Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

Between privacy and security: the factors that drive intentions to use cyber-security applications

Hadas Chassidim , Christos Perentis , Eran Toch & Bruno Lepri

To cite this article: Hadas Chassidim , Christos Perentis , Eran Toch & Bruno Lepri (2020): Between privacy and security: the factors that drive intentions to use cyber-security applications, Behaviour & Information Technology, DOI: 10.1080/0144929X.2020.1781259

To link to this article: https://doi.org/10.1080/0144929X.2020.1781259

Published online: 29 Jun 2020.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2020.1781259

Between privacy and security: the factors that drive intentions to use cyber-security applications

Hadas Chassidim[a], Christos Perentis[b], Eran Toch[c] and Bruno Lepri[b]

[a]Department of Software Engineering, Shamoon College of Engineering, Beer-Sheva, Israel; [b]Mobile & Social Computing Lab, Fondazione Bruno Kessler, Trento, Italy; [c]Department of Industrial Engineering, Tel-Aviv University, Tel-Aviv, Israel

ABSTRACT

Installing security applications is a common way to protect against malicious apps, phishing emails, and other threats in mobile operating systems. While these applications can provide essential security protections, they also tend to access large amounts of people's sensitive information. Therefore, individuals need to evaluate the trade-off between the security features and the privacy invasion when deciding on which protection mechanisms to use. In this paper, we examine factors affecting the willingness to install mobile security applications by taking into account the invasion levels and security features of cyber-security applications. To this end, we propose a visual language that depicts the coverage of different security features as well as privacy intrusiveness levels. Our user study (n=300) shows that users assessing security applications find their trade-off balance in highly secure apps with a medium level of privacy invasion. The results indicate that a low privacy invasion might signal that the security application provides less security. We discuss these findings in the context of understanding the trade-off between privacy and security.

ARTICLE HISTORY
Received 14 January 2020
Accepted 5 June 2020

KEYWORDS
Privacy; cyber-security; mobile security applications; visualisation; user study

1. Introduction

Smart mobile devices are quickly becoming essential to daily life, trusted by users to hold everything from contacts and appointments to banking and retail transactions. At the same time, our dependence on these devices brings new security challenges, such as device hijack (Lala and Panda 2001) and Wifi-based man-in-the-middle attacks (Suo et al. 2013). Smartphones are also vulnerable to malicious software known as *malware* that spread through various means, by attaching themselves to useful mobile applications (Hern 2015), transmitted via SMS/MMS or via web-browsing (Suo et al. 2013), and through data collection tools hidden within smartphone apps (McCarthy 2009). As a result, people have growing concerns about the security and privacy of their mobile devices, including identity fraud and leakage of personal information (Clarke et al. 2016).

Users' awareness and ability to protect themselves in mobile devices is still questionable (Clarke et al. 2016; Koyuncu and Pusatli 2019). One of the common ways for self-protection is by installing security applications (or apps, as we henceforth will call them), which requires an interaction with the user, including the acceptance of the application's conditions, and the application's access to sensitive information stored on the phone (Seneviratne 2018). Security apps often trace the identity of the users and access personally identifiable information that can result in privacy risks (Toch et al. 2018). In particular, many security apps ask for extensive access to activate their features, thus increasing their potential vulnerability (Felt et al. 2011). For example, microphone, camera, and location permissions are usually requested to activate anti-theft features (e.g. tracking the lost device), while permissions related to call and SMS functionalities are asked to enable anti-phishing features (Seneviratne 2018).

Privacy risks raise a severe challenge to both users and developers of security systems: to find a balance between the security risks and privacy concerns. In many cases, privacy concerns can lead users to refrain from the security systems and to use alternative channels (Dincelli and Goel 2017). In the case of general mobile apps, people make decisions about installing an app by weighting the signals about the benefits of installing the app versus privacy concerns (Felt et al. 2011; Kelley et al. 2012; Di Stefano et al. 2018; Henke, Joeckel, and Dogruel 2018; Kummer and Schulte 2019). A recent study demonstrates that a privacy calculus is adopted by mobile app users (Wottrich, van Reijmersdal, and Smit 2018). In particular, this study has found that the value of a mobile app (i.e. benefit) trumps the costs (i.e.intrusiveness, privacy concerns). However, security apps are inherently

CONTACT Hadas Chassidim hadasch@ac.sce.ac.il, hadasc@post.tau.ac.il

different than regular ones: they collect more information than regular apps, and by collecting more information, they have better potential of protecting the user against outside threats. For instance, if a security app needs to protect against phishing text messages, it needs to access the communication information stored on the device. Therefore, there is a gap in understanding how users make decisions about cyber-security apps, which may pose an utterly new trade-off to users.

In this paper, we aim at identifying the key factors that affect mobile users' intentions to install security applications. For this purpose, we propose an innovative approach that synthesises two well-known models, the Theory of Planned Behaviour (TPB) (Ajzen 1991, 2002; George 2004) and the Mobile Privacy-Security Knowledge Gap (Crossler and Bélanger 2017). The two frameworks are based on a wide set of well-established constructs of attitudes, motivation and perceptions (see Table 1). However, these constructs didn't consider an objective dimension of the actual privacy or security levels.

Our proposed model contributes to this by adding objective factors of security and privacy levels as control variables (i.e. Intervention). We have developed visualisation scores for mobile application security levels and extended a privacy score for mobile apps (Kelley et al. 2012). We have investigated the effects of these scores on users' willingness to install cyber-security apps in a user study (n =300). Our results show that the intention to install increases as more security features are offered, while users are willing to compromise on medium levels of privacy intrusiveness. These results hold even when controlling for security and privacy perceptions of the user, personal experience regarding data breaches, attitude towards sharing data with apps, and social norms. Our findings may support practical implications both on how users are provided with information regarding privacy invasion and security levels of cyber-security applications as well as in terms of regulations (see Section 6).

The remainder of the paper is organised as follows: Section 2 presents the background of modelling security and privacy behaviours, while Section 3 states our model and research hypotheses. Furthermore, in Section 3, we extensively describe the computation and visualisation of security and privacy intrusiveness levels for cyber-security apps of the research model. In Section 4, we present our methodology, while Section 5 describes the obtained results. Finally, we discuss the findings and draw some conclusions in Section 6.

2. Background

The distinction between privacy and security has been investigated in several recent papers (Bansal 2017; Dincelli and Goel 2017; Crossler and Bélanger 2017; Dincelli, Goel, and Warkentin 2017). While both privacy and security describe risks to information, their focus is different. Information security focuses on ensuring the protection of data from outside attackers, hackers, and entities that were not part of the communication (Bansal 2017). In contrast, information privacy concentrates on

Table 1. Description of the dependent (DV) and independent (IV) variables and their source.

Construct	Dimension	Description	Items
Intention (George 2004)	Intention	The willingness to install a security app	I1 (DV)
Attitudes (George 2004)	Security Attitudes	Feeling safe sharing data with an app	SA1(Malhotra, Kim, and Agarwal 2004; Acquisti and Grossklags 2003)
	Privacy Attitudes	Importance of privacy preservation	PA1, PA3, PA4 (Malhotra, Kim, and Agarwal 2004) PA2 (Foltz, Newkirk, and Schwager 2016)
Motivation (Crossler and Bélanger 2017)	Self Experience	Indirect/direct personal experience of improper privacy intrusiveness	SE1, SE2 (Malhotra, Kim, and Agarwal 2004)
	Norms	What my close friends/family think about security apps	N1-N4 (George 2004)
Perceptions (George 2004)	Perceived Security	The extent an application can protect me against hackers/viruses (per app)	PS1, PS2 (IV/DV) (Malhotra, Kim, and Agarwal 2004)
	Perceived Privacy	The extent an app collects information about me (per app)	PP1 (IV/DV) (Malhotra, Kim, and Agarwal 2004)
Perceived Behavioural Control (George 2004)	Beliefs (similar to Self-Efficacy)	Ability of managing apps, familiarity with permission requests/countermeasures to self-protect	Be1 (Ajzen 1991, 2002, Fishbein and Ajzen 1977) Be2, Be3 (Foltz, Newkirk, and Schwager 2016) Be4, Be5, Be6 (Sawaya et al. 2017)
	Knowledge	Answering security/privacy questions	K1, K2, K3 (Sawaya et al. 2017) K4 (Malhotra, Kim, and Agarwal 2004) K5, K6 (self developed based on common knowledge)
Intervention (Section 4.1)	Security	Level based on calculated security score (per app)	Security & Privacy Invasion Level (see Sections 3.2 and 3.3 for computations and see Figure 1 for design)
	Privacy Invasion	Level based on calculated privacy invasion score (per app)	

Notes: All the variables used in this study are presented. First column describes the construct each variable belongs to (e.g. Attitudes, Perceptions, etc.), the second column lists the dimensions of the constructs, and the third column holds a description of each construct's dimension. Finally, Items column contains the exact variables abbreviation for the corresponding dimension. Each variable's abbreviation (except those of the Intervention construct, which are calculated in Section 3 for both Security and Privacy Invasion dimensions) corresponds to a question mapped in Appendix Table A1.

