Putting the privacy paradox to the test

Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources

Barth, Susanne; de Jong, Menno D.T.; Junger, Marianne; Hartel, Pieter H.; Roppelt, Janina C.

DOI
10.1016/j.tele.2019.03.003

Publication date
2019

Document Version
Final published version

Published in
Telematics and Informatics

Citation (APA)
Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Telematics and Informatics 41 (2019) 55–69

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources

Susanne Barth[a,b,*], Menno D.T. de Jong[b], Marianne Junger[c], Pieter H. Hartel[a,d], Janina C. Roppelt[a]

[a] University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Services, Cybersecurity and Safety Research Group, PO Box 217, 7500 AE Enschede, The Netherlands
[b] University of Twente, Faculty of Behavioural, Management and Social Sciences, Department of Communication Science, PO Box 217, 7500 AE Enschede, The Netherlands
[c] University of Twente, Faculty of Behavioural Management and Social Sciences, Department of Industrial Engineering and Business Information Systems, PO Box 217, 7500 AE Enschede, The Netherlands
[d] Delft University of Technology, Faculty of Electrical Engineering, Mathematics, and Computer Science, Department of Intelligent Systems, PO Box 5, 2600 AA Delft, The Netherlands

ARTICLE INFO

Keywords:
Privacy paradox
Mobile phones
Apps
Privacy valuation
Privacy intrusion

ABSTRACT

Research shows that people's use of computers and mobile phones is often characterized by a privacy paradox: Their self-reported concerns about their online privacy appear to be in contradiction with their often careless online behaviors. Earlier research into the privacy paradox has a number of caveats. Most studies focus on intentions rather than behavior and the influence of technical knowledge, privacy awareness, and financial resources is not systematically ruled out. This study therefore tests the privacy paradox under extreme circumstances, focusing on actual behavior and eliminating the effects of a lack of technical knowledge, privacy awareness, and financial resources. We designed an experiment on the downloading and usage of a mobile phone app among technically savvy students, giving them sufficient money to buy a paid-for app. Results suggest that neither technical knowledge and privacy awareness nor financial considerations affect the paradoxical behavior observed in users in general. Technically-skilled and financially independent users risked potential privacy intrusions despite their awareness of potential risks. In their considerations for selecting and downloading an app, privacy aspects did not play a significant role; functionality, app design, and costs appeared to outweigh privacy concerns.

1. Introduction

At the time of publication, the number of smartphone users worldwide was just shy of 4.5 billion, with projections for the number of mobile phone users expected to reach the 5 billion mark by 2020 (Statista, 2019). Smartphone users store information and surf

* Corresponding author at: University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Services, Cybersecurity and Safety Research Group, PO Box 217, 7500 AE Enschede, The Netherlands.
E-mail addresses: s.barth@utwente.nl (S. Barth), m.d.t.dejong@utwente.nl (M.D.T. de Jong), m.junger@utwente.nl (M. Junger), Pieter.hartel@tudelft.nl (P.H. Hartel), j.c.roppelt@student.utwente.nl (J.C. Roppelt).

https://doi.org/10.1016/j.tele.2019.03.003
Received 14 November 2017; Received in revised form 13 February 2019; Accepted 16 March 2019
Available online 18 March 2019

online, and by doing so collect (and distribute) large amounts of information. For billions of people around the world, the smartphone has become an indispensable daily companion. For many, the device remains within reach even while sleeping. Some researchers even argue that mobile phones can be seen as an extension to the human body (Shklovski et al., 2014). Because of their round the clock close proximity, smartphones can provide private behavioral information, including location, fitness, both on– and offline activities, social networking operations, and even audio-visual recordings (Aditya et al., 2014). However, most of this data aggregation is not voluntarily or consciously established by the end-user but initiated by business models based on data generation (Buck et al., 2014).

By downloading and installing apps, smartphone users increase the risks associated with design flaws, malware attacks, and data theft. From a technical standpoint, the security and privacy risks associated with mobile applications have long been a cause for concern. By requesting irrelevant permissions, loosely defining permissions, or misusing permissions, combined with highly personalized data aggregation, mobile apps can and actually do provide third parties with sensitive data (Buck et al., 2014; Egele et al., 2011; Enck et al., 2014). Most mobile users are unaware of these threats to their personal data or unable to understand the technical mechanisms behind data leakage (Acquisti et al., 2016). Consequently, information exchanged between electronic devices can be used for user monitoring, leading to a generally wary user attitude towards the credibility of a smartphone's privacy protection mechanisms. Although users might have ominous feelings when sharing information online, they still download and use apps in exchange for financial benefits, personalized services, or enjoyment in any way (Shklovski et al., 2014). Despite a foreboding feeling many users express, the number of mobile app downloads worldwide increases continuously (Statista, 2019). It seems that users download and install mobile applications without hesitation, even if apps require excessive permissions.

When it comes to privacy-related online behaviors, various researchers have drawn attention to the so-called 'privacy paradox', which refers to a discrepancy between users' attitude towards privacy and their actual behavior. Users claim to be seriously concerned about their privacy but in fact do very little to protect their personal data (Acquisti, 2004; Barnes, 2006). Although the downloading and usage of mobile applications, for example, is often accompanied by a sense of insecurity and safety concerns, information sharing online is still on the rise (Zafeiropoulou et al., 2013). This seemingly paradoxical behavior can be explained by various psychological processes that take place during decision-making: (a) Users perform a risk-benefit calculation, guided by rationality, (b) they do show concerns but these concerns are overridden by factors such as desirability of the app, time constraints, or promised gratifications, or (c) they act on their intuition without assessing risk of information sharing online (Barth and De Jong, 2017).

This study aims to address deficiencies in the current privacy paradox literature. Firstly, when compared to the desktop online environment, research into the privacy paradox as it pertains to the mobile online environment is still very limited. Most available studies focus on social networking (Debatin et al., 2009; Dienlin and Trepte, 2015; Flender and Müller, 2012; Hu and Ma, 2010; Hughes-Roberts, 2013; Krämer and Haferkamp, 2011; Oetzel and Gonja, 2011; Poikela et al., 2015; Shklovski et al., 2014; Sundar et al., 2013; Young and Quan-Haase, 2013) and e-commerce activities (Acquisti, 2004; Acquisti and Grossklags, 2005; Motiwalla et al., 2014; Sundar et al., 2013; Wilson and Valacich, 2012), while research focusing on smartphone behavior and the use of mobile applications in particular remains scarce (Deuker, 2010; Oetzel and Gonja, 2011; Zafeiropoulou et al., 2013). Unlike when using traditional phones or computers, users are more prone to privacy intrusion in a (smart) mobile environment (Benenson et al., 2012; Williams et al., 2017), which underlines the need for more research in the mobile domain. Mobile application usage and the resulting data storage are continuously increasing. Considered alarming by many, the user is often excluded from decisions about which data can be shared and which should remain private. In order to support user empowerment, more research is needed into mobile application usage as it pertains to conscious, unintended or unwitting data distribution and sharing.

Secondly, actual behavior is seldom measured in studies addressing the privacy paradox. In order to gain better insights into the privacy paradox and offer an explanation of why people behave online as they do, we want to measure actual behavior instead of drawing conclusions based on stated intentions. This study aims to explore whether or not the privacy paradox is observable in actual behavior, making it more than a theoretical phenomenon which may be attributed to a measurement bias known as the intention-behavior gap.

Thirdly, research has shown that a knowledge and awareness gap can lead to a certain paradoxical behavior as it pertains to information disclosure online. For most users, technical processes that run in the background when doing business online are neither visible nor understandable. Consequently, technical skills (e.g., downloading an app) cannot be equated with technical literacy (e.g., understanding the data flow processes in play while downloading an app), leading to a situation in which users make use of online services despite concerns about privacy or security issues (Liccardi et al., 2014). In order to mitigate the potential influence a lack of technical know-how might have, we studied the privacy paradox among users with a high level of technical expertise and awareness regarding online privacy and security.

Fourthly, financial restrictions are considered a significant factor in this paradoxical behavior as well, especially as they pertain to mobile computing and more specifically, when installing apps on smartphones. Users have a tendency to not buy their apps, even if they cost mere cents (Liccardi et al., 2014). App developers often use advertising or re-use app data for other purposes to generate revenues. It is a proven fact that free versions of many types of apps require a broader scope of permissions—often unrelated to the apps' functionality—than purchasable versions of similar apps (Chia et al., 2012), opening the door to user data misuse. In order to compensate for the possible effects of financial restrictions, participants in our study were provided with a certain amount of money that could be used for, among other things, an app purchase.

