International Journal of Information Management 50 (2020) 261–272

Contents lists available at ScienceDirect

International Journal of Information Management

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

Mobile users' information privacy concerns and the role of app permission requests

Kenan Degirmenci

School of Information Systems, Queensland University of Technology, 2 George Street, Brisbane QLD 4000, Australia

ARTICLE INFO

Keywords:
Mobile users
App permission requests
Information privacy concerns
Online survey
Structural equation modeling

ABSTRACT

Recent privacy-related incidents of mobile services have shown that app stores and providers face the challenge of mobile users' information privacy concerns, which can prevent users from installing mobile apps or induce them to uninstall an app. In this paper, we investigate the role of app permission requests and compare the impact on privacy concerns with other antecedents of information privacy concerns, i.e., prior privacy experience, computer anxiety, and perceived control. To test these effects empirically, we conducted an online survey with 775 participants. Results of our structural equation modeling show that prior privacy experience, computer anxiety, and perceived control have significant effects on privacy concerns. However, concerns for app permission requests have approximately twice as much predictive value than the other factors put together to explain mobile users' overall information privacy concerns. We expect that our findings can provide a theoretical contribution for future mobile privacy research as well as practical implications for app stores and providers.

1. Introduction

Once again, information privacy concerns have been in the main focus of the most recent Facebook privacy scandal, where 14 million users have unknowingly posted private information to the public due to a software bug (Kuchler, 2018). Earlier this year, Facebook was under investigation due to the use of its data by political consulting firm Cambridge Analytica, which collected personal information of approximately 87 million Facebook users without their explicit consent to access their data (Hern, 2018). Social networking services other than Facebook have also been at the heart of information privacy concerns. For example, a few years ago, the social networking app Path had collected personal information from mobile users' address books without their knowledge and consent (Federal Trade Commission, 2013). Such privacy-related incidents that mobile users may experience are one of a few reasons for them to abandon the use of mobile apps. In a survey of 714 mobile app users, the Pew Research Center found that 54 percent of the respondents had decided not to install and 30 percent had decided to uninstall mobile apps due to privacy concerns about their personal information (Boyles, Smith, & Madden, 2012). Although the access to personal information can be advantageous for mobile users, for example, the access to location is used for navigation purposes by some apps, it also evokes privacy concerns with the result that users delete apps from their devices (eMarketer, 2016). For app providers, it is therefore important to understand and alleviate mobile users' concerns for their information privacy.

From an economic perspective, mobile app revenues are expected to grow from $69.7 billion in 2015 to $188.9 billion in 2020, with $71.7 billion from app stores and $117.2 billion from in-app advertising (App Annie, 2016). In information systems (IS) research, information privacy concerns has been a topic of wide interest in the context of the use of mobile applications (Gu, Xu, Xu, Zhang, & Ling, 2017; Jung & Park, 2018; Junglas, Johnson, & Spitzmüller, 2008; Sutanto, Palme, Tan, & Phang, 2013; Wang, Duong, & Chen, 2016; Wottrich, van Reijmersdal, & Smit, 2018; Xu, Teo, Tan, & Agarwal, 2009; Xu, Teo, Tan, & Agarwal, 2012), in which, for example, app popularity, privacy seals, or location-based services have been in the focus of mobile privacy research; however, app permission requests have played an underrated role so far. Recent studies have examined the impact of the sensitivity and justification of app permission requests on privacy concerns (Gu et al., 2017), or desensitization to permission requests and the influence on the perceived risk of installing an app (Harris, Brookshire, & Chin, 2016). While sensitivity and justification provide insights into an evaluation of low-risk vs. high-risk permissions and the effects of presenting information why permissions are being requested, desensitization refers to users who have allegedly become desensitized to excessive permissions. While these studies focus on distinct characteristics of app permissions including sensitivity, justification, and desensitization, we extend the literature by analyzing mobile users' concerns for app permission requests per se and the impact on their overall information

E-mail address: kenan.degirmenci@qut.edu.au.

https://doi.org/10.1016/j.ijinfomgt.2019.05.010
Received 9 August 2018; Received in revised form 5 April 2019; Accepted 14 May 2019
Available online 02 July 2019
0268-4012/ © 2019 Elsevier Ltd. All rights reserved.

privacy concerns. To that end, we expect that our results will provide implications, which will be relevant to app stores and providers regarding decision-making of implementing app permissions, such that privacy concerns can be further mitigated. As an initial step, our survey-based data analysis reveals a problem with existing designs of permission requests, which refers to app permission concerns and offers implications for practice and directions for future research. Based on the findings of our study, we anticipate that the design of app permission requests will require a change due to mobile users' growing privacy concerns, which we discuss more in-depth in Sections 6.3 and 7.2.

The purpose of this paper is to investigate the role of app permission requests regarding mobile users' concerns for information privacy. To address this gap, we draw on the construct of mobile users' information privacy concerns (MUIPC) (Xu, Gupta, Rosson, & Carroll, 2012) to measure users' privacy concerns in a mobile context, and we situate our research within the framework of the overarching macro model labeled "Antecedents–Privacy Concerns–Outcomes" (APCO) (Dinev, McConnell, & Smith, 2015; Smith, Dinev, & Xu, 2011), of which we focus on the antecedents of prior privacy experience (Smith, Milberg, & Burke, 1996), computer anxiety (Stewart & Segars, 2002), and perceived control (Xu, Gupta et al., 2012). In our mobile user context, we add app permission concerns as an antecedent of MUIPC and propose the following research question: *What impact do app permission concerns have on mobile users' overall information privacy concerns compared to the privacy-related antecedents prior privacy experience, computer anxiety, and perceived control?* The paper is structured as follows: First, a theoretical foundation of the MUIPC construct and antecedents of information privacy concerns is presented, followed by our research model and hypothesis generation. Then, we describe the research design and show results from our survey-based data analysis. Following the discussion of our findings, we provide a contribution to theory and implications for practice. Finally, we conclude with limitations and future research directions.

2. Theoretical foundation

2.1. Mobile users' information privacy concerns

The MUIPC construct was first introduced by Xu, Gupta et al. (2012), which is based on the scale of concern for information privacy (CFIP) (Smith et al., 1996) and Internet users' information privacy concerns (IUIPC) (Malhotra, Kim, & Agarwal, 2004). The CFIP scale measures "individuals' concerns about organizational information privacy practices" with four subscales: *collection*, *errors*, *improper access*, and *unauthorized secondary use* (Smith et al., 1996, p. 169). *Collection* describes individuals' perception that "great quantities of data regarding their personalities, background, and actions are being accumulated" (Smith et al., 1996, p. 171). The collection of personal information enables companies to use this information about individuals in relationship marketing and to target offers more accurately to individuals' interests (Culnan & Armstrong, 1999). Due to *errors* and *improper access*, individuals become concerned that companies should take more measures to reduce errors and control access to personal information (Smith et al., 1996). With regard to companies' potential opportunistic behaviors (Laufer & Wolfe, 1977), *unauthorized secondary use* refers to the selling or sharing of a person's information without their authorization (Smith et al., 1996). Referring