Figure 1. The developed visualisations regarding Privacy Invasion and Security features for mobile security applications. The upper part of the mock-ups holds the Privacy labelling visualisation, while the lower part of the mock-ups the Security labelling. The different sub-figures show an example of the designed experiment (Section 4) for a mobile security application: (a) Actual Privacy invasion level, and (b) High Privacy invasion level, while both screens hold the same Security level. (a) Actual Privacy Invasion and (b) High Privacy Invasion.

adhering to information flow norms in specific contexts by parties that can be insiders to the communication (Nissenbaum 2009). While the two concepts are intertwined, most existing works refer either to privacy or to security concerns, thus producing two separate research streams (Acquisti and Grossklags 2003; Jensen, Potts, and Jensen 2005; Kelley, Cranor, and Sadeh 2013; Chen et al. 2015; Crossler and Bélanger 2017; Kokolakis 2017; Chong et al. 2018; Xie, Fowler-Dawson, and Tvauri 2019).

Even though privacy and security concerns are known to strongly impact user behaviour, the distinction between these two constructs is highly contested (Bansal 2017). Some papers suggest that privacy and security are perceived as the same construct by users (Casaló, Flavián, and Guinalíu 2007; McCole, Ramsey, and Williams 2010), while others suggest that these are two distinct constructs (Dincelli and Goel 2017; Bansal 2017). For example, Dincelli and Goel (2017) found that security and privacy behaviours were inherently distinct and were differently affected by cultural characteristics and by different sets of factors. In the context of social media monitoring and surveillance, people's willingness to share private information was affected by sociodemographic variables and the security goal (Aldehoff, Dankenbring, and Reuter 2019). Crossler and Bélanger (2017) aimed to tie the privacy and security research streams, pointing to the role of knowledge and skills in users' behaviours. In particular, they point to the security-privacy knowledge gap, which illustrates how people understand the impacts of sharing information when they deal with privacy or security-related decisions. Mobile security apps provide a test case to assess these theories and to understand the dynamics between protection from outside threats and the protectors themselves.

Characterising the security-privacy relationship raises several theoretical and methodological challenges. Contemporary theories of privacy emphasise the importance of context in people's privacy attitudes and behaviours (Nissenbaum 2009). These attitudes and behaviours are not static but rely on the context of the information flow, which includes the actors that receive the information, the type of data, and the transmission principles. Extending this contextual approach to the privacy-security relationship requires us to understand how the context, or at least the most critical aspects of the context, impact the relationship. As Crossler and Bélanger (2017) notice, differences between privacy and security aspects can be rooted either in the knowledge gap or actual preferences of users. Users are often overconfident about their knowledge and skills over security (Kokolakis 2017), while their real understanding of security is somewhat limited (Jensen, Potts, and Jensen 2005).

Meaningfully analysing those relations requires some ways to control this gap.

From the methodological point of view, the existing literature is based almost exclusively on surveys that asked for people's attitudes according to predefined questionnaires (Casaló, Flavián, and Guinalíu 2007; Bansal 2017; Dincelli and Goel 2017; Crossler and Bélanger 2017). Given this methodology, it is challenging to understand how the context and intrusiveness level impact this trade-off. Another gap relates to the domain of the studied apps. Several works have looked at either privacy or security in mobile environments (Jain and Shanbhag 2012; Suo et al. 2013; Clarke et al. 2016; Perentis et al. 2017; Yao, Chuang, and Hsu 2018; Chong et al. 2018; Wolf, Kuber, and Aviv 2018), thus studying security apps provides a unique methodology to close the gap in understanding the trade-off between privacy and security in people's decision-making processes.

3. Research model

3.1. Decision-making model

Our research framework aims at investigating the role played by privacy and security perceptions as well as by beliefs and knowledge in evaluating the trade-offs between privacy and security in mobile security apps. The focus on this specific type of apps provides us with two advantages. First, these applications introduce a real trade-off between privacy and security as they access large amounts of personal data (Toch et al. 2018). Therefore, they can serve as a realistic and concrete focus of attention to gather users' intentions. Second, the fact that security applications collect various amounts of data can help us analyse the impact of context and intrusiveness level on people's intentions.

Two existing models inspire our work: (i) the Mobile Privacy-Security Knowledge Gap Model (Crossler and Bélanger 2017), and (ii) the Theory of Planned Behaviour (TPB) (Ajzen 1991, 2002; George 2004). Our approach integrates these two models, while also adding additional control dimensions, including the beliefs and knowledge about the fact that an individual may have the opportunities and resources needed to engage in a given behaviour (George 2004). This gap was defined by Crossler and Bélanger (2017) as the gap between knowing how to do something and believing to know the important things to do for enabling a specific behaviour.

In our approach, users' intentions to install cybersecurity apps are informed by their privacy and security perceptions regarding the characteristics of a particular app. We test the effect of these perceptions while controlling for general privacy and security attitudes, security and privacy experience, knowledge, beliefs, and the subjective norms about engaging in the behaviour. To account for the knowledge gap and the challenges users face in understanding what a security application does, we are proposing a way to visualise the privacy intrusiveness levels and the protection levels of the security apps.

3.2. Modelling security capabilities

Mobile security apps have different levels of security and different levels of data permissions they ask to access to provide their service (Yao, Chuang, and Hsu 2018). We aim to model the variability of the cyber-security apps under investigation, taking into account their security and privacy intrusiveness levels. Security score calculation is based on the quantity and the importance of the features, using data obtained from the av-comparatives.org report (AV-Comparatives, Mobile Security Review 2015), which details the availability of products that include security features such as Safe Browsing, Remote Lock, On-install Scan, etc. To build the security score we first estimate the important factor for each of the security features. Similarly to Yao, Chuang, and Hsu (2018), we calculate the importance of feature *ft*, which belongs to Security Category *cat*, by counting the number of times found present among the security apps. Specifically, for each feature *ft* of a Security Category *cat* and for each security application *app*, we count the presence (1) or absence (0) of a feature, then we divide by the total number of security apps *app*, as shown in the following equation:

$$Importance_{ft,cat} = \frac{\sum_{i=1}^{app} (Feature\ Presence_{ft,cat})_i}{\#\text{Security Apps}}, \quad (1)$$

where $Feature\ Presence = (1{:}Present/0{:}Non-Present)$

Next, we estimate the security score for each security category of each security application, while incorporating the contribution of each feature. Thus, we compute the weighted average of a feature presence by using its *Importance* as defined in Equation (1). Finally, this quantity is divided by the sum of the *Importance* scores in this category (e.g. Anti-Malware, Anti-Spam, Anti-Theft, etc.) as shown in the following equation:

$$Security\ Category\ Score_{app,cat} = \frac{\sum_{i=1}^{ft} (Feature\ Presence_{i,cat} \times Importance_{i,cat})}{\sum_{j=1}^{ft} Importance_{j,cat}} \quad (2)$$

After calculating a score for each Security Category, we simply calculate the overall Security Score per application by averaging the scores over the total number

of security categories, as depicted in the following equation:

$$Security\ Score_{app} = \frac{\sum_{i=1}^{cat} (Security\ Category\ Score_{app,cat})_i}{\#\text{Security Categories}} \quad (3)$$

3.3. Modelling privacy invasion

We model privacy invasion as the amount and the kind of access an application requests. Often, granting access to sensitive or other personal information (e.g. high-granularity location data, contact list, etc.) can serve a given feature of a mobile application or advertising purposes. To model the actual setting of the mobile security apps' data permissions, we employ real data from Google Play (Google Play Store 2019). We measure for each category the requested permissions in the following 15 data type categories: (1) In-app Purchases, (2) Device & App History, (3) Network Settings, (4) Identity, (5) Contacts, (6) Location, (7) SMS, (8) Calendar, (9) Phone ID, (10) Photos/Media/Files, (11) Storage, (12) Camera, (13) Microphone, (14) WiFi connection info, and (15) Device ID & Call info.

