, we had to devise two sets of permissions that would be generally considered to be 'low' privacy risks, and two others that would be generally perceived as 'high' privacy risks. Based on real-world application permissions, we developed and validated statements that would be recognised and understood by the participants. The development of this instrument was carried out in three stages. The first stage was the creation of sets of permissions based on real mobile applications. The second stage was to ask participants to rank these sets by their perceived acceptability. The last stage consisted of testing the instrument on a larger sample of respondents and analysing the results.

We created 11 sets of permissions based on genuine applications. In order to avoid any bias due to systematic reflexion, 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 11 sets based on their level of threat (low, middle, high) having reached agreement on the content.

To test this categorization, 15 people were invited to an experiment. They were told that we were developing a new mobile application for the municipal tourist office and, aware of some concerns regarding the extent of permissions requested by mobile applications, we needed their help in order to determine sets of acceptable permissions. Participants in the experiment had to read a document presenting the context and the facts of this mobile application and were given 15 minutes to sort 11 cards. The card sorting technique has been successfully used in past studies (Moore & Benbasat 1991).

Each card represented a given set of permissions, and they had to sort them into three piles based on their own perception of the acceptability of these sets. The piles were labelled 'totally acceptable', 'possibly acceptable' and 'not at all acceptable'. There was no description of the 'capabilities' of the application, in order to prevent participants from bias toward usefulness of features. The sample consisted of 8 females (53%) and 7 males (47%). In terms of smartphone ownership, 13% of the participants did not own one, 27% owned an Apple iPhone and the remaining 60% owned an Android smartphone. All of the subjects were university graduates.

From this first pre-test experiment, three sets of permissions were perceived as low threat and three others perceived as highly threatening. None of the cards perceived as low threat sought access to personal information. Of the three cards perceived as highly threatening, two requested permissions relative to services that would cost money – the only such cards in the whole set. The third card differentiated itself by clearly stating ‘access to confidential information’.

Based on these six cards, two sets emerged, each containing two cards, representing respectively the permissions universally perceived as low threat and those perceived to be highly threatening. With the new card sets, a second experiment was needed to validate these instruments. The result was an agreement of 83% on a sample of six people, four male and two female. The collection of this data was made by direct encounter, shuffling the sets for each subject. Consequently, we were satisfied that we had four sets of permission statements distinctly recognizable as involving both low and high risks to users’ privacy.

Based on these four sets, four corresponding mobile applications were imagined. These were based on the same global municipal tourist office application scenario but with four different sets of functionalities and corresponding permissions. The richer the application functionally, the more demanding were the application permissions required. All the permissions were directly related to one or more functions of the mobile application.

For each application scenario presented, we measured the behavioural 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, i.e. measuring the intent to not install, in order to check the validity of the survey (Johnston and Warkentin 2010).

Like Grover (2000), we ran a first pre-test with collaborators from the University, practitioners in the field, to validate the content, clarity and wording of the questionnaires. Eight people took the survey and each participant was then debriefed. Based on their comments and questions, we made some minor changes, in order to reach a higher level of global comprehension of the questionnaires. A second pre-test was conducted with 15 business undergraduate students.

4.2 Experimental protocol

The experiment was conducted with 122 undergraduate students in business and management information systems study courses from a medium-sized Business School. We made five different rounds with 20 to 50 students. The subjects were invited to participate in the selection process for a new mobile smartphone application for a regional tourist office. They were told that the office was intending to develop a new application. The overall objective of the application was presented as an opportunity to promote and develop the attractiveness of the region, through more than 500 activities referenced, geolocalized and regularly updated.

The first section of each questionnaire collected demographic information on the participant such as gender, age and study area, as well as information about their experience with smartphones. We then measured the global information privacy concern (GIPC) on a five-point Likert scale (Malhotra, Kim, and Agarwal 2004). Section 3 measured the subject's literacy in privacy risks (*Table 1. Privacy risk literacy measurement items*) and in coping behaviours (*Table 2. Coping behaviour literacy measurement items*).