Consequently, this research aims to explore users' actual behavior when installing an app on their smartphone, compensating for any influences attributable to technical knowledge and privacy awareness deficits while mitigating the influences of financial restrictions, leading to the following research question: *To what extent do technically skilled mobile phone users, in a setting that is controlled*

for a prominent role of financial considerations, show a discrepancy between perceived privacy concerns and actual privacy-related behavior while downloading and installing a mobile app?

Below, a review is given of the relevant literature on the current situation of data handling and privacy threats, the privacy paradox and privacy concerns as they pertain to the use of mobile computing technology. This is followed by a description of, respectively, the design of our study and the results found. The paper concludes with a discussion of the main findings and their implications, a reflection on the limitations of this study, and general conclusions.

2. Theoretical framework

The purpose of this study was to further investigate some of the factors that play a role in the decision-making process of consumers while downloading and installing an app. The main focus was on the privacy and security precautions users might take during the installation and usage of an app. Many definitions of privacy exist and the concept of privacy has changed over time and with continuously evolving new (smart) technologies. When we talk about privacy, we refer to information privacy. It involves deciding what personal information may be revealed to others and understanding how this personal information is obtained by others and how other parties make use of this information (Westin, 2003).

2.1. Mobile users' privacy and security behavior

The new age of information technology, especially with regard to mobile computing and the associated collection of huge amounts of private data, underlies a substantial business model as organizations might profit from extensive data gathering by trading personal data with other parties, developing new markets and services (Acquisti et al., 2016). Users seemingly disclose information and share their data without hesitation. Relatively vague legislation enables organizations to trade consumer data in order to reduce costs, enhance returns via advertising, and offer personalized services. The legality of the data handling practices conducted by many organizations is considered a grey zone (Spiekermann et al., 2015). Through sharing data publicly on the internet, the line between legitimacy and invasion of privacy is blurred by the users themselves. This does not mean that users are satisfied with the current situation. On the contrary, generally speaking, most users are only pro data sharing if they are consciously involved in the data exchange process, or if the extent of their personal data processing is considered acceptable (Spiekermann et al., 2015). Nevertheless, one can observe that those users that are ill-informed about data handling in particular, are more prone to sharing information. Acquisti et al. (2015) argue that users have to deal with fuzzy boundaries regarding online interactions. From a user perspective, the actual goings on in the cyber world are unclear. Consequently, the privacy experience and the effects of privacy intrusion are not felt directly. If people's personal space is violated in the offline world, many feel immediately uncomfortable with the situation. However, if the proximity related to privacy preferences is breached online, the effect of this violation is less tangible. Benenson et al. (2012) found that users do not translate their knowledge about desktop devices to the mobile context, even though security and privacy threats are similar. Protection mechanisms (e.g. the installation of a firewall) are prominent on computers but not in mobile environments. Furthermore, the technical processes running in the background of certain apps cannot be ascertained via the permissions; even if users take the time to read and understand the agreement covering such permissions. Liccardi et al. (2014) illustrated this problem using the example of a weather app that asks for access to the internet and location information in order to deliver accurate information on current weather conditions. In such cases, users are often unaware that the information in question might also be used for other purposes such as tailoring advertising from third parties. Williams et al. (2017) found that users perceive Internet-of-Things (IoT) devices as less privacy-respecting compared to non-IoT devices, possibly due to hidden data collection or unknown technical processes underlying such smart devices. Privacy valuation seems to be lower in a mobile environment and users seem to value perceived benefits above perceived risks. Although Chin et al. (2012) found that users are less likely to share sensitive data (e.g. health data) on their mobile phones than on their laptops, they use other sensitive services (e.g. location based) because of the perceived benefits of such services. However, the data obtained in a mobile environment are much richer than those in a desktop environment: Portable devices permit service providers to grasp not only few glimpses of users' daily lives but to get a fine-grained picture about daily activities and even inner thoughts and feelings (Wang et al., 2016).

2.2. The privacy paradox

Research into online privacy shows that users are interested in privacy protection but that their privacy concerns rarely translate into actual behavior (Barth and De Jong, 2017; Joinson et al., 2010; Tsai et al., 2006). The discrepancy between expressed privacy concerns and actual, contradictory behavior is known as the privacy paradox: Users claim to have privacy concerns but do not behave accordingly as they engage in risky downloads and seemingly reveal private information without hesitation.

When examining factors influencing this contradictory online behavior, different explanations emerge, many of them focusing on general internet activities such as e-commerce or social networking. According to Kokolakis (2017), users might show distinct privacy behavior in different contexts, suggesting that privacy behavior is highly context dependent. Bergström (2015) found that privacy concerns are increasingly present the more personal an application is, but nevertheless users tend to negate their privacy concerns for the mere reason of enjoying certain services, including mobile computing. In their study on general online behavior, Hoffman et al. (2016) considered privacy cynicism as an explanation for the paradoxical behavior users show online, even intensifying online self-disclosure. Few studies discuss the privacy paradox in a mobile computing context, although the privacy paradox seems to be even more complex for mobile app usage as users might be unable to employ the same protection mechanisms they would in a desktop

environment. In their study on smartphone security, Volkamer et al. (2015) concluded that lacks of awareness, concern, self-efficacy and compulsion prevent users from adopting smartphone security apps. As far as mobile app users are concerned, restricting one's profile as one can on social networks, or adjusting privacy settings is not an option. In this line, Pentina et al. (2016) found that future app use is not limited by privacy concerns. Here, social and informational benefits seem to be the driving forces behind mobile app adoption. In their study on the privacy-personalization paradox among Chinese participants, Guo et al. (2012) found that trust highly mediates the effect of privacy concerns and personalization concerns on intention to adopt a mobile health service, suggesting that benefits of a health service should outweigh privacy concerns. Morosan and DeFranco (2015) found that positive emotions influence the perception of absolute value of mobile hotel apps, obscuring the sight of privacy concerns and enhancing the willingness to disclose personal information. However, ensuring secure data handling methods should be the top priority in order to overcome fear of data misuse and eventually paradoxical behavior. In this line, Sutanto et al. (2013) concluded that a privacy-safe design enhances app usage (process gratification) and interaction with the app (content gratification) and at the same time lowers feelings of personal data being breached, eventually diminishing the privacy paradox.

Furthermore, a lack of technical expertise regarding the conditions and procedures behind mobile computing, the seemingly impenetrable app market business models, and the economics of privacy may play an important role in strengthening the mechanism of the privacy paradox. In their study on users' perceptions of privacy in the IoT domain, Williams et al. (2017) concluded that price and functionality outweigh privacy, leading to the adoption of IoT devices or services despite having privacy concerns. In general, their study showed that users of smart devices engage less in privacy protection tools than non-IoT users. Several underlying psychological processes may eventually lead to people's contradictory behavior: (1) decision-making is based on a rational weighing of benefits and risks of downloading and using apps, (2) the weighing of benefits and risks is biased by psychological processes through extenuating circumstances such as immediate gratification, time constraints, or information deficits or overload, and (3) the risks involved in downloading and using apps is not even part of people's considerations (Barth and De Jong, 2017). All processes may lead to a situation in which benefits overshadow risks. Threats to privacy, such as the excessive collection of data and the installation of malware causing data leakage, monetary loss or disclosure of identifiable data to unauthorized parties are accepted for nothing more than the satisfaction of mobile computing. Users of Android operating systems are often confronted with an all-or-nothing choice in which they must accept all of the requested permissions if they want to download a specific app to their smartphone. Consequently, though users may have permission-related concerns, the desire to use an app seems to outweigh any risks associated with the installation process. Furthermore, searching for and actually downloading and installing an app is characterized by habitual, impulsive or limited processes due to the technical environment in which app purchases take place. The design of app stores and the way apps are presented do not seem to call for high involvement of users; apps are purchased rather automatically, without sufficient attention to privacy considerations (Buck et al., 2014).