It is worth noting that for most of the data types more than one permission exists. Moreover, some permissions can only be viewed (e.g.Location), while others can be only edited (e.g. Photos/Media/Files). Specifically, we assign to each permission one of the following weights depending on its permission access type: '0' when the permission is not collected; '1' when the permission is collected and it is of type *read*; '2' when the permission is collected and it is of type *edit*. Next, to simplify the presented information we resort to the 15 permission categories assigning a unique value by applying the following rule: Each permission category takes a final permission access value based on the maximum permission value observed in the relevant category. If at least one permission out of the whole category (for example, Contacts) is *edit*, then the whole group (i.e. Contacts) is characterised by *edit*.

We proceed now to compute the privacy invasion scores taking into account the number of edits, views and absence of collecting permission access types. Note that out of the 15 categories, 3 of them are exactly the same for all the apps (i.e. Storage, WiFi and Device ID), therefore we exclude them from the computation. Moreover, seven categories can take the value of *edit*, while the maximum intrusiveness for five categories can be *view* or *not collecting*. The final Privacy Invasion Score per application is given by the following equation:

$$\text{Privacy Invasion Score} = w_1 \times Edits + w_2 \times Views \quad (4)$$

3.3.1. Visualisation

We developed a simple visualisation for the security capabilities and privacy invasion of apps as depicted in Figure 1. The visualisation presents the permissions the security application requires to access (i.e. collect, read, edit). Our visualisation is inspired by the work of Kelley, Cranor, and Sadeh (2013), resorting to the same three icons for the permissions, consisting of *not collecting* , *can view* , and *can edit* , and we derive the type from its category based on the privacy score computed as described in Section 3.3. The aforementioned Privacy labelling in the designed mock-up can be seen in the upper part of Figure 1(a,b).

In a different context, we visualise the security features using shape and colour to express the notion of *absence of a feature* , *basic* , *advanced* , and *high* . This security labelling is shown in the lower part of the designed mock-up, depicted in both sub-figures of Figure 1. We map the above-mentioned categories by using the quantile range of the security score. The design of the security labels is based on the data visualisation theory showing that encodings with icon shapes are more effective and may improve the understanding of the risk involved (Nowell 1997). We also use colour-in-context theory that exploits the strong link between colour and psychological reasoning to enforce the communication with the users (Elliot and Maier 2012).

3.4. Research hypotheses

Based on the security and privacy visualisations that subjects receive in our study, we formulate research hypotheses regarding: (i) privacy and security perceptions effect on the willingness to install cyber-security mechanisms and (ii) apps' privacy invasion and security level effect on user perceptions. In all our hypotheses we control for well-known behavioural constructs such as security and privacy attitudes, user motivation (i.e. self-experience of breaches and social norms in user environment) and user knowledge and beliefs. Besides the aforementioned constructs, note that in H1 we also control for the actual security and privacy invasion level of the apps, while in H2 for the privacy invasion and security perceptions, respectively.

- *H1: Security and Privacy Invasion Perceptions*
  - H1.1: Higher perceived security for a specific app has a positive influence on the intention to install this application;
  - H1.2: Higher perceived privacy invasion for a specific app has a negative influence on the intention to install this application.

- *H2: Security and Privacy Invasion Visualisation*

  – H2.1: Security perceptions per application will be positively associated with the visualisation of security levels;

  – H2.2: Privacy perceptions per application will be positively associated with the visualisation of privacy invasion levels.

4. Methodology

4.1. Experimental design

The user study is based on a split-plot online experimental design. The core of this design is the creation of an intervention that combines the mock-up visualisation of Figure 1 with the calculated security and privacy invasion levels, computed in Section 3.2 and Section 3.3, respectively into a randomised experiment. In the first part, all (n =300) participants are presented with one randomised set of six apps using the mock-ups of Figure 1 and asked for feedback regarding (i) intention to install as well as (ii) privacy and (iii) security perceptions.

Specifically, half of the users (n=150) of the study evaluated one set of six randomised apps, i.e. the green set of Figure 2 by receiving six mock-ups of Actual Invasion shown in Figure 1(a). While the other half (n=150) of the study evaluated another one set of six randomised apps, i.e. the red set of Figure 2 by receiving six mock-ups of High Invasion shown in Figure 1(b). In total the number of evaluated apps for all users (n=300) is 12. The difference between those sets is explained in Figure 2, where the first (green set) assigns users to Actual Invasion group and the second set (red set) assigns users to the High Invasion group. Note that the two sets present the same levels of Security Level, but differ in Privacy Invasion level. The Actual Invasion set contains applications of varying levels of privacy invasion, while the High Invasion set contains apps with the same three levels of security but they are turned into high privacy invasive apps. This enables us to create the Privacy Assignment variable, used in all our models to control for keeping the security level the same, but splitting users into varying and high invasion privacy groups will play a role on their decisions and perceptions.

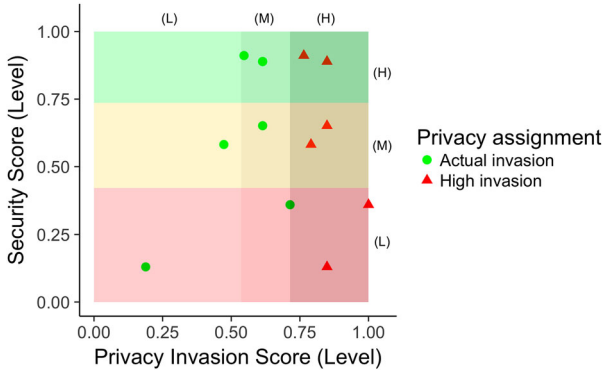

Figure 2. Security and Privacy Invasion scores (levels) for different privacy assignment groups of security apps. Note that the security score is the same for both groups (x-axis). The difference between groups is the privacy invasion. Levels for both dimensions are acquired by their actual quantile range.

For the Actual Invasion group (green circles in Figure 2) we have two apps for each category of the security level: Low, Medium and High; while for privacy invasion we have two apps for Low, three for Medium and one for High. If we move our attention to the High Invasion group (red triangles in Figure 2) we have the same security pairs as the first set, but in terms of privacy invasion they all belong to the High level. The experiment design is counterbalanced among the participants: each participant is presented with the three privacy invasion and three security levels. Thus, they yield nine potential combinations. However, we based our survey on real-world applications, covering seven of these combinations. The explanation for this is that the two combinations, namely High security-Low privacy invasion and Low security-Medium privacy invasion, are not found in the commercial applications we analysed (see Figure 2).

The set of apps is validated in a pilot study among 30 participants to test if they have understood the meaning of the labels. In the following subsection, we introduce the questionnaires used in the study to collect the constructs information.