Privacy risk	*Permissions*	*Application examples*
(Q1) It is likely that your personal data are relayed	use accounts on the device, read your contacts, full network access	Viber: Free Calls & Messages, Whatsapp Messenger
(Q2) ... that your movements are recorded and relayed	approximative location, full network access	Angry Birds, Facebook, Twitter
(Q3) ... that the publisher of the application accesses the photos and videos stored on your phone	modify/delete internal media storage contents, full network access	Badoo – Do more meetings, Instagram
(Q4) ... that an application could record a conversation and relay it	record audio, modify/delete internal media storage contents, full network access	Shazam, Soundhound
(Q5) ... that the content of your agenda is relayed	read calendar events plus confidential information, full network access	Google Agenda, Outlook.com
(Q6) ... that surcharged rate calls are made without your knowledge	directly call phone number,	Viber: Free Calls & Messages, Skype
(Q7) ...that phone usage patterns are collected for marketing purposes	read phone status and identity, full network access	Iron Man 3 – The game
(Q8) ... that potentially confidential information is extracted from your messages	read your text messages (SMS or MMS)	Viber: Free Calls & Messages, Skype
(Q9) ... that emails are sent without your knowledge.	add or modify calendar events and send emails to guests without owners' knowledge, full network access	Google Agenda, Outlook.com
(Q10) ... that the application retrieves all your contacts	use accounts on the device, read your contacts, full network access	Facebook Messenger, Whatsapp Messenger

Table 1. Privacy risk literacy measurement items

Coping behaviour	*Privacy risks*
(Q11) It is effective to block communication networks to prevent data transfers	*Q1–Q5, Q7, Q9, Q10*
(Q12) ... to paste a sticker on my camera so it does not capture photos / videos without my knowledge	—
(Q13) ... to control my bills in order to detect anomalies	*Q6*
(Q14) ... to encrypt my data to make it unreadable to malicious persons	*Q3,*
(Q15) ... to deny access to the data stored on my phone	*Q1–Q10*
(Q16) ... to control the transfer of data over Internet	*Q1–Q5, Q7, Q9, Q10*

Table 2. Coping behaviour literacy measurement items

After responding to these survey items, subjects were then asked to read the descriptions of two applications (one application presenting high privacy risks and the other presenting low privacy risks) and had to decide if they would install them on a mobile device (five-point Likert scale, from ‘strongly agree’ to ‘strongly disagree’). This was followed by a manipulation of the literacy in either privacy risks or coping behaviours. Subjects were randomly assigned to one of the manipulations.

4.2.1 Manipulation of the literacy in privacy risks

The subject was asked to read an article about a mobile application that posed a privacy threat. The application was presented as an inoffensive tool that could improve the camera capabilities of the user’s smartphone. However, the application was running a background process that was able to collect pictures unbeknown to the user. These pictures are then sent to a third-party server and could be used to build a three-dimensional representation of the user’s house, compromising the privacy and security of the user.

4.2.2 Manipulation of the literacy in coping behaviours

The subject was asked to read an article about a group of users who had organized themselves to cope with threats to their privacy. The article presented a mobile application that collected and stored a user’s personal data for marketing purposes without their consent. The article then describes different behaviours that users adopted to cope with this potential privacy threat of the mobile application.

4.2.3 Control groups

In these groups, the manipulation text was replaced by a simple and non-manipulating article telling the success story of a similar tourism application in a European country.

In order to test their understanding of the texts, each subject was asked 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 (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.

In the final section, we asked unrelated questions about their experiences with research in the Business School in order to create a cognitive distance from the current experiment. Finally, we devised a manipulation check for each group to measure their current literacy in risks or coping behaviours, depending on their assignment.

The four applications presented to each subject were randomized before and after the manipulation; the low- and high-risk application cards were shuffled between the manipulations. All experiments took place in a controlled environment and were conducted by the same co-author.

5 Data analysis

The market share of smartphones among mobile phone users has reached 42% in Switzerland; 70% among 20–29 year olds (Beyeler 2012). In view of this observation, we conducted our research on university students. Of all the survey respondents, only one did not actually own a smartphone, the rest having been previously exposed to various mobile applications market.

Once the surveys were completed, the first step was to eliminate surveys containing missing or incomplete answers (9.10%). Afterwards, thanks to the reverse record checks, we verified the accuracy of data that the respondents had provided (Öztaş Ayhan and Işiksal 2005), and 54.05% of the questionnaires were omitted after this check.

The final demographic data of the participants are shown in Table 3. The majority of them are male undergraduates between 18 and 25. Almost all the participants (92.15%) had at least six months' experience of a smartphone and in most cases they currently own an Android smartphone or an Apple iPhone. Respondents from two subject disciplines participated: information systems students and commerce students.