3. Method

3.1. Research design

Gaining in-depth insight into the decision-making process of mobile users requires intensive collaboration with actual users. In order to accomplish this, a manageable user group with substantial technical knowledge and skills was studied intensively. For this study we recruited Computer Science students who participated in a Master course on Cyber Crime Science in 2017 and 2018. We placed them in an experimental setting, in which they received sufficient money for buying a mobile app within a certain category and had to choose from five alternative apps, with varying degrees of privacy threats. Instead of merely expressing behavioral intentions, our participants were obliged to download the app on their mobile phone and use it for a week, so that they could write a review of the app. Apart from the actual app selection and downloading, we also administered questionnaires focusing on technical knowledge and skills, privacy awareness, and download considerations, and analyzed the app reviews the participants wrote. The entire research covered a period of three weeks. Fig. 1 gives an overview of the overall design of our study.

The study was approved by the ethical committee of EEMCS faculty, University of Twente. All personal identifiable information was coded so that data from participants in all three parts of the study could be connected. We introduced the research to the participants as a user experience experiment focusing on mobile apps.

3.2. Stimulus materials: Selection of apps

For our study, five apps out of two categories were chosen: utilitarian versus hedonic apps. Utilitarian apps serve to fulfill users' task completion needs, while hedonic apps serve to fulfill entertainment needs (Hazarika et al., 2016). We chose apps from these two categories to explore whether users' privacy considerations differed between them. Hazarika et al. (2016) expect differences in consumer addiction and frustration between utilitarian and hedonic apps. In a study on mobile computing, Wakefield and Whitten (2006) suggest that perceived enjoyment (attributable to hedonic value) enhances cognitive absorption, which in turn promotes usage behavior of a mobile device. Based on these findings we assumed that using an app for a utilitarian or hedonic purpose might lead to differences in privacy evaluation. Entertainment needs might make users less cautious when it comes to privacy valuation, as fun and enjoyment might be valued as more important than privacy protection.

As a typical representative in the utilitarian category we chose a to-do-list app; for the hedonic category we chose a tower defense gaming app. The selection of app categories was based on the study of Heinonen and Pura (2006) and a pre-test with 25 participants. Only apps that were actually available in the Google Play Store (Android Version 7.1.1) were selected.

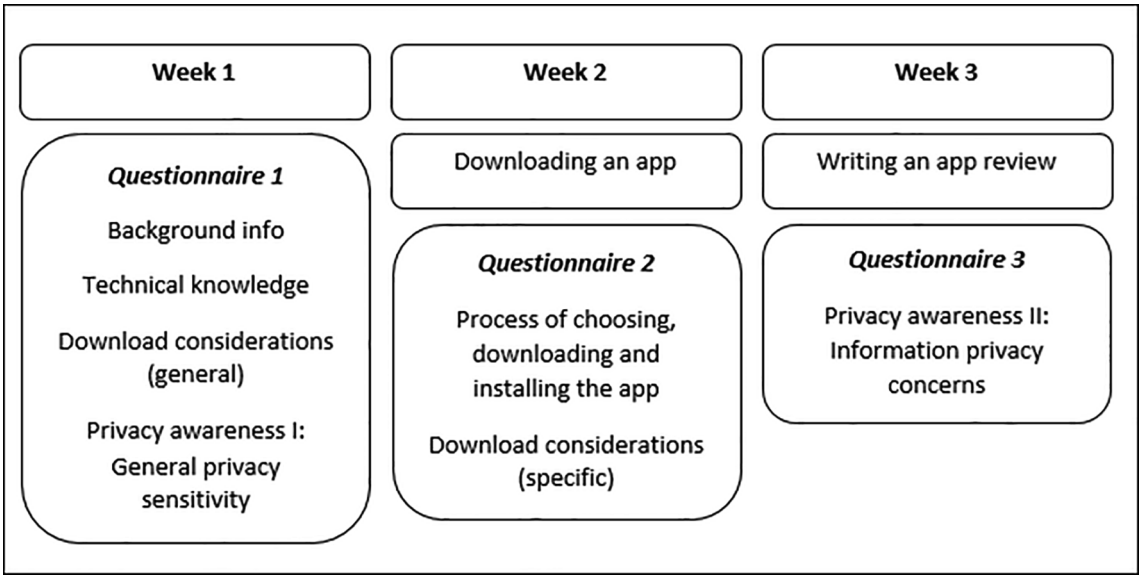

Fig. 1. Overview of the research.

Within both categories, we selected apps with similar core features and an increasing number of permissions requested. Hence, all apps from the to-do-list category had to (1) use the term "to-do-list" in the title or in the description of the app, (2) provide creation, management and categorization of tasks, (3) be able to set reminders, and (4) share notes and (5) have a user rating of four or higher out of five stars. For the gaming app, all five apps had to (1) belong to the tower defense game category, (2) provide different gaming levels to be achieved, (3) protect someone or something from someone or something, and (4) have a user rating of at least four or higher out of five stars. The apps in both categories had to differ in terms of permissions requested, ranging from a purchasable app that asked zero permissions to free of charge apps that asked up to seven permissions (identity, contacts, phone, photos/media/files, WIFI connection information, device ID, and call information). The increasing number of permissions had to be similar between the two categories. Another selection criteria for the apps was that the permissions requested had to be shown to users before they actually install the app on their smartphone. The apps were selected in collaboration with a computer science expert and a privacy intrusiveness score was assigned to them, ranging from not intrusive (zero permissions requested) to very intrusive (between five and seven permissions requested). The privacy intrusiveness scores were used to classify the apps according to the number of permission requested: The more permissions requested that were unrelated to the apps' core functionality, the higher the intrusiveness score. An overview of the selected apps, requested permissions, and privacy intrusiveness scores can be found in Appendix A.

3.3. Procedure

The first part of the study took place during the first lecture of the Master course. After reading and signing a consent form, participants started by filling out the first questionnaire, focusing on participants' background information, technical smartphone knowledge and skills, privacy awareness, and download considerations in general. The privacy awareness questions in the first questionnaire were rather general, so that participants were not prompted that privacy was the main point in the research.

In week 2, the experimental part of the study took place. We explained to the participants that we would like them to evaluate the user experience of a specific app and therefore asked them to download an app in a specific category, use it, and write a short review. Participants were randomly assigned to one of two categories of apps (to-do-list vs. game). Before starting with the selection of an app, participants were given 10 euros with the instruction that they could use the money for an app purchase but were also allowed to keep it. We explicitly informed participants that they were totally free to decide which app to download and install on their smartphone. We requested all participants to use the app over the course of the following seven days to be in the position to write a comprehensive review about the app. After having installed the app, participants were asked to describe the process of choosing, downloading and installing the app and to explain why they had chosen for this particular app (and not for the other options). After that, participants filled out the same questionnaire about their download considerations, this time in relation to the downloading and installing of the specific app.

In week 3, participants were asked to write a review of the app they had downloaded and used over the course of the previous week. This was deliberate, as writing a review significantly differs from describing individual decision-making processes when downloading an app, or justifying ones selection for a particular app. User reviews can be defined as an implicit form of user-centered communication focusing on 'perceived ease of use' or 'perceived usefulness' (Davis, 1989; Vasa et al., 2012). Our main goal of the review assignment was to verify if privacy related factors played a role in the creation of co-value for other users (Tan and Vasa, 2011). We also included three control questions to ensure that subjects actually downloaded the app. After writing the review, the

participants filled out a third questionnaire about their privacy awareness.

3.4. Measurement instruments

In questionnaire 1, participants answered several *background questions*, regarding demographics (age, gender, study program) and general app usage. One item was adapted from Yang (2013), investigating the number of apps someone has ever installed by his/herself on their smartphone (open question). Furthermore, we asked the participants which categories of apps they used on their smartphone: Participants could choose from 36 categories (as mentioned in the Google Play Store) in total.

To verify participants' *technical knowledge and skills*, four self-report questions about their knowledge and skills, based on Kraus et al. (2014), were asked in questionnaire 1. For instance, participants had to indicate whether they are able to protect themselves against data misuse. This scale's Cronbach's alpha was 0.61. In addition, questions were asked in questionnaire 1 about the extent to which they showed privacy and security related behaviors on their mobile phone. The questions were adapted from Androulidakis and Kandus (2011), and focused on behaviors such as using Bluetooth functions and running an antivirus app on their smartphone.

In questionnaire 1, the Westin Privacy Index, based on Kumaraguru and Cranor, 2005 survey of Westin's studies, was used to obtain a general privacy sensitivity index of the participants and to investigate *general privacy awareness*. Three items concerning perceived loss of control over private data, data handling practices by third parties and laws and regulations pertaining data protection were measured on four-point Likert scales (1 = strongly disagree; 4 = strongly agree). The calculation of the privacy index was done according to Kumaraguru and Cranor guidelines, 2005.