4.2. Variables and questionnaire

We use a set of 27 questions to represent the 5 constructs with 9 dimensions, displayed in Table 1. The Intervention construct, consisting of the security and privacy invasion dimensions, is not informed by any item question but by the computations of Sections 3.2 and 3.3, respectively. Note that when we use the *Intention to Install* as dependent variable (DV), we control for all the other dimensions. In contrast, when we use *Security* or *Privacy Perceptions* as DV we do not include as a predictor the *Intention to Install* variable, but we control for all the rest. The full list of questions and the correspondent constructs and dimensions appear in Table A1 of Appendix 1. Specifically, the questionnaire is composed of two parts:

(1) An application-related questionnaire that refers to a set of questions for each set (i.e. red or green) of the six apps (Figure 2) regarding user security perceptions (PS1, PS2), privacy perceptions (PP1),

and willingness to install security applications (I1). In this way, the constructs of Perceptions and Intention listed in Table 1 are informed, respectively.

(2) An exit questionnaire (Appendix Table A1) referring to a set of general questions to inform the constructs and their dimensions, namely: Attitudes (Privacy, Security), Motivation (Self-Experience, Norms) and Perceived Behavioural Control (Knowledge, Beliefs) as detailed in Table 1. The purpose of the exit questionnaire is to inform the aforementioned constructs and their dimensions. Furthermore, this questionnaire follows the app-related questionnaire in order not to introduce any bias to user responses on security and privacy perceptions as well as intentions. Note that demographic information is also collected (see Section 4.3).

4.3. Participants

The study questionnaire has been distributed to 300 participants via Amazon Mechanical Turk (MTurk), a crowd-sourcing service that is commonly used for research purposes and is also able to represent a diverse population sample in terms of age, gender and education (Komarov, Reinecke, and Gajos 2013; Kang et al. 2014; Paolacci and Chandler 2014). Qualified users for our study have a 95% approval rate, and the 5% of the fastest responses have been filtered out, thus yielding an average response time of $\mu = 6.67$ minutes with $\sigma = 4.4$. 52% of the participants are male and 48% female. Almost half of the participants (45%) is between 25 and 34 years old, while 24% belongs to the 35–44 age group. Therefore, the majority of the participants falls into the age range that widely uses apps and installs mobile security software. The rest of the sample is distributed in other age-bins. Most of the participants do not use mobile security apps (82%), however, the 85% evaluate themselves as confident and expert computer users.

4.4. Data analysis

The basic goal of the study is to shed light on the factors that affect the (i) intention to install mobile security applications as well as (ii) privacy invasion and (iii) security perceptions. Therefore, we test the aforementioned Dependent Variables, one in each model, while controlling each time for all the remaining constructs of Table 1. In all three models the constructs of Intention, Perceptions and Intervention and their dimensions are represented by one variable in each case (note that for security perceptions we only use PS1 variable in the models due to the strong correlation($r_S = 0.49$, $p \ll .0001$) between PS1 and PS2), thus they are all used in the analysis without any further manipulation. However, for the constructs of Attitudes, Motivation and Perceived Behavioural Control and their dimensions there are multiple items that constitute each construct. Those variables within each construct often present high correlations with each other, potentially leading to multicollinearity issues. In addition, our intention is to create few representative factors for each construct, but more importantly preserve the most of the information contained in each single item (this would be not possible using a variable selection strategy). Furthermore, by gathering all the information derived from single-item questions we manage to reduce the size of the data and provide succinct models.

For all the above reasons we decide to reduce the dimensionality created by the multiple Likert items measuring similar concepts, and thus we apply Principal Component Analysis (PCA) (Jolliffe and Cadima 2016; Neill 2008). Our goal is to come up with specific factors holding the underlying dimensions we wish to control for: Beliefs, Norms, Experience, Knowledge, Security Attitudes, and Privacy Attitudes. Security Attitudes are represented by only one question variable (SA1); hence, this variable is not included in the factor analysis. As seen in Table A2 of Appendix 2, the factor analysis yields six factors. We have used a well-recognised criteria for the factorability of a correlation (Neill 2008). The Kaiser–Meyer–Olkin measure (Kaiser 1960) of sampling adequacy is 0.82, thus significantly above the commonly recommended threshold of 0.6, and the Bartlett's test of sphericity (Kaiser 1960) is significant ($\chi^2(378) = 19.727$, $p < .05$). The diagonals of the anti-image correlation matrix are also all over 0.5. Moreover, we observe from the outputs for components 1 to 3 and 5 that 80% of the selected items load higher than 0.70 on the designated factor and at the same time load less than 0.30 on other factors, and also the outputs represent clearly and independently the predefined concepts' factors.

Components 4 and 6 show the lowest cohesion (*Cronbach's alpha*$<<0.8$), indeed Knowledge and Experience questions fail to create meaningful factors. Therefore, for the representation of Self-Experience we use the raw question (SE1). Regarding Knowledge, only the component 'Knowledge 2' has a relative high *Cronbach's alpha* $= 0.562 < 0.8$, but still less than the recommended one, thus we decide to control for Knowledge by using factor 5, but also the raw question from another component (K6). We use a weighted average of the items belonging to each factor, based on the loading scores.

Data are analysed using Cumulative Link Mixed Models (CLMMs) to deal with the ordinal response variables. We

have also tested an approach based on Linear Mixed Models (LMMs), yielding very similar results. To understand how user's perceptions and willingness to install are associated with the actual security and privacy invasion levels of the apps under study, we assess the differences and trends that emerge between the different computed 'objective' levels and those answers (i.e. Likert data). To do so, we use the non-parametric Mann–Whitney U test, which measures distributions location shift.

All models are built in R (Christensen 2018) and use the probit link function since it is more adequate with random effects, large samples, and when all the dependent variables have an underlying continuous concept (i.e.Likert item 1–7) (Hahn and Soyer 2005). Dependent variables in all models are ordinal, while the independent variables with ordinal nature are treated as latent continuous.

5. Results

5.1. Intention to install

Regarding the *Intention to install* security apps, the results shown in Table 2 confirm the first hypothesis, showing that the security perceptions per app has the strongest significant effect, thus positively affecting the willingness to install the security application (H1.1). Specifically, a unit of increase of the *Perceived Security*, increases the odds by 91% (i.e. $1.91 - 1 = 0.91$; $e^{\beta=0.65} = 1.91$) for the willingness to install (i.e. a shift to a higher level). The fitted CLM model with dependant variable *Intention to install* and the effects of the independent variables are summarised in Table 2, yielding a Nagelkerke pseudo R^2 of 0.48 when compared to a null model. Note that the independent variables are the result of PCA yielded factors and variables as explained in Section 4.4. The variance of the random effect that participants introduce has been captured in the model and has a significant effect. Regarding users' general dispositions about security, *Security Attitudes* positively affect ($e^{0.22} = 1.24$) the installation of security apps. This means that the safer a user feels to share data, the more probable it is to install a security application.

Perceived Privacy Invasion negatively affects the willingness to install the security application, thus confirming H1.2. In particular, every unit of increase in the perception of the user for the privacy invasion of a specific application decreases the odds to install it by 18% ($e^{-0.19} = 0.82$). This could mean that users, who believe that an app collects too much personal data, are less willing to install it.

In our study, we also measure Motivation, defined by (i) Self-Experience, and (ii) Social Norms. Self-Experience positively affects the intention to install the security apps; a unit of increase on experiencing more privacy intrusiveness incidents increases the odds of installing security software by 15% ($e^{0.14} = 1.15$). A similar effect is observed regarding the Social Norms among close contacts: they are found to significantly and positively affect the intention to install the security application. A unit of increase in the Social Norms (*Norms*) increases the odds ($e^{0.24} = 1.27$) of yielding a higher intention level for installing. This could mean that being affected more by own social ties' decisions, increases the odds of installing security apps. Knowledge and Beliefs were found with no significant effect on the intention to install.

Table 2. Observed effects of CLM model for the dependent variable *Intention to install* a security application.