	Percentage (%)
1. Gender	
Male	66.67
Female	33.33
2. Age	
18−25	80.39
26−35	17.65
36−45	1.96
3. Education (completed)	
Matura	49.02
Higher education diploma	21.57
Bachelor	25.49
Other	3.92
4. Discipline	
Commerce	45.10
Information Systems	52.94
5. General experience with a smartphone	
No	1.96
<6 months	1.96
6–12 months	9.80
1–2 years	29.41
2–3 years	31.37
>3 years	41.18

6. Experience with actual smartphone	
No	1.96
<6 months	25.49
6–12 months	29.41
1–2 years	31.37
2–3 years	7.84
>3 years	3.92
7. Actual Smartphone	
No	1.96
Android Phone	62.75
iPhone	29.41
Windows Phone	1.96
Other	3.92

Table 3. Demographic data

Partial least squares (PLS) (Chin 1998), a variance-based structural equation modelling (SEM) analysis technique (Bollen and Lennox 1991), was used for assessing our model and hypotheses. 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 (Ringle, Sarstedt and Straub 2012). In order to analyse our data, the SmartPLS software was used. The measure of the intention to install an application was the latent variable of the PMT, itself predicted by the user's privacy risk literacy, the user's coping behaviour literacy and of the user's GIPC. Furthermore, the need of formative constructs to describe and define some of our own constructs (Petter, Straub, and Rai 2007) confirmed our choice of PLS–SEM modelling. The multidimensional second-order constructs favoured the use of the SEM technique to test our model (MacKenzie, Podsakoff and Jarvis 2005).

Users' risk privacy literacy, users' coping behaviour 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.

Group	*Items*	*Mean*	*S.D.*	*Weight*	*Group Mean*	*Grou p S.D.*
Users' risk privacy literacy from 1 (very unlikely) to 5 (very likely)	*It is likely* that your personal data are relayed	3.94	1.10	−1.30	3.05	1.58
	... that your movements are recorded and relayed	3.76	1.62	0.91		
	... that the publisher of the application accesses the photos and videos stored on your phone	2.86	1.72	−1.15		
	... that an application could record a conversation and relay it	2.59	1.93	1.67		
	... that the content of your agenda is relayed	2.75	1.95	0.54		
	... that surcharged rate calls are made without your knowledge	2.20	1.76	0.59		
	...that phone usage patterns are collected for marketing purposes	4.24	0.86	0.54		
	... that potentially confidential information is extracted from your messages	2.53	1.37	−1.40		
	... that emails are sent without your knowledge.	2.35	1.79	-0.61		
	... that the application retrieves all your contacts	3.33	1.67	0.73		
Users' coping behaviour literacy from 1 (very ineffective) to 5 (very effective).	*It is effective* to block communication networks to prevent data transfers	3.96	1.28	0.86	3.55	1.31
	... to paste a sticker on my camera so it does not capture photos / videos without my knowledge	3.61	1.88	−0.05		
	... to control my bills in order to detect anomalies	4.25	0.71	−0.20		
	... to encrypt my data to make it unreadable to malicious persons	3.22	1.21	0.33		
	... to deny access to the data stored on my phone	3.41	1.29	−0.26		
	... to control the transfer of data over Internet	2.86	1.48	−0.16		

Table 4. Users' risk privacy and coping behaviour literacy

5.1 Effects of the manipulation

Before any manipulation, we predicted that the likelihood of a subject intending to install an application was 11.5%, purely based on the PMT and the applications' characteristics. The PMT itself was the most influential construct, exerting an influence of 32.2% versus the 10.6% of the applications' characteristics alone. It was also interesting to note that the PMT is determined at 98.8% by the users' privacy risk and coping literacy, with respectively 54.3% and 61.9% of influence. Clearly, the users' privacy risk literacy was more effective in triggering awareness than coping behaviour literacy, which had the opposite effect (sign opposition). Global information privacy concern could be predicted at 13.5% purely on the user's demographic information. The demographic aspects and the GIPC of a user were predictive at 56.7% of the user's privacy risk literacy and at 24.5% of the user's coping behaviour literacy.

T-statistics were used to test the proposed hypotheses for the standardized path coefficients, by specifying the same number of cases as 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.