In questionnaire 3, participants filled out a Mobile Users' Information Privacy Concerns Scale, which was adapted from Xu et al. (2012). The scale consisted of 9 items measured on seven-point Likert scales (1 = completely disagree; 7 = completely agree). The scale contained the following constructs: perceived surveillance ($\alpha = 0.91$), perceived intrusion ($\alpha = 0.84$), and secondary use of personal information ($\alpha = 0.80$). To enhance Cronbach's Alpha value of the construct perceived surveillance, one item was deleted, ending up with 8 items for this scale.

To investigate participants' *download considerations*, we presented them with a list of 18 aspects that could be considered when deciding to download an app, both in questionnaire 1 (in general) and in questionnaire 2 (after downloading the specific app). By doing so, we explored if the perceived importance of factors differs when participants give general estimations versus when they have just made a decision to download an app. The questionnaire contained seven privacy and security related factors (e.g., trustworthiness of the app, and number of permissions requested), and 11 other factors (e.g., prior experience with the app, price, and design). Participants answered on seven-point scales (from "completely disagree" to "completely agree").

The complete set of questionnaires can be found in Appendix B.

3.5. Participants

All participants (N = 66) were university students with a technical background in the Netherlands: 60 students followed the Computer Science Master program, three students attended the Electrical Engineering Master curriculum, two students studied Technology Management, and one student was completing a Business Information Technology Master. Their ages ranged between 19 and 55 years, with an average age of 23.5 years (SD = 4.6). At 83% male and 17% female, the gender distribution in this study reflects the current male–female ratio in the technical Master programs. Obtaining a viable participation number large enough to compensate for any gender issues was deemed unfeasible. For the analysis of the experimental part of the study, only data from participants running an Android operating system (77%) on their smartphones who had filled out all three questionnaires were included in the analysis (N = 39).

Since owning their devices, participants reported having installed an average of 53 apps (SD = 41) on their smartphone. On average, participants had already owned a smartphone for 7.1 years (SD = 2.8). They spent an average of 2.6 h a day using their mobile devices and interacted with an average of 10 mobile apps (SD = 6.1) during a normal week. In general, participants considered themselves to be experienced in using mobile apps (M = 6.0, SD = 0.7; measured on a seven-point Likert scale).

Apps with a communication purpose (e.g. 'WhatsApp') were the most popular app category participants use on their smartphones (95%), followed by 'business' (77%; e.g. Office and PDF') and 'maps and navigation' (76%; e.g. GPS navigation). In contrast, categories such as 'medical' (8%; e.g. 'DocCheck') or 'house and home' (8%) were rarely used.

Usually, when looking for new applications, 52% consulted an app store in general, whereby 46% indicated Google Play Store to be the main app store used to gather new info on new apps on the market. Furthermore, 6% of participants based their decisions for downloading new apps on reviews, 14% used search engines to gather information on new apps available and 2% relied on their own experience.

Of the participants, 98% indicated that their smartphones had never been lost or stolen. Only 3% of the participants claimed that they lent their smartphone to others without hesitation, whereas 64% would only do so for a short while and if physically present; almost one third of the sample claimed that they never shared their smartphones with others (33%).

3.6. Analysis

Quantitative data analysis was divided into two parts: For the first questionnaire, the analysis was done on the basis of the 66 participants that completed the questionnaire. However, for the analysis of the downloading process and the second questionnaire, subjects that did not run Android operating system on their smartphones and did not go to the Google Play Store to obtain the app,

were removed from further analysis. This resulted in a sample of N = 39 participants that took part in all three parts of the study.

The description of the process of choosing, downloading and installing the app and the reviews were analyzed qualitatively by means of a coding scheme, aiming at identifying concepts that relate to the question of interest (here: willingness to download an app). The coding scheme was based on the 17 download considerations asked for in the first and second questionnaire. Based on an open coding process, which means identifying other key factors that are not pre-determined or based on existing literature and concepts but emerging from the textual data directly, 13 factors were eventually added to the coding scheme (e.g. color, interface, name of the app). To ensure inter-rater reliability and for validation of the coding scheme, the two open questions from the second part of the study and the review were coded by two independent coders. Subsequently, the coding of the two raters were compared and an agreement score, called Cohen's kappa, was calculated. Cohen's kappa measures the agreement between raters in their codings, correcting for chance agreement. The Cohen's kappa was 0.88, which indicates substantial agreement between the two coders.

4. Results

Below, the results of the quantitative and qualitative analysis of the data will be presented. In the first two sub sections, overviews will be given of, respectively, participants' technical knowledge and skills and their privacy awareness. After that, the focus will be on their app downloading and installing behavior. The final sub sections will, respectively, focus on the results regarding download considerations and the reviews.

4.1. Technical knowledge and skills

The following results give an indication of the participants' level of technical knowledge as it pertains to smartphones and how participants actually deal with situations that might affect smartphone privacy and security. Overall, the results show that participants confirmed to have a relatively high knowledge level regarding the technical aspects of their smartphones (see Table 1). This reflects the technical backgrounds of the participants. Looking at the cumulative percentages of disagreement or agreement, participants considered themselves to be highly knowledgeable and well-informed.

Asking participants about a smartphone's technical specifications, 73% indicated to know where you can find the mobile phone's IMEI (International Mobile station Equipment Identity: a 15-digit code that uniquely identifies valid smartphone devices, comparable with a PC's MAC address). In case of loss or theft, the IMEI code can prove helpful in smartphone retrieval. Thus, for security reasons, it is helpful to know its IMEI.

After (re)starting their smartphones, 92% made use of a PIN code for unlocking their SIM card and almost the same number of participants used a PIN code or password to unlock the phone itself/screen-saver (85%). Locking one's SIM card with a PIN code supports data security as this inhibits unauthorized access. Furthermore, entering the wrong PIN code several times may lock the SIM card permanently. Activating the locking-function of the screen-saver is an additional security protection mechanism.

From the sample, 38% never used the Bluetooth function of their smartphone, whereas 52% claimed they do use Bluetooth but only for a specific purpose, after which the Bluetooth function is deactivated. Only 9% had their Bluetooth permanently activated and thereof 8% claimed to use to have their device visibility setting set to 'not visible'. The current security processes employed by Bluetooth wireless technologies are considered adequate, but the protocol might present a door-opener for attackers, such as worms and viruses or 'bluebugging'.

Relatively few participants employed an antivirus app on their mobile device (27%) and even fewer ran static analysis apps to monitor malicious code patterns, to inspect control flow between apps, or to review requested permissions (17%). While these results may appear low, it should be noted that, compared to the results of Androulidakis and Kandus' (2011) study, the antivirus numbers in this sample are approximately 100% higher.

When analyzing any sensitive data owners store on their smartphones, 5% stored passwords without encryption, 32% stored passwords such as credit card passwords with encryption, and 62% indicated to never store passwords on their mobile devices. The protection of personal data through encryption technologies reduces the risk of surveillance by third parties and enhances both anonymity and privacy. However, 83% of the sample confirmed that they have sensitive personal data such as photos, videos or audio recordings on their smartphones.

Of the sample, 70% claimed to create backup copies of their phone's data; 3% of them indicated that such backups follow no particular schedule (e.g., after resetting the mobile phone or a cleaning action), 20% backed up their data continually, for instance in

Table 1
Participants' knowledge about mobile phone's privacy and security (N = 66).

	M	SD	Disagreement (%)	Agreement (%)	Undecided (%)
Communication through mobile phones is safe.	3.4	1.7	61	38	1
I am aware about how technical characteristics affect security.	5.1	1.5	17	76	7
I know how to protect myself against data misuse.	5.2	1.6	15	82	3
I know how to protect myself from malicious apps.	4.9	1.5	23	73	4

Note: Measured on seven-point Likert scales (1 = completely disagree, 7 = completely agree).

Table 2
Overview of mobile users' information privacy concerns (MUIPC; Xu et al., 2012).

Construct	Explanation	M	SD
Perceived surveillance	Practice of data collection, track and profile mobile users	5.5	1.3
Perceived intrusion	Violation of physical and informational space	4.8	1.4
Secondary use of personal information	Unauthorized data usage for secondary purpose	5.3	1.1

Note: Measured on seven-point Likert scales (1 = completely disagree, 7 = completely agree).

a cloud, 12% ran a backup on a daily basis, 6% weekly, 12% monthly, 5% quarterly, 8% semiannually, and 5% annually. Backup copies are considered essential by security experts as security violations can often result in data losses.