Parameter	Estimate (β)	Std. error
Security Level=[High] [a]	**0.22****	0.07
Security Level=[Low]	**0.21****	0.07
Privacy Invasion Level=[High] [a]	−0.20	0.13
Privacy Invasion Level=[Low]	**0.32*****	0.09
Beliefs (factor 1)	−0.0004	0.08
Norms (factor 2)	**0.24*****	0.06
Privacy Attitudes (factor 3)	−0.15	0.09
Security Attitudes (SA1)	**0.22*****	0.05
Knowledge (K6)	0.03	0.04
Knowledge 2 (factor 5)	0.06	0.11
Self-Experience (SE1)	**0.14******	0.04
Perceived Privacy Invasion PP1 (per app)	**0.19******	0.03
Perceived Security PS1 (per app)	**0.65******	0.03
Privacy Assignment=[High Invasion]	0.15	0.16

Notes: Variables significant at $p<0.0001$ are marked with ****, at $p<0.001$ with ***, at $p<0.01$ with **, while at $p<0.05$ with *. Marginally significant variables are marked with # at $p<0.1$.[a] Medium is used as a reference level.

5.2. Assessing security and privacy invasion levels of applications

Mobile security apps vary depending on the security features they offer and the personal data they require to have access to. The more secure an application is, the more willing are users to install it. The security intervention is significant: the coefficients show that a low security level is associated with a decrease of 19% in intention to install ($e^{-0.21} = 0.81$) compared to a medium security level, while a high security level increases the odds of installing security apps by 24% compared to the medium reference level ($e^{0.22} = 1.24$). This tension is clearly confirmed graphically (Figure 3) by plotting the observed data and comparing the distributions of the ratings. The trend is clearly showing that higher security level results in higher installation preference with significant differences between the security groups.

Turning to the privacy invasion, Figure 3 (right) shows that users prefer to install apps of medium intrusiveness. The results confirm that low privacy invasion is associated with a decrease in the odds of installing ($e^{-0.32} = 0.72$) by 28% compared to the medium privacy

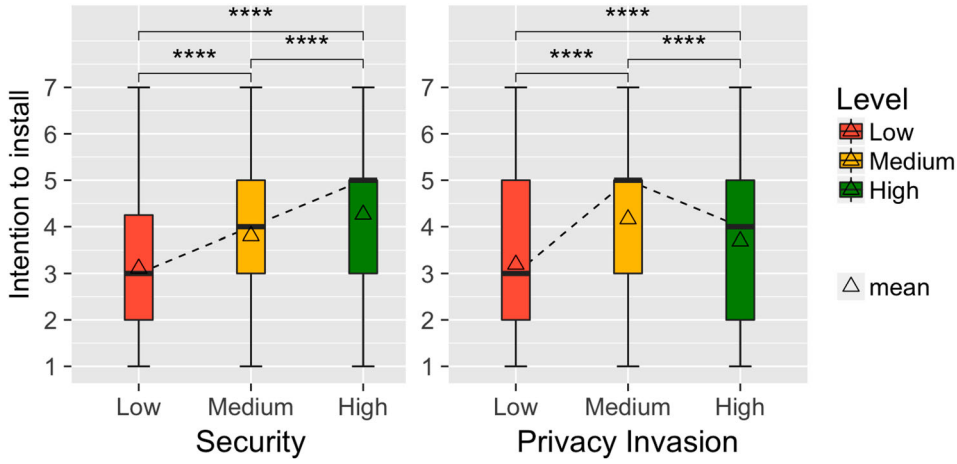

Figure 3. The intention to install as function of Security level perceptions (left) and Privacy intrusiveness perceptions (right). Mann–Whitney *U* Test test applied, ****$p<0.0001$.

invasion reference level, while a high privacy level does not significantly affect the choice. It is worth noticing that users do not prefer the lowest data exposure option: a plausible explanation may be that users realise that an app accessing limited data offers less security features and they seem to consider the offered security level as very important when installing security apps. However, we can also see that users prefer the apps with a medium privacy invasion level (*median*=5) and not the ones of high privacy intrusiveness. This could be interpreted as a statement of the users to mediate data exposure, but sacrifice some of it to obtain a more secure app.

5.3. Evaluating security and privacy invasion level effects on user perceptions

In this section, we investigate how user security and privacy invasion perceptions per application are affected by the security and the privacy invasion level of cyber-security apps (i.e Intervention) as well as by the user perceptions for security or privacy and all the aforementioned behavioural constructs, respectively. Finally, we assess the effect of our Privacy Assignment manipulation.

Hence, we fit two CLM models to explain the security (*Nagelkerke* $R^2 = 0.28$) as well as the privacy invasion (*Nagelkerke* $R^2 = 0.40$) perceptions of users both measured in a 1–7 Likert scale (see Table 3). Note that the independent variables are the result of the PCA yielded factors and variables as explained in Section 4.4. For both models, the random effect created from participants is captured and found significant.

Regarding security perceptions, the question each participant has answered for each security application is: 'The app can protect me from hackers'. As expected, security

Table 3. Observed effects of the CLM models for each dependent variable: (i) perceived security and (ii) perceived privacy per application.

	Perceived Security [per app]		Perceived Privacy Invasion [per app]	
Parameter	Estimate (β)	Std. error	Estimate (β)	Std. error
Security Level=[High]	**0.24*****	0.06	−0.05	0.07
Security Level=[Low]	**0.80******	0.07	**0.26*****	0.07
Privacy Invasion Level=[High]	0.06	0.09	**0.67******	0.12
Privacy Invasion Level=[Low]	**0.4*****	0.1	**0.3******	0.09
Beliefs (factor 1)	0.05	0.06	0.15$^{\#}$	0.08
Norms (factor 2)	**0.11***	0.05	−**0.15***	0.06
Privacy Attitudes (factor 3)	**0.29*****	0.08	**0.71******	0.09
Security Attitudes (SA1)	**0.13*****	0.04	**0.21******	0.05
Knowledge (K6)	0.04	0.03	**0.11***	0.04
Knowledge2 (factor 5)	0.04	0.09	0.01	0.1
Self-Experience (SE1)	0.03	0.031	**0.13******	0.04
Perceived Privacy Invasion PP1 (per app)	−0.02	0.02		
Perceived Security PS1 (per app)			−0.02	0.02
Privacy Assignment=[High Invasion]	−0.10	0.13	**0.40****	0.15

Notes: Variables significant at $p<0.0001$ were marked with ****, at $p<0.001$ with ***, at $p<0.01$ with **, while at $p<0.05$ with *. Marginally significant was marked with # at $p<0.1$.

mobile apps that have *low security level* (i.e. fewer security features) decreases the odds of rating them as protective by 55% compared to the medium reference level ($e^{-0.8} = 0.45$). On the same pattern, apps with *high security level* increase the odds by 27% to be ranked as secure by the user ($e^{0.24} = 1.27$) compared with the medium security reference level, confirming H2.1. Thus, our security intervention is found significant for low and high level, meaning that users understood the score and the visualisation regarding security.

Interestingly, security apps that have *low privacy invasion* level are less probable to be rated as more protective ($e^{-0.4} = 0.67$) in comparison to a medium privacy

invasion level. This perhaps shows that an app with low personal data access requirement could be considered as less secure. Comparing Tables 2 and 3, we observe that security and privacy invasion levels have similar effects to both intention to install and security perceptions, meaning that those two notions are being managed by users similarly.

Regarding the control variables it is worth noticing that *Security Attitudes* (SA1) are measured in terms of how safe users would feel about giving information to mobile security apps. It turns out that the more safe users feel with sharing data to mobile apps, the more probable it becomes to rate an application as more safe ($e^{0.13} = 1.13$). *Privacy Attitudes* factor consists of questions where high scores express user considering privacy preservation important. We observe that users who value privacy as very important are more probable to rate an application as secure ($e^{0.29} = 1.33$). This may suggest that for users who wish to keep their privacy intact, their security perceptions are more probable to be increased by installing a cyber-security application, i.e. they may rely more on it. Finally, being affected more from own social ties increases the odds of rating an app as more safe.