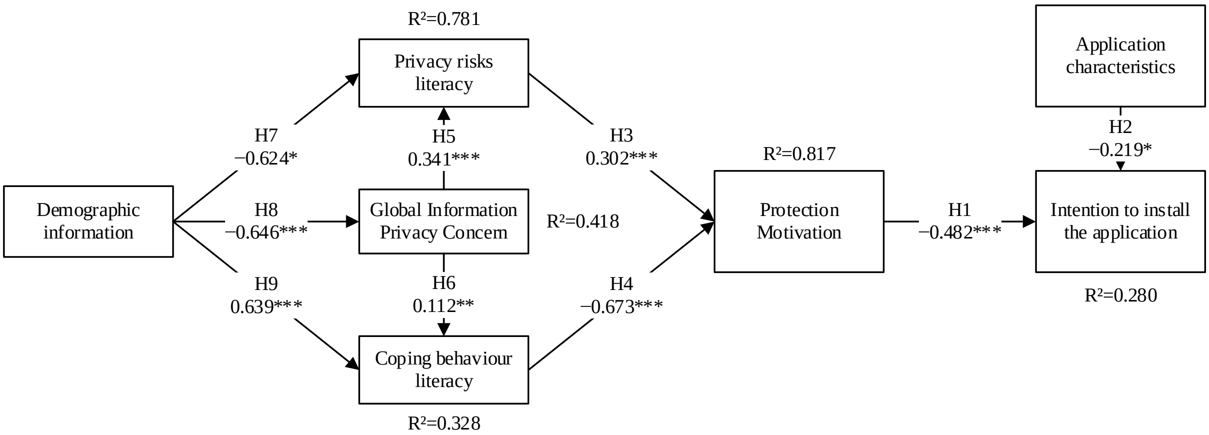

Figure 2. Model results after manipulation

After the users' privacy risk literacy manipulation, the intention to install an application was predicted at 28.0% by the PMT and the applications' characteristics. In other words, these two elements were 16.5% more predictive than before the manipulation. In that assertion, the PMT was the most influencing construct with an influence of 48.2% against 21.9% from the applications' characteristics. It was interesting to note that the values of these last two elements almost doubled with the manipulation. The PMT was then predicted at 81.7% by the users' privacy risk literacy and the users' coping behaviour literacy. That represented a decrease of 17.3%, which suggests that something new influences the calculation of the PMT. It could certainly be the behavioural experience, but this point is not part of the actual study and could be the subject of further research. We also note that if before the users' privacy risk literacy could have been predicted at 56.7% by the demographic information and the GIPC, it was then predicted at 78.1%. The influence of the GIPC decreased from 66.8% to 34.1%, which seemed reasonable because we didn't measured again the GIPC, so the GIPC was less influencing than before because the users' privacy risks literacy changed.

To measure the users' risk privacy and coping behaviour literacy we based our indicators on respectively 10 and 6 Likert scales variables. The weight of each item demonstrated the item's contribution to the construct. We retained non-significant indicators to preserve content validity (Bollen and Lennox 1991).

	Mean	*S.D.*	*AVE*	*CR*	*GIPC*	*Intention to install the application*
GIPC	4.78	2.82	0.631	0.836	0.794	
Intention to install the application (low/high privacy risk threatening)	2.14/1.88	1.95/1.45	0.953	0.881	−0.429	0.976

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

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) (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 (Table 5), and the cross-loadings show each item loading higher on its own factor than on others (Table 6).

	GIPC	*Intention to install an application*
GIPC08	0.845	−0.377
GIPC09	0.717	−0.560
GIPC10	0.815	−0.178
INTBEF	−0.387	0.986
PLABEF	0.474	−0.956
PREBEF	−0.387	0.986

Table 6. Loadings and cross-loadings for reflective measures

6 Discussion

As seen in the previous section, the results largely support our hypotheses. First, we found that the protection motivation has more influence on the intention to install an application than the application’s own characteristics (H1 and H2). This is not surprising, as it also explains why so many privacy-threatening applications are installed on users’ devices. Indeed, if people have a low protection motivation and given that its influence is more than two times greater than the application’s own characteristics, there is a high risk of seeing potentially dangerous applications on users’ devices. This first result is also a confirmation of our general approach, consisting of studying the antecedents of the intention to install an application in order to understand how to better protect the privacy of smartphone users.