4.2. Privacy and security awareness

A calculation of privacy sensitivity scores based on Westins' Privacy Index (Taylor, 2003) showed that privacy was not an issue for 9% of the sample. These individuals showed little or no hesitation when it comes to disclosing private information as they considered the benefits of information disclosure to far outweigh any potential risks. Of the sample, 41% can be assigned to the group of pragmatists. They weighed the potential costs and benefits of information disclosure before progressing. Pragmatists are willing to disclose information if they perceive their privacy protection expectations met and the party in question to be trustworthy. The majority of the participants can be described as fundamentalists (50%). Fundamentalists are at the maximum end of privacy concerns. They put responsibility for privacy protection at the individuals' level and require proactive refusal of information disclosure by users.

With regard to user privacy and security issues, the results showed that the significant concerns participants have in general are intensified when it comes to their smartphone usage. Generally speaking, participants were concerned that mobile apps monitor their activities and that often too much personal information is collected. The level of privacy intrusion by mobile apps in general was perceived to be relatively high. The level of concern regarding secondary use of personal information was even higher. A comprehensive overview of the results is given in Table 2.

4.3. Actual privacy-related behavior

Below, the results from the experimental part will be presented. Although there were less intrusive alternatives available, many participants selected the most intrusive mobile app, i.e. the app that requested most permissions that did not relate to functionality (28%). Furthermore, 49% downloaded the app that was analyzed as intrusive, and another 18% chose the app that was somewhat intrusive. Only 5% of the participants decided to buy an app that did not ask for any permissions. One participant withdrew from downloading and installing an app due to privacy concerns. Table 3 provides an overview for both types of app. We can observe that for both app categories most participants chose the intrusive or very intrusive app, despite having the extra money for buying a non-intrusive app. The differences between the type of app (utilitarian vs hedonic) were not statistically significant.

4.4. Participants' download considerations

Table 4 provides an overview of participants' download considerations in general (before the assignment to download a specific app) and immediately after downloading the app. Based on these results, several observations can be made. The first is that in both questionnaires the privacy and security related considerations did not play a prominent role. In the first questionnaire, only trust in the app and the relation between permissions and app functionality were in the upper half of the considerations. In the second questionnaire, only the number of permissions requested and the relation between permissions and app functionality were in the upper half.

A second observation is that specific and relatively easily judgeable considerations were more prominent in the second questionnaire than in the first. General considerations participants had in the first questionnaire when reflecting on downloading apps, all requiring the combination and weighing of several features, were often replaced by much more straightforward considerations in the

Table 3
Relation between app intrusiveness and participants' download decisions for the two types of apps (in percentages) (N = 39).

Type of app	Number of requested permissions				
	0	1–2	2–4	4–6	5–7
To-do-list	0	0	18	55	27
Game	12	0	18	41	29
Overall	5	0	18	49	28

Note: See Appendix A for a more detailed overview of the categorization of app intrusiveness.

Table 4
Mean ranks of download considerations before and after downloading and installing the app.

Considerations	Before installation	After installation
Perceived functionality of the app	1	4
Perceived usefulness of the app	2	8
* Trust in the app	3	12
Price of the app	4	1
Ratings given by others ("star system" in the app store)	5	2
Reviews about the app (written by others)	6	6
* If permissions relate to functionality	7	7
Number of downloads (as indicated in the app store)	8	10
Recommendation of others	9	15
Prior experience with app	10	17
* Number of permissions requested	11	5
* Clarity of permissions (if permissions are understandable)	12	9
Familiarity with the app	13	16
Design of the app	14	3
* Privacy conditions (e.g., information disclosure to third parties)	15	13
* Readability of permissions (comprehensibility for the user)	16	11
* Security conditions (e.g., if data protection is ensured)	17	14

Note: Privacy and security related factors indicated with asterisks.

second questionnaire. The top three considerations in the first questionnaire (functionality, usefulness, and trust) were replaced by price, ratings, and design in the second questionnaire. Especially the role of design is remarkable: In the first questionnaire it took a 14th rank. Within the privacy and security domain, trust in the app went down from a third rank to the 12th position, and some of the more specific considerations, most notably the number of permissions requested got higher ranks. This tendency seems to reflect that it may have been hard for participants, despite their technical knowledge and skills and their privacy awareness, to incorporate privacy and security considerations in their download decisions.

A third observation involves a mismatch between the considerations mentioned by the participants and their actual downloading behavior. The number of permissions requested ranked 5 in the second questionnaire. However, many participants ended up downloading the app that asked for the most permissions. Thus, it appears that participants claimed to have privacy concerns that are not reflected by their actual behavior. Privacy considerations are anchored in users' mindset but do not manifest themselves as a top-priority.

When describing their decision-making process while choosing for an app, downloading the app and eventually installing it, about 8% of the participants mentioned the factor *permissions.* Of these, the majority indicated that permissions asked by the app played a role in their decision whether or not to download it as they "*looked at […] the permissions it required,*" "*checked permissions,*" or "*secondly I looked at the permissions the app needed.*" However, participants who claimed to have looked at permissions asked by the app often chose to download the app that was judged as somewhat intrusive rather than the paid app that asked for zero permissions nonetheless. Some participants appeared to be discouraged by the required permissions and withdrew from downloading an app even though they thought it to be the most attractive one "*because it required a lot of privacy sensitive information."* Some comments were more nuanced and specifically mentioned if permissions relate to functionality by reviewing the privileges the app asked for "*to check whether they were logical for this kind of app."* Sometimes, users felt uncomfortable because of the requested permissions as one participant stated that he had *"inspected the permissions and was baffled by what some applications wanted."*

When asking participants why they chose the app they actually downloaded instead of another, price is mentioned more often as in the former description of their decision making process. Hence, the factor price and whether the app can be downloaded for free seems to play a major role in the decision-making process. Some participants simply considered an app as feasible to download "*because it is free*" or they generally "*never*" pay for an app. Some participants indicated a willingness to only pay under certain circumstances or for specific types of apps as they prefer "*not to give my banking information for a simple game."* Free alternatives available in app stores was also a reason for not paying for an app, or as one participant put it: *"why would I pay for something that I can get for free?"* Other participants indicated that they are only willing to pay for an app if someone within their social circle recommended it: *"only when good friends advise on a payed app, I will buy that straight away."* Other users would like to test an app before buying it because *"if I have to pay for every app I test, and most probably discard, that's not a good incentive for the app writer to make it better."* Again, design of an app, functionality and requested permissions seem to have top priority in the evaluation process as well as 9%, 7% and 6% of the sample mention these factors respectively. The quotes of these categories are similar to the ones mentioned in the description of the decision-making process and will therefore not be presented twice.

4.5. Privacy and security related considerations in the reviews

When looking at the reviews participants wrote about their app, it is remarkable that privacy and security considerations were barely mentioned. In line with the descriptions of the decision making process, factors that are visible and that can be directly experienced by the user were dominant in the reviews. An analysis of the reviews showed that usability (19%), ease of use (17%), design (16%), and functionality of the app (12%) were most often mentioned. Privacy and security issues only played a minor role, if

any, in the participants' evaluations of the chosen apps for others. Although the requested permissions had played a minor role during the downloading and installation process, they were virtually absent in the reviews. Privacy and security considerations were discussed in only 8% of the reviews. Participants, for instance, were worried about the permissions requested, because the app *"asked for too many permissions like creating and deleting accounts and even changing the password of accounts."* One participant linked permissions to the functionality of the app as he recognized that *"the app asks for permissions that are (in my opinion) not needed for normal use of the app."* Consequently, this participant declined the permissions after having downloaded the app. Another participant reported having changed the permissions afterwards because he felt *"that the game required too many permissions* (i.e. *wanting to access your contact list)"* and he *"turned the permissions off immediately."* However, participants mentioning privacy concerns still had chosen to download the app that was deemed to have privacy problems.

5. Discussion

The purpose of this paper was to research the phenomenon of the privacy paradox. More specifically, this study aimed at exploring whether or not the privacy paradox is in fact observable in actual behavior and not attributed to a given intention/attitude-behavior gap as reported in literature (Baek, 2014; Barth and de Jong, 2017; Dienlin and Trepte, 2015).