As we can see from Table 3, users strongly consider as intrusive the apps with a high privacy invasion level, since it increases the odds ($e^{0.67} = 1.95$) of scoring higher in *Perceived Privacy Invasion* by 93% (H2.2). While the apps with low privacy invasion levels decrease the odds that a user rates them as intrusive by 27% ($e^{-0.3} = 0.74$) compared to the medium privacy invasion reference level. This tension is confirmed also graphically by Figure 4 (right), where we can observe that for all the different levels of privacy invasion the majority of the users rate them as intrusive (median value is equal to 5). This means that the baseline of intrusiveness is quite high for all the apps of different invasion levels. Clearly users consider all levels as rather invasive, however as we move to higher levels the ratings concentrate on the high intrusiveness values and the groups significantly differ. Moreover, we observe that the apps of low security level are more likely to be considered by users as less invasive ($e^{-0.26} = 0.77$) when compared to the medium reference level. This may be another manifestation of user feeling that low security level is connected with low data intrusiveness. Concerning the controls of this model we denote that *Privacy Attitudes* factor, i.e. user valuing privacy as important, positively affects the characterisation of an application as more invasive ($e^{0.71} = 2.03$), increasing the odds of scoring high in *Perceived Privacy* by 103%.

Our manipulation to assign users in groups (Figure 2) based on the privacy invasion level of the apps (half of the users rated only highly invasive apps, while the other half rated all privacy invasion levels), keeping security stable (viewing all three levels), has an effect only on user *Perceived Privacy Invasion* ($e^{0.40} = 1.49$), but not on security perceptions (*Perceived Security*) or on the intention to install a cyber-security application. This result indicates that users evaluating only high privacy invasive apps of different security levels have a very high baseline about personal data consumption for all the apps. This may have made users to rate the personal data consumption of the apps even higher, but it has no effect on the willingness to install an app and on the security perception. In addition, users who have self-experienced security or privacy violations tend to rate the apps as more invasive ($e^{0.13} = 1.13$). Finally, an increase of users' *Security Attitudes*, meaning users that would feel more safe to share data with mobile apps,

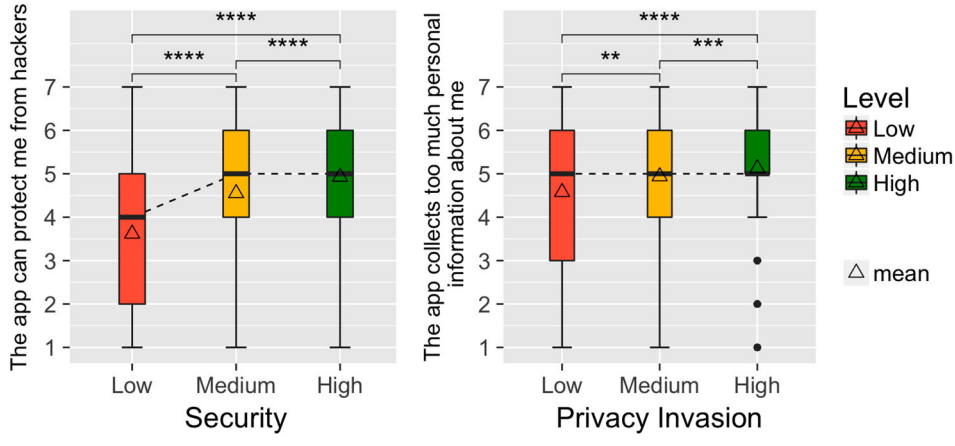

Figure 4. The security perceptions (*Perceived Security*) per app as a function of the security level (left) and the privacy invasion perceptions (*Perceived Privacy Invasion*) as function of Security (left) and Privacy Invasion (right) level. Mann–Whitney *U* Test applied, $^{****}p<0.0001$.

make them more likely to consider cyber-security apps as less invasive ($e^{-0.21} = 0.81$).

6. Discussion and conclusions

In this paper, we analysed the mechanisms and factors behind the willingness to install mobile security apps. We examined not only privacy and security perceptions, attitudes, self-experience, knowledge, and social norms, but also considered the actual privacy intrusiveness and security features of real apps. We have exposed our participants to an informed decision-making process where they are able to express their willingness to install cyber-security mechanisms with varying levels of privacy intrusiveness and security. At the same time, we are able to observe the installation intention as well as to measure the effects of several factors on privacy intrusiveness and security perceptions: specifically, the impact of personal experiences regarding privacy and security, their knowledge on technology, and the impact of social norms.

Our results show that users focus their attention more on security than on privacy when evaluating cyber-security apps. In addition, the Security score is found as a significant factor to explain the Intention to install as well as security and privacy perceptions. For instance, the security level of the application has an increasing positive effect on the installation as it gets higher. Similarly to previous studies, privacy was found to play only a marginal role in smartphone users' selection of apps (Henke, Joeckel, and Dogruel 2018). These findings are supported also by the recent work of Wottrich, van Reijmersdal, and Smit (2018), showing perceived intrusiveness has a negative effect on mobile app users' intention to accept permission requests and that privacy concerns are negatively related to permission acceptance intention. However, this study also finds that users perceive the app value as the more important factor. Chin et al. (2012) also demonstrated that while individuals are concerned with privacy on their phones, the majority of them are comfortable with using location services because of their perceived utility. Similarly, Reuter et al. (2019) have found that app data sensitivity does not play an important role for users' choices for security mechanisms (e.g. information, biometric, token-based).

We also found that privacy intrusiveness has a non-monotonous effect on the willingness to install the application. Apps of medium privacy invasion level are preferred by users for installation (see Figure 3), while apps of low privacy invasion level, are not considered safe enough (see Table 3). From this combination of results, it seems that users are ready to make trade-offs and sacrifice part of their privacy in order to gain additional security features. In our study, for a given security level of an application, users considered the more invasive applications to be more secure (high and medium privacy invasion levels are more selected than low ones for all the security levels). These interesting findings show that low privacy invasion has a negative effect because it can signal that the cyber-security system provides less security.

The willingness to install the application was also affected by the users' privacy attitudes and personal experience. While privacy attitudes about keeping privacy found more intact to adversely affect the decision to install security mechanisms, personal experience of privacy and security incidents had a positive effect. These insights may reinforce the need to provide users with clear information, in addition to their attitudes.

Strengthening privacy in the mobile environment can be approached by different ways. One could think about the re-identification risks and thus use anonymization and aggregation techniques (de Montjoye et al. 2013). Also controlling the re-identification of location and contact data could reduce the risks and sensitive communication patterns that may be monitored could be obfuscated or aggregated, and systems' access to them could be controlled (Toch et al. 2018). Moreover, privacy may be strengthened during the data generation by minimising their collection and reducing data that is collected by privileged apps. The main idea here is allowing the user to control and to understand the rationale behind the data collection. Our findings point to the power of consistent visualisation frameworks on users' decision-making. Frameworks such as those by Kelley, Cranor, and Sadeh (2013) or Chong et al. (2018) have suggested that by presenting privacy information in a clear fashion, users chose apps that request fewer permissions. We extend these results also to present security information, and show that these visualisations have a clear impact on users' intentions. We, therefore, argue that mobile operating systems and similar platforms should try to incorporate these visualisations to facilitate a more informed decision-making process among users.

In this study, we have demonstrated an innovative approach to visualise real security and privacy information, incorporating a visual language at the same frame to represent aggregated scores for different data types. Our findings show that participants understood well the design of the display: however, the security icons are better understood whereas the permissions' framework requires a further investigation. Hence, application designers and developers may adopt the privacy/security design to better inform users about the features offered and the data usage. The

General Data Protection Rules (GDPR) moves in the direction of privacy-by-design and increased user awareness and control (Eur 2016). Users should be part of this trade-off between security and privacy and have the tools to make easy decisions about the privacy implications of the cyber-security technologies that they install. Our work paves the way for further steps towards reaching a clear presentation of privacy implications of cyber-security tools. Future studies may gain further insights and examine the actual installation of security apps rather than the participants intentions.