The second set of hypotheses (H3 and H4), which related to the influence of the privacy risks and coping behaviour literacy, is also validated by the data collected. One very interesting fact is that the coping behaviour literacy has twice the influence of the privacy risks literacy on the protection motivation. This brings interesting elements to light since we now have evidence that efforts should be put into the development of personal abilities to cope with privacy-threatening applications more than on a better risk assessment. We can use these results to plan and execute better campaigns, knowing that the goal should be to increase the coping behaviour literacy in the population, rather than to increase its privacy risks literacy.

The next question that we explored in this study, is the influence of the user's privacy concern on its literacy (H5 and H6). As we would have expected, we have a significant influence of the privacy concerns on the privacy risks literacy. Both represent cognitive processes, and the more the person is concerned by their own privacy, the more they will process privacy risks information, enhancing their own literacy on the topic. However, we surprisingly found that the privacy concern has very little influence on the coping behaviour literacy. We are in dealing with both a cognitive process and a practical ability. As we would expect, the development of abilities is a much slower process because personal experience plays a far greater role than in the acquisition of intellectual concepts. However, when acquired, and certainly due to the role of the personal experience, these abilities can be used almost instinctively to moderate privacy risks. The second explanation is probably related to the privacy calculus (Dinev and Hart 2006), which presents information disclosure as a trade-off between benefits and risks. Studies on this topic explore the subject while measuring the individual's willingness to provide information in exchange for various services (e.g. Bart et al. 2005; Schoenbachler and Gordon 2002). They found that the actual behaviour of disclosing information is only tenuously correlated to the user's privacy concern. Given that we measured that coping behaviour literacy has more than two times the influence of privacy risks literacy on the protection motivation, this follows from the results of studies on privacy calculus. Indeed, if the user's privacy concern has little influence on the disclosure of personal information, as found by privacy calculus researches, it should be expected that it will have little influence on the most influencing construct, in our case, the coping behaviour literacy.

Finally, as we had expected, we found that demographics have some sort of influence on the antecedents of the protection motivation (H7 to H9). However, we cannot draw conclusions on demographic aspects leading to more or less exposure to risks from our results. The only conclusion that can be drawn is that in order to enhance the user's protection, we need to design highly customizable solutions that can adapt to the user's preferences, literacy and concerns.

6.1 Limitations

As this is an exploratory study, it has some limitations. The first is the sample size coupled with the poor data quality of the surveys completed. This resulted in a relatively small sample, which was sufficient to achieve our PLS analysis, but was not sufficient to study the effects of the manipulation of the coping behaviours. In order to extend the scope of the research, we will definitely need a larger sample.

The second limitation concerns the environmental information source. We did not try to manipulate or evaluate the effects of verbal persuasion. However, given the artificial functionalities of the fictitious application, we might expect that the intention to install the application might differ if the application was presented by a trusted friend. Thus in a further study, we should try to manipulate verbal persuasion in order to measure its effects.

6.2 Future works

There are many opportunities to further explore this subject. It seems that very often the awareness context (Glaser and Strauss 1964) 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 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 against application developers. This should then help policymakers in designing public awareness campaigns on mobile applications' privacy risks.

7 Conclusion

Our study provides 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 regardless of the characteristics of the application.

These results are very interesting as they validate our assumption that, in the context of mobile applications, the privacy as a commodity view (Bennett 2011) could no longer hold because the users are no longer aware of the magnitude of the private information they share with application writers. 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 leaks of private information. Moreover, this could also assist OS writers in developing some sort of risk training in their software in order to increase the privacy risks literacy of their users' basis.

8 References

Anderson, Catherine L. and Ritu Agarwal. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions." *MIS Quarterly* 34 (3) (September): 613–643.

Angst, Corey M. and Ritu Agarwal. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly* 33 (2) (June): 339–370.

Bart, Yakov, Venkatesh Shankar, Fareena Sultan and Glen L. Urban. 2005. "Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study." *Journal of Marketing* 69 (4) (October): 133–152. doi:10.1509/jmkg.2005.69.4.133.

Bélanger, France and Robert E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4) (December 1): 1017–1042. http://dl.acm.org/citation.cfm?id=2208940.2208951.

Bennett, CJ. 2011. "In Defense of Privacy: The Concept and the Regime." *Surveillance & Society* 8 (4): 485–496. http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewArticle/privacy_defence.

Beyeler, Ralf. 2012. "2,9 Millions de Suisses Ont Un Smartphone."