First, by means of an experiment, actual behavior was examined with regards to downloading and installation patterns. Here, we controlled for technical expertise and financial considerations by studying a tech-savvy user group and providing monetary compensation. Second, we determined the factors that play a role in the decision-making process as it pertains to selecting, downloading and installing an app at two moments in time: before and after the actual installation process with a major focus on privacy and security. The reasoning behind this model was to compare declared intention and attitude with self-reports on actual behavior. By doing so, data from the experimental part of this study could be collated with results of self-reports. Both parts of the study served for confirmation and validation of each other. In this final section, the main results will be reviewed and implications for user empowerment, support and future research will be given.

5.1. Main findings

Results showed that, in general, users do not rank privacy and security related aspects as a high priority when considering factors that guide the downloading and installation process of an app. Factors such as price, ratings and design seem to play a major role in the downloading decision, although participants indicated previously that usefulness, functionality and trust in particular influence their app choice. This is in line with the findings of Kelley et al. (2013) who found in their study on app decision-making process that users consider factors such as cost, functionality, design, ratings, reviews and downloads as more important than requested permissions. Apps with higher ratings are higher listed in the display search function of the app-store. Hence, these apps will be more often recognized, valued and downloaded by users (Dehling et al., 2015). Furthermore, while self-reporting on the actual downloading and installation process of an app, participants mentioned that permissions play a major role in their selection of an app. However, the experiment showed that participants did not behave in accordance with their previous indications. When talking about location based applications, Zafeiropoulou et al. (2013) found that users to not act according to their previous stated privacy preferences as benefits of such apps outweigh privacy concerns. This behavior is also represented in the peer reviews, written by the participants, as privacy and security related factors are rarely mentioned. This leads us to assume that privacy and security as concepts seem to play a minor role in the mental representations of users. Functionality and design seem to outweigh privacy concerns or privacy is not considered as an important part in the overall evaluation or recommendation of an app. Hence, it seems that privacy does not play a role in the social representation of factors that are considered important when talking about, reviewing, or actually downloading an app. This is in line with Kehr et al. (2015) who suggest that the social representation about privacy is not yet formed by lay-users. It would seem that privacy is but a marginal note in the adoption process of mobile apps. This prompts the question: How much do consumers really value their data and privacy?

5.2. Implications

The results of this study were ascertained from a tech-savvy target group possessing technical expertise above the average user. Not only did participants describe themselves as informed about technical issues regarding smartphones and mobile applications, but the sample expressed privacy concerns by implementing data protection measures and restricting unauthorized information distribution to third parties. Despite these concerns, these individuals where not willing to pay for an app that asked for less information by means of permissions. These finding correspond with the study of Williams et al. (2017) who found that knowledge about risks regarding IoT does not prevent users from buying and using such products. Although users knew about certain risks pertaining to IoT products and revealing private information, such users seemed to value their personal data less and struggled significantly more to protect their data compared to non-IoT users. Furthermore, the paradoxical behavior (having concerns and revealing private information) was more present among IoT users compared to non-IoT users. This again raises the question about privacy valuation of mobile app users and how they actually perceive privacy aspects in an online environment.

On a similar note, this paradoxical behavior prompts the question as to whether or not even subjects with a technical background understand enough about permissions and their potential ramifications. The understanding of permissions is a crucial component in privacy consideration as without sufficient knowledge about permissions warning, users are unable to make adequate privacy decisions (Felt et al., 2012). Benton et al. (2013) also concluded that permissions are difficult to understand for users and ineffective

when it comes to privacy considerations. In their study on user attention, comprehension and behavior regarding Android permissions, Felt et al. (2012) determined that only 17% of participants paid attention to permissions and almost half of the sample did not notice permissions at all. Comprehension levels were also rather low. Deuker (2010) concluded that enhancing privacy awareness alone is not the solution for this complex problem. Users need supporting tools in order to react according to their privacy preferences.

When looking at even the newest version of the Android permission system, permission requests take place rather late in the process. Users have already installed the app on their smartphones before being asked to grant certain permissions. One might hypothesize that this is a conscious ploy that takes advantage of a weaknesses in human nature: If a user has already carried out the cognitively demanding efforts employed when selecting an app such as evaluating price, design and reviews, then downloads and installs an app, the cognitive effort to evaluate the ramifications of granting permissions afterwards might be too high, leading to a situation in which privacy and security risks are accepted despite privacy concerns. Furthermore, explanations of single permissions (or from Android 6.0 on the higher permissions groups) are not directly visible for the user, meaning they have to perform a further task to obtain this information. This might lead to a decision guided by simple heuristics: the user denies and uninstalls an app, implying that all efforts made are nullified, or the problem is relativized and accepted despite privacy concerns. The latter seems to be more common and could prove a major factor in the privacy paradox. This assumption however, has not been researched to date. The scope of permissions and their implications might be considered an inherent part of privacy valuation. As such, more research is needed into this domain, not only from social and behavioral perspectives, but from a technical point of view as well. The key questions remain the same for both perspectives: How can we improve the existing Android permission system to enhance user empowerment and what are the alternatives to the permission system in question? Privacy has to become part of the social presentation of users in order to be a valuable asset. Understanding the public's mindset as it applies to the handling of mobile applications and adapting interface design (of permissions) to cognitive styles, raising awareness, increasing knowledge and providing support while simultaneously empowering users seems to be the key to putting online privacy on the agenda. Considering the impact of privacy and security risks, Dehling et al. (2015) suggest that the type of app (e.g. what and how much data is gathered) should be taken into account for protection mechanisms but also for tailored risk sensitization (e.g. what is the impact of a specific data sharing process). However, empowerment of users to make self-determined and self-protective decisions with regards to their personal data behavior should be a top priority. Promotion of privacy protection behavior should help users to overcome the paradoxical behavior that we can still observe when dealing with mobile computing and in particular with apps.

5.3. Limitations and future research

This study reflects a first attempt to put the existence of the privacy paradox to the test in more extreme circumstances, focusing on actual behavior instead of behavioral intentions and eliminating some of the potential explanations for the paradoxical behavior (a lack of knowledge, privacy awareness, or money). The results support the existence of the privacy paradox in these circumstances. However, it is important to keep in mind three limitations of our study. The first limitation involves the sample size. Mainly due to the intensive nature of the data collection, our sample size was rather small, even after two years of collecting data. The experimental results of our study are quite clear, even within the limited sample, but a larger sample would have enabled us to further explore the relationships between knowledge, awareness and download considerations. Future research could study such relationships more extensively.

A second limitation involves the artificial context used in the research. The participants in our study were only required to download and use the app for one week, and we cannot be certain whether they would have downloaded and used the particular type of app in real life. It is imaginable that the participants acted somewhat pragmatically, knowing that they could discard the app one week later. However, during that week, they still exposed themselves to the privacy and security risks of the app they downloaded. Future research could focus more on apps that users actively use for a longer period of time. For instance, by first inventorying and discussing the apps users have on their mobile phone, then analyzing the privacy and security issues of these apps, and discussing them in a second round with the users.

A third limitation involves the types of apps used in this study. We selected two types of apps, as typical representatives of apps with a utilitarian or hedonic purpose. However, the privacy and security considerations of users might be totally different with other types of apps. It is imaginable that users privacy and security considerations are more important when, for instance, the app focuses explicitly on their health status, their social network, their geographical location, or their photos, videos and sound recordings. Future research could therefore focus on users' download behavior and considerations regarding different types of apps.

5.4. Conclusions

The main purpose of this study was to examine whether or not a given paradoxical behavior is still observable in users not disadvantaged by a lack of technical knowledge, privacy awareness, or financial means. We can indeed confirm, that despite the fact users still claim to be concerned about the potential misuse of their personal data, they remain unwilling to invest either the time and effort or the money necessary to protect their privacy. Despite their technical backgrounds and a higher than average understanding of privacy intrusion possibilities, participants were not willing to pay for their privacy. We highly question whether or not privacy as a concept is already implanted in users' perception and social representation. If not, this might explain the discrepancy between claims to highly value privacy and the behavior that indicates otherwise.

Acknowledgements

This work was supported by Nederlandse Organisatie voor Wetenschappelijk Onderzoek (grant number: 628.001.011) in collaboration with TNO, Wetenschappelijk Onderzoek- en Documentatiecentrum and Centric.