Finally, our study could be replicated by following a similar strict experimental protocol. Future research may consider different participants or mobile security applications' samples, different levels of privacy and security, and diverse contexts. In terms of confirmability, our outcomes are derived from regression models (Section 5); in almost all cases, independent variables were informed by several item-questions (Appendix Table A1), collapsed into factors through PCA (Section 4.4) and not by using single item-questions for representing a construct. Regarding the constructs used as dependent variables (i.e. Intention, Perceptions) we repeatedly measured user privacy and security perceptions as well as intentions over a randomised set of real applications, covering wide security and privacy levels combinations based on our Intervention (Section 4.1). Our approach also captures user feedback by using several mechanisms such as randomised mock-ups evaluation and answering multiple questions for similar contexts, thus reducing the generated noise during data collection and increasing credibility. Furthermore, we apply validation processes (pilot for mock-ups) and in the analysis we treat variables in their physical ordinal nature. The study depends on public data for the scores' computation and well-known validated constructs for informing the variables.

Our findings have some implications for regulation and policy. Our results point to the uniqueness of cyber-security systems. Similarly to previous findings (Clarke et al. 2016), where users are ready to opt-in for somewhat invasive security countermeasures (e.g. biometrics) to strengthen security, we see that users take different trade-offs when making decisions about security applications. Given the shortcomings of notice and consent in privacy (Nissenbaum 2009), we argue that regulators and policy-makers should set specific frameworks for regulating cyber-security applications. As privacy signals are perceived differently by users for cyber-security, a regulatory framework should include stricter rules on how information can be processed and constraints on the use of the data.

Acknowledgments

The work was supported by the Italian Ministry of Foreign Affairs and Israel's Ministry of Science, Technology and Space project PACS 'Privacy-Aware Cyber-Security', grant number 3-12288. We would also like to thank Claudio Bettini and Erez Shmueli for their helpful comments and feedback.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The work was supported by the Italian Ministry of Foreign Affairs and Israel's Ministry of Science, Technology and Space project PACS 'Privacy-Aware Cyber-Security' [grant number 3-12288] and by Blavatnik Interdisciplinary Cyber Research Center (ICRC) [grant number 590713].

References

Acquisti, A., and J. Grossklags. 2003, May. "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior." In *2nd Annual Workshop on Economics and Information Security-WEIS*, Vol. 3, pp. 1–27.

Ajzen, I. 1991. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50 (2): 179–211.

Ajzen, I. 2002. "Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior 1." *Journal of Applied Social Psychology* 32 (4): 665–683.

Aldehoff, L., M. Dankenbring, and C. Reuter. 2019. "Renouncing Privacy in Crisis Management? People's View on Social Media Monitoring and Surveillance." In *Proceedings of the Information Systems for Crisis Response and Management (ISCRAM)*, València, edited by José H. Canós Zeno Franco and José J. González.

AV-Comparatives, Mobile Security Review. 2015. Accessed May 26, 2019 https://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015 _en.pdf.

Bansal, G. 2017. "Distinguishing Between Privacy and Security Concerns: An Empirical Examination and Scale Validation." *The Journal of Computer Information Systems* 57 (4): 330.

Casaló, L. V., C. Flavián, and M. Guinalíu. 2007. "The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking." *Online Information Review* 31 (5): 583–603.

Chen, J., C. S. Gates, N. Li, and R. W. Proctor. 2015. "Influence of Risk/safety Information Framing on Android App-installation Decisions." *Journal of Cognitive Engineering and Decision Making* 9 (2): 149–168.

Chin, E., A. P. Felt, V. Sekar, and D. Wagner. 2012. "Measuring User Confidence in Smartphone Security and Privacy." In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pp. 1–16.

Chong, I., H. Ge, N. Li, and R. W. Proctor. 2018. "Influence of Privacy Priming and Security Framing on Mobile App Selection." *Computers & Security* 78: 143–154. http://www.sciencedirect.com/science/article/pii/S01674048 18305856.

Christensen, R. H. B. 2018. "Ordinal–Regression Models for Ordinal Data". R package version 2018.8-25. http://www.cran.r-project.org/package=ordinal/.

Clarke, N., J. Symes, H. Saevanee, and S. Furnell. 2016. "Awareness of Mobile Device Security: A Survey of User's Attitudes." *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)* 7 (1): 15–31.

Crossler, R. E., and F. Bélanger. 2017. "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors." In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

de Montjoye, Y.-A., C. A. Hidalgo, M. Verleysen, and V. D. Blondel. 2013. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3: 1376.

Dincelli, E., and S. Goel. 2017. "Can Privacy and Security be Friends? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks." In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Dincelli, E., S. Goel, and M. Warkentin. 2017. "Understanding Nuances of Privacy and Security in the Context of Information Systems."

Di Stefano, A., A. Fornaia, E. Tramontana, and G. Verga. 2018. "Detecting Android Malware According to Observations on User Activities." In *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 241–246. IEEE.

Elliot, A. J., and M. A. Maier. 2012. "Color-in-context Theory." In *Advances in Experimental Social Psychology*, Vol. 45, 61–125. Elsevier.

Eur. 2016. "Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation)." *Official Journal of the European Union*L119: 1–88. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

Felt, A. P., E. Chin, S. Hanna, D. Song, and D. Wagner. 2011. "Android Permissions Demystified." In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 627–638. ACM.

Fishbein, M., and I. Ajzen. 1977. "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research."

Foltz, C. B., H. E. Newkirk, and P. H. Schwager. 2016. "An Empirical Investigation of Factors That Influence Individual Behavior Toward Changing Social Networking Security Settings." *Journal of Theoretical and Applied Electronic Commerce Research* 11 (2): 1–15.

George, J. F. 2004. "The Theory of Planned Behavior and Internet Purchasing." *Internet Research* 14 (3): 198–212.

Google Play Store. 2019. Accessed January 19, 2019. https://play.google.com.

Hahn, E. D., and R. Soyer. 2005. "Probit and Logit Models: Differences in the Multivariate Realm." *The Journal of the Royal Statistical Society, Series B* Series B: 1–12.

Henke, J., S. Joeckel, and L. Dogruel. 2018. "Processing Privacy Information and Decision-making for Smartphone Apps Among Young German Smartphone Users." *Behaviour & Information Technology* 37 (5): 488–501.

Hern, A. 2015. "Apple Removes Malicious Programs After First Major Attack on App Store." Accessed February 25, 2019. https://www.theguardian.com/technology/2015/sep/21/apple-removes-malici ous-programs-after-first-major-attack-on-app-store.

Jain, A. K., and D. Shanbhag. 2012. "Addressing Security and Privacy Risks in Mobile Applications." *IT Professional* 14 (5): 28–33.

Jensen, C., C. Potts, and C. Jensen. 2005. "Privacy Practices of Internet Users: Self-reports Versus Observed Behavior." *International Journal of Human-Computer Studies* 63 (1-2): 203–227.

Jolliffe, I. T., and J. Cadima. 2016. "Principal Component Analysis: a Review and Recent Developments." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*374 (2065): 20150202.

Kaiser, H. F. 1960. "The Application of Electronic Computers to Factor Analysis." *Educational and Psychological Measurement* 20 (1): 141–151.

Kang, R., S. Brown, L. Dabbish, and S. Kiesler. 2014. "Privacy Attitudes of Mechanical Turk Workers and the US Public." In *Symposium on Usable Privacy and Security (SOUPS)*.

Kelley, P. G., S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. 2012. "A Conundrum of Permissions: Installing Applications on an Android Smartphone." In *International Conference on Financial Cryptography and Data Security*, 68–79. Springer.

Kelley, P. G., L. F. Cranor, and N. Sadeh. 2013. "Privacy as Part of the App Decision-Making Process." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3393–3402. ACM.

Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64: 122–134.

Komarov, S., K. Reinecke, and K. Z. Gajos. 2013. "Crowdsourcing Performance Evaluations of User Interfaces." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 207–216. ACM.