Bollen, Kenneth and Richard Lennox. 1991. “Conventional Wisdom on Measurement: A Structural Equation Perspective.” *Psychological Bulletin* 110 (2): 305–314. doi:10.1037/0033-2909.110.2.305. http://doi.apa.org/getdoi.cfm?doi=10.1037/0033-2909.110.2.305.

Chin, Wynne W. 1998. “Commentary: Issues and Opinion on Structural Equation Modeling.” *Management Information Systems Quarterly* 22 (1) (November): vii–xvi.

De Santo, Alessio and Cédric Gaspoz. 2015. “Influence of Users ‘ Privacy Risks Literacy on the Intention to Install a Mobile Application.” *New Contributions in Information Systems and Technologies* 2: 358. http://www.springer.com/engineering/computational+intelligence+and+complexity/book/978-3-319-16527-1.

Dinev, Tamara and Paul Hart. 2006. “An Extended Privacy Calculus Model for E-Commerce Transactions.” *Information Systems Research* 17 (1) (March): 61–80. doi:10.1287/isre.1060.0080.

Glaser, Barney G. and Anselm L. Strauss. 1964. “Awareness Contexts and Social Interaction.” *American Sociological Review* 29 (5) (December 31): 669–679. http://www.jstor.org/stable/info/2091417.

Grover, Varun. 2000. “A Tutorial on Survey Research: From Constructs to Theory.”

Günther, Oliver and Sarah Spiekermann. 2005. “RFID and the Perception of Control.” *Communications of the ACM* 48 (9) (September): 73–76. doi:10.1145/1081992.1082023.

Johnston, Allen C. and Merrill Warkentin. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study.” *MIS Quarterly* 34 (3) (September): 549–566.

MacKenzie, Scott B, Philip M Podsakoff and Cheryl Burke Jarvis. 2005. “The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions.” *The Journal of Applied Psychology* 90 (4) (July): 710–730. doi:10.1037/0021-9010.90.4.710. http://www.ncbi.nlm.nih.gov/pubmed/16060788.

Maddux, James E and Ronald W. Rogers. 1983. “Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change.” *Journal of Experimental Social Psychology* 19 (5) (September): 469–479. doi:10.1016/0022-1031(83)90023-9. http://dx.doi.org/10.1016/0022-1031(83)90023-9.

Malhotra, Naresh K., Sung S. Kim and James Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” *Information Systems Research* 15 (4) (December): 336–355. doi:10.1287/isre.1040.0032. http://isr.journal.informs.org/cgi/doi/10.1287/isre.1040.0032.

Öztaş Ayhan, H. and Semih Işiksal. 2005. “Memory Recall Errors in Retrospective Surveys: A Reverse Record Check Study.” *Quality & Quantity* 38 (5) (January): 475–493. doi:10.1007/s11135-005-2643-7. http://www.springerlink.com/index/10.1007/s11135-005-2643-7.

Pavlou, Paul A. 2011. “State of the Information Privacy Literature: Where Are We Now and Where Should We Go?” *MIS Quarterly* 35 (4) (December 1): 977–988. http://dl.acm.org/citation.cfm?id=2208940.2208949.

Petter, Stacie, Detmar W. Straub and Arun Rai. 2007. “Specifying Formative Constructs in Information Systems Research.” *MIS Quarterly* 31 (4): 623–656.

Ringle, Christian M., Marko Sarstedt and Detmar W. Straub. 2012. “Editor’s Comments: A Critical Look at the Use of PLS-SEM in MIS Quarterly.” *MIS Quarterly* 36 (1) (March 1): iii–xiv. http://dl.acm.org/citation.cfm?id=2208955.2208956.

Schoenbachler, Denise D. and Geoffrey L. Gordon. 2002. “Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing.” *Journal of Interactive Marketing* 16 (3) (January): 2–16. doi:10.1002/dir.10033.

Smith, H. Jeff, Tamara Dinev and Heng Xu. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35 (4): 989–1015. http://misq.org/information-privacy-research-an-interdisciplinary-review.html.

Smith, H. Jeff, Sandra J. Milberg and Sandra J. Burke. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices.” *MIS Quarterly* 20 (2) (November 9): 167–196. http://www.jstor.org.ezproxy.library.ubc.ca/stable/info/249477.

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner and Stephen McClure. 1983. “A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations.” *Journal of Applied Psychology* 68 (3): 459–468. doi:10.1037/0021-9010.68.3.459. http://content.apa.org/journals/apl/68/3/459.