Appendix A. .

Table A.1

Table A.1
Selection of apps used for the experimental part of the study.

App	Amount of permissions	Permissions	Degree of intrusiveness
Utilitarian app (to-do-list)			
My ToDo List	0	–	not intrusive
ToDo list – Private Tasks	1	Photos/Media/Files	slightly intrusive
Tasks + To Do List Manager	2	Identity; Photos/Media/Files	somewhat intrusive
List & Notes	4	In-app purchases; Identity; Location; Photo/Media/Files	intrusive
EveryDay ToDo List Task List	5	Identity; contacts, location, photos/media/files; camera	very intrusive
Hedonic app (game)			
Mellow Meadows Tower Defense	0	–	not intrusive
New Eskimo Defense	2	Photos/media/files; device ID & call information	slightly intrusive
Astroid Defense Classic	4	Location; photo/media/files; WIFI connection information; Device ID & call information	somewhat intrusive
Safe the cave: Tower Defense	6	In-app purchases; photos/media/files; microphone; camera; WIFI connection information; Device ID & call information	intrusive
Tower Defense: Infinite War	7	In-app purchases; identity; contacts; phone; photos/media/file; WIFI connection information; Device ID & call information	very intrusive

Appendix B. . Questionnaires

Background information (Questionnaire 1)

1. What is your age?
2. What is your gender? (1) *male (2) female*
3. Which study program do you follow?
4. How long have you owned a smartphone:
5. On a daily basis, the average time I spent using mobile apps is:
6. On average, the number of mobile apps I use on a weekly basis is:
7. Which operating system do you use on your mobile phone? *(1) Android (2) IOS (3) other*
8. Where do you usually look for applications?
9. Was your mobile phone ever lost or stolen? *(1) never (2) once (3) twice (4) more than twice*
10. Do you sometimes lend your mobile phone to others? *(1) yes (2) yes but only for a while and if I am present (3) never*
11. How many apps have you ever installed **yourself** on your mobile phone? (such as Facebook app, games, ringtones, GPS etc.). Please give an indication: *(from* Yang, 2013*)*
12. Which categories of apps do you use? *(from Google App Store)*

Technical knowledge (Questionnaire 1)
from Androulidakis and Kandus (2011) and Kraus et al. (2014)

1. Do you know where you can find your mobile phone's IMEI (International Mobile station Equipment Identity)? *(1) yes (2) no (3) I don't know what it is*
2. After (re)starting your mobile phone, do you have to enter a PIN for unlocking your SIM card? *(1) Yes (2) no (3) I don't know*
3. Do you use a PIN code or password to unlock your screen-saver? *(1) Yes (2) no (3) doesn't have such feature (4) I don't know*
4. Do you use the Bluetooth function? *(1) yes, switched on and visible (2) yes, switched on and* ***in****visible (3) yes, but only for a specific purpose (4) no, switched off (5) I don't know*
5. Do you run a antivirus app on your mobile phone? *(1) Yes (2) no (3) I don't know*
6. Do you run a static analysis app on your mobile phone, for instance to monitor malicious code patterns, to inspect control flow between apps, or to review requested permissions? *(1) yes (2) no (3) I don't know*

7. Do you store passwords in your mobile phone (e.g. credit card password, ATM password)? *(1) yes, encrypted (2) yes, without encryption (3) no (4) I don't know*
8. Do you create backup copies of your phone's data? *(1) yes (2) no (3) I don't know*
   If yes:
   How often do you create backup copies of your phone's data? *open question*
9. Do you store sensitive personal data in your mobile phone (e.g. photos, videos, audio recordings)
   (1) yes (2) no (3) I don't know

   Scale 1–7: *(1) completely disagree to (7) completely agree*

10. Communication through mobile phones is safe.
11. I am aware about how the technical characteristics of my mobile phone affect its security.
12. I know how to protect myself against data misuse while surfing in a public network.
13. I know how my mobile phone can be protected from malicious apps.

Download considerations (Questionnaire 1 and 2)

1. Which aspects do you consider when searching for an app? *(1)completely disagree to (7) completely agree*
   (1) trustworthiness of the app (2) prior experience with the app (3) ratings (4) reviews (5) amount of downloads (6) privacy conditions (e.g. information disclosure) (7) security conditions (e.g. data protection) (8) amount of permissions requested (9) clarity of permissions requested (10) readability of permissions requested (11) if permissions are related to functionality (12) usefulness of the app (13) functionality of the app (14) design of the app (15) recommendation (e.g. from your social group) (16) price of the app (17) familiarity with the app (18) other:

Privacy awareness I: General privacy sensitivity (Questionnaire 1)
Westin Privacy Index – *see* Kumaraguru and Cranor, 2005
Scale 1–4: *(1) strongly disagree to (4) strongly agree*

1. Consumers lost all control over how personal information is collected and used by companies.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Downloading an app

Experimental part
Process of choosing, downloading and installing the app (Questionnaire 2)

1. Which app have you downloaded and are you planning to use for the review?
2. Please describe as extensive as possible the decision making process you followed while (1) choosing for an app, (2) downloading this app and (3) eventually installing this app.
3. Why have you chosen for this app and not for another app?
4. Which aspects of the app did determine your choice for downloading and installing this app? *See point 'download considerations'*

Writing an app review

1. Which app have you downloaded and will you use for the review?
2. Where did you get the app from? *(1) Apple App Store (2) Android Play Store (3) Amazon Marketplace (4) Other*
3. Did you pay for the app? *(1) yes (2) no*

   If yes: How much did you pay the app? *(1) 1,55 Euro (2) 0,96 Euro (3) 2,99 Euro (4) 1,46 Euro*

4. How often did you use the app during the last days? Please give an indication of the total length of time *in hours*:
5. How satisfied are you with the app? Please give an indication on a scale going from 1 to 10
   (1 = not satisfied at all to 10 = completely satisfied)
6. Please write a comprehensive review about the app you have downloaded and used during the last week. Please feel free to consider all factors you want to discuss about the app (e.g. in terms of usability, design, functionality etc.) *Open question*

Privacy awareness II: Information privacy concerns (Questionnaire 3)
MUIPC, from Xu et al. (2012)
Scale 1–7: *(1) completely disagree to (7) completely agree*
Perceived surveillance

1. I am concerned that mobile apps are collecting too much information about me.
2. I am concerned that mobile apps may monitor my activities on my mobile device.

Perceived intrusion

3. I feel that as a result of my using mobile apps, others know about me more that I am comfortable with.
4. I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
5. I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.

Secondary use of personal information

6. I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
7. When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
8. I am concerned that mobile apps may share my personal information with other entities without getting my authorization.

References

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In: EC '04 Proceedings of the 5th ACM Conference on Electronic, pp. 21–29.

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347 (6221), 509–514.

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Privacy 3 (1), 26–33.

Acquisti, A., Taylor, C.R., Wagman, L., 2016. The economics of privacy. J. Econ. Lit. 52 (2), 442–492.

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., Lentz, M., 2014. Brave new world: Privacy risks for mobile users. SPME, 2014, Maui, Hawaii, USA, 7-11.

Androulidakis, I., Kandus, G., 2011. Mobile phone security awareness and practices of students in Budapest. In: The Sixth International Conference on Digital Telecommunications, pp. 18–24.

Baek, Y.M., 2014. Solving the privacy paradox: a counter-argument experimental approach. Comput. Hum. Behav. 38, 33–42.

Barnes, S.B., 2006. A privacy paradox: social networking in the United States. Retrieved from. First Monday 11 (9). http://firstmonday.org/article/view/1394/1312.

Barth, S., De Jong, M.D.T., 2017. The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telemat. Inf. 34, 1038–1058.

Benenson, Z., Kroll-Peters, O., Krupp, M., 2012. Attitudes to IT security when using a smartphone. In: Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 1179–1183.

Benton, K., Jean Camp, L., Garg, V., 2013. Studying the effectiveness of Android application permissions requests. San Diego, USA In: Fifth International Workshop on SECurity and SOCial Networking, pp. 291–296.

Bergström, A., 2015. Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. Comput. Hum. Behav. 53, 419–426.

Buck, C., Horbel, C., Kessler, T., Germelmann, C.C., 2014. Mobile consumer apps: Big data brother is watching you. Market. Rev. St. Gallen 26–34.