Koyuncu, M., and T. Pusatli. 2019. "Security Awareness Level of Smartphone Users: An Exploratory Case Study." *Mobile Information Systems* 2019.

Kummer, M., and P. Schulte. 2019. "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications." *Management Science*.

Lala, C., and B. Panda. 2001. "Evaluating Damage From Cyber Attacks: A Model and Analysis." *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 31 (4): 300–310.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–355.

McCarthy, C. 2009. "ACLU Chapter Flags Facebook App Privacy." Accessed February 25, 2019. https://www.cnet.com/news/aclu-chapter-flags-facebook-app-privacy/.

McCole, P., E. Ramsey, and J. Williams. 2010. "Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns." *Journal of Business Research*63 (9-10): 1018–1024.

Neill, J. 2008. "Writing up a Factor Analysis." 7. http://www.bwgriffin.com/gsu/courses/edur9131/content/Neill2008_Writing UpAFactorAnalysis.pdf.

Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Standford, CA: Stanford University Press.

Nowell, L. T.. 1997. "Graphical Encoding for Information Visualization: Using Icon Color, Shape, and Size to Convey Nominal and Quantitative Data." PhD thesis, Virginia Tech.

Paolacci, G., and J. Chandler. 2014. "Inside the Turk Understanding Mechanical Turk As a Participant Pool." *Current Directions in Psychological Science* 23 (3): 184–188.

Perentis, C., M. Vescovi, C. Leonardi, C. Moiso, M. Musolesi, F. Pianesi, and B. Lepri. 2017. "Anonymous Or Not? Understanding the Factors Affecting Personal Mobile Data Disclosure." *ACM Transactions on Internet Technology (TOIT)* 17 (2): 13.

Reuter, C., K. Häusser, M. Bien, and F. Herbert. 2019. "Between Effort and Security: User Assessment of the Adequacy of Security Mechanisms for App Categories." In *Proceedings of Mensch und Computer 2019*, 287–297.

Sawaya, Y., M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada. 2017. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior." In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2202–2214.

Seneviratne, S. 2018. "Some Cybersecurity Apps Could be Worse for Privacy Than Nothing at All." govtech.com. Accessed March 26, 2019. http://www.govtech.com/applications/Some-Cybersecurity-Apps-Could-Be-Wo rse-for-Privacy-than-Nothing-at-All.html.

Suo, H., Z. Liu, J. Wan, and K. Zhou. 2013. "Security and Privacy in Mobile Cloud Computing." In *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, 655–659. IEEE.

Toch, E., C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, and B. Lepri. 2018. "The Privacy Implications of Cyber Security Systems: A Technological Survey." *ACM Computing Surveys* 51 (2): 36:1–36:27. http://doi.acm.org/10.1145/3172869.

Wolf, F., R. Kuber, and A. J. Aviv. 2018. "An Empirical Study Examining the Perceptions and Behaviours of Security-conscious Users of Mobile Authentication." *Behaviour & Information Technology* 37 (4): 320–334.

Wottrich, V. M., E. A. van Reijmersdal, and E. G. Smit. 2018. "The Privacy Trade-off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns." *Decision Support Systems*106: 44–52.

Xie, W., A. Fowler-Dawson, and A. Tvauri. 2019. "Revealing the Relationship Between Rational Fatalism and the Online Privacy Paradox." *Behaviour & Information Technology* 38 (7): 742–759.

Yao, M.-L., M.-C. Chuang, and C.-C. Hsu. 2018. "The Kano Model Analysis of Features for Mobile Security Applications." *Computers & Security*78: 336–346. http://www.sciencedirect.com/science/article/pii/S01674048 18303341.

Appendices

Appendix 1. Questionnaire and mapping

A.1. Questionnaire

Table A1. Description of the items in the questionnaire corresponding to the constructs and their dimensions of Table 1.

Construct	Dimension	Items
Intention to install mobile security app	Intention	I1 -- I would consider installing this app
Attitudes	Security	SA1- I would feel safe giving information to mobile security apps
	Privacy	PA1-I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of mobile applications collection of data and information PA2- It is very important to me that I am aware and knowledgeable about how my personal will be used by mobile apps PA3 Mobile apps should take more steps to make sure that unauthorised people cannot access personal information in their databases/servers. PA4-To me, it is the most important thing to keep my privacy intact from mobile apps
Motivation	Self Experience	SE1-How frequently have you personally been the victim of what you felt was an improper invasion of privacy SE2- How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet
	Norms	N1- People who influence my behaviour would think that I should install mobile security apps N2-People who are important to me would think that I should install mobile security apps N3-My friends think that I should install mobile security apps N4- Generally speaking, I want to do what my friends think I should do
Perceptions	Security	PS1- The application can protect me from hackers PS2- The application protects against viruses
	Privacy	PP1- The application collects too much personal information about me
Perceived Behavioral Control	Beliefs	Be1-If I wanted to, I could easily manage apps on my own Be2-To what extent are you familiar with the permission requests and the types of data the mobile apps collect Be3- I am familiar with the mobile security apps benefits Be4-I know about countermeasures for keeping the data on my device from being exploited Be5-I know about countermeasures to protect myself from a monetary loss when using mobile apps. Be6-I know about countermeasures to prevent my IDs or Passwords being stolen
	Knowledge	K1-I use a PIN or pass-code to unlock my mobile phone K2-When someone sends me a link, I open it only after verifying where it goes K3-I verify that my anti-virus software has been regularly updating itself K4-Suppose that an app asks to register and to provide personal information. When asked for such information, what proportion of the time do you falsify the information K5-To what extent do you pay attention to read the privacy policy before installing a mobile application K6-To what extent SIM card number can affect the privacy of the user
Intervention	Security level	Calculated security score
	Privacy invasion	Calculated privacy invasion score

Note: Questions were adjusted to the context of this study.

Appendix 2. Factor analysis

Table A2. Factor analysis outputs.

		Pattern Matrix						
	Likert Item	Component 1	2	3	4	5	6	Cronbach's alpha
Beliefs	Be5	**0.8**	−0.023	−0.01	0.011	−0.07	−0.1	0.875
	Be6	**0.86**	−0.097	−0.024	0.03	−0.12	−0.12	
	Be4	**0.84**	−0.02	−0.09	0.03	−0.12	0.000	
	Be2	**0.71**	0.033	0.097	−0.05	0.11	0.18	
	Be3	**0.71**	0.174	0.065	−0.19	0.06	0.17	
	Be1	**0.61**	0.044	0.04	0.08	0.07	−0.01	
Norms	N2	0.026	**0.92**	0.05	−0.01	−0.02	0.03	0.871
	N3	0.056	**0.92**	0.05	−0.07	−0.02	−0.03	
	N1	0.006	**0.91**	0.023	−0.004	0.03	0.05	
	N4	−0.095	**0.59**	−0.15	0.4	0.003	−0.09	
Privacy	PA4	0.05	0.07	**0.84**	0.06	−0.02	−0.1	0.830
Attitudes	PA2	0.05	0.116	**0.82**	−0.14	−0.11	−0.42	
	PA3	−0.0.9	−0.03	**0.79**	−0.18	0.014	0.12	
	PA1	0.03	0.096	**0.74**	0.17	0.04	0.03	
Knowledge1	SE1	0.018	0.09	−0.21	**0.75**	0.11	0.13	0.288
	K6	0.05	0.075	0.28	**0.56**	−0.15	0.06	
Knowledge2	K3	0.10	0.092	−0.006	−0.24	**−0.78**	0.2	0.562
	K2	−0.03	-0.04	0.11	0.12	**−0.71**	0.05	
	K5	0.3	0.02	0.00	0.4	**−0.48**	−0.09	
Knowledge3	K1	−0.07	0.08	−0.09	−0.06	−0.22	**0.76**	0.389
	SE2	0.023	−0.09	0.27	0.19	−0.067	**0.58**	
	K4	0.25	0.04	−0.02	0.14	0.24	**0.47**	

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalisation.
Rotation converged in 8 iterations.