Chia, P.H., Yamamoto, Y., Asokan, N., 2012. Is this app safe? A large scale study on application permissions and risk signals. In: Proceedings of the 21st International Conference on World Wide Web 2012, pp. 311–320.

Chin, E., Felt, A.P., Sekar, V., Wagner, D., 2012. Measuring user confidence in smartphone security and privacy. In: Symposium on Usable Privacy and Security. ACM, pp. 1–16.

Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart. 13 (3), 319–340.

Debatin, B., Lovejoy, J.P., Horn, A.-K., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput. Mediated Commun. 15, 83–108.

Dehling, T., Gao, F., Schneider, S., Sunyaev, A., 2015. Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and Android. JMIR Mhealth Uhealth 3 (1).

Deuker, A., 2010. Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. In: Bezzi, M., Duquenoy, P., Fischer-Hüber, S., Hansen, M., Zhang, G. (Eds.), Privacy and Identity Management for Life. Springer-Verlag, Berlin, Heidelberg, pp. 275–283.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.

Egele, M., Kruegel, C., Kirda, E., Vigna, G., 2011. PiOS: detecting privacy leaks in iOS applications. San Diego, California In: Proceedings of the 18th Annual Network and Distributed System Security Symposium 2011, pp. 77–183.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L.P., Jung, J., McDaniel, P., Sheth, A.N., 2014. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In: 9th USENIX Symposium on Operating System Design and Implementation, pp. 1–15.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., 2012. Android permissions: user attention, comprehension, and behavior. Symposium on Usable Privacy and Security (SOUPS), July, 11–13, 2012. Washington DC USA.

Flender, C., Müller, G., 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Busemeyer, J., Dubois, F., Lambert-Mogiliansky, A., Melucci, M. (Eds.), Quantum interaction Lecture notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, pp. 148–159.

Guo, X., Sun, Y., Yan, Z., Wang, N., 2012. Privacy-personalization paradox in adoption of mobile health service: The mediating role of trust. PACIS 2012 Proceedings, Paper 27.

Hazarika, B., Khuntia, J., Parthasarathy, M., Karimi, J., 2016. Do hedonic and utilitarian apps differ in consumer appeal? In: Sugumaran, V., Yoon, V., Shaw, M. (Eds.), E-Life: Web-Enabled Convergence of Commerce, Work, and Social Life. WEB 2015. Lecture Notes in Business Information Processing. vol. 258 Springer, Cham.

Heinonen, K., Pura, M., 2006. Classifying Mobile Services. In: Proceedings of Helsinki Mobility Roundtable. Sprouts: Working Papers on Information Systems, pp. 42.

Hoffman, C.P., Lutz, C., Ranzini, G., 2016. Privacy cynicism: a new approach to the privacy paradox. Cyberpsychology: J. Psy. Res. Cybersp. 10 (4) article 7.

Hu, Q., Ma, S., 2010. Does privacy still matter in the era of Web 2.0? A qualitative study of user behavior towards online social networking activities. Taipei, Taiwan In: Proceedings of Pacific Asia Conference on Information Systems (PACIS 2010), pp. 591–602.

Hughes-Roberts, T., 2013. Privacy and social networks: is concern a valid indicator of intention and behaviour? Washington, D.C., USA In: International Conference on Social Computing, pp. 909–912.

Joinson, A.N., Reips, U.-D., Buchanan, T., Paine Schofield, C.B., 2010. Privacy, trust, and self- disclosure online. Hum.-Comp. Int. 25, 1–24.

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25 (6), 607–635.

Kelley, P.G., Cranor, L.F., Sadeh, N., 2013. Privacy as part of the app decision-making process. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3393–3402.
Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134.
Krämer, N.C., Haferkamp, N., 2011. Online self-presentation: balancing privacy concerns and impression construction on social networking sites. In: Trepte, S., Reinecke, L. (Eds.), Privacy Online. Springer-Verlag, Berlin, Heidelberg, pp. 127–141.
Kraus, L., Wechsung, I., Möller, S., 2014. A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. Workshop on Privacy Personas and Segmentation.
Kumaraguru, P., Cranor, L.F., 2005. Privacy Indexes: A Survey of Westin's Studies (Report No. CMU-ISRI-5-138). Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.
Liccardi, I., Pato, J., Weitzner, D.J., Abelson, H., De Roure, D., 2014. No technical understanding required: Helping users make informed choices about access to their personal data. MOBIQUITOUS, 2014, London, Great Britain, 140-150.
Morosan, C., DeFranco, A., 2015. Disclosing personal information via hotel apps: a privacy calculus perspective. Int. J. Hosp. Manage. 47, 120–130.
Motiwalla, L.F., Li, X., Liu, X., 2014. Privacy paradox: does stated privacy concerns translate into the valuation of personal information? Proceeding of the 19th Pacific Asia Conference on Information Systems (PACIS 2014). Paper 281.
Oetzel, M.C., Gonja, T., 2011. The online privacy paradox: a social representations perspective. Vancouver, BC, Canada In: Paper presented at the Proceedings of the 2011 Annual Conference Extended Abstracts on Human factors in Computing Systems, pp. 2107–2112.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring privacy paradox in information- sensitive mobile app adoption: a cross-cultural comparison. Comput. Hum. Behav. 65, 409–419.
Poikela, M., Schmidt, R., Wechsung, I., Mueller, S., 2015. FlashPolling privacy: the discrepancy of intention and action in location-based poll participation. In: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers, pp. 813–818 Osaka, Japan.
Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H., 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. Chi, 2014, Toronto, ON, Canada, 2347-2356.
Spiekermann, S., Acquisti, A., Böhme, R., Hui, K.-L., 2015. The challenges of personal data markets and privacy. Electron. Markets 25, 161–167.
Statista, 2019. Number of mobile phone users worldwide from 2015 to 2020 (in billions). Retrieved via https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users- worldwide/.
Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: do cognitive heuristics hold the key? In: Proceedings of CHI'13 Extended Abstracts on Human Factors in Computing Systems, pp. 811–816 France.
Sutanto, J., Palme, E., Tan, C.-H., Phang, C.W., 2013. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quart. 37 (4), 1141–1164.
Tan, F.T.C., Vasa, R., 2011. Toward a social media usage policy. Proc. CECIIS 309–316.
Taylor, H., 2003. Most People are "Privacy Pragmatists" Who, While Concerned about Privacy, will Sometimes Trade it off for Other Benefits. The Harris Poll, pp. 44.
Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H., 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. Chi, 2014, Toronto, ON, Canada, 2347-2356.
Vasa, R., Hoon, L., Mouzakis, K., Noguchi, A. 2012. A preliminary analysis of mobile app user reviews. OZCHI'12, Melbourne, Victoria, Australia, 241-244.
Volkamer, M., Renaud, K., Kulyk, O., Emeröz, S., 2015. A socio-technical investigation in smartphone security. Vienna, Austria, 21- 22 Sep 2015 In: 11th International Workshop (STM 2015), pp. 265–273.
Wakefield, R.L., Whitten, D., 2006. Mobile computing: a user study on hedonic/utilitarian mobile device usage. Eur. J. Inf. Syst. 15 (3), 292–300.
Wang, T., Duong, T.D., Chen, C.C., 2016. Intention to disclose personal information via mobile applications: a privacy calculus perspective. Int. J. Inform. Manage. 36, 531–542.
Westin, A.F., 2003. Social and political dimensions of privacy. J. Soc. Issues 59 (2), 1–37.
Williams, M., Nurse, J.R.C., Creese, S., 2017. "Privacy is the boring bit": user perceptions and behaviour in the Internet-of-Things. Proceedings of the 15th International Conference on Privacy. Security and Trust.
Wilson, D.W., Valacich, J.S., 2012. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. Orlando, Florida In: Thirty Third International Conference on Information Systems, pp. 1–11.
Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M., 2012. Measuring mobile users' concerns for information privacy. In: Thirty Third International Conference on Information Systems, Orlando, pp. 1–16.
Yang, H., 2013. Bon appétit for apps: Young American consumers' acceptance of mobile applications. J. Comput. Inform. Syst. 53, 85–95.
Young, A.L., Quan-Haase, A., 2013. Privacy protection strategies on Facebook. Inf. Commun. Soc. 16 (4), 479–500.
Zafeiropoulou, A.M., Millard, D.E., Webber, C., O'Hara, K., 2013. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decision? New Your, USA In: WebSci '13 Proceeding of the 5th Annual ACM Web Science Conference, pp. 463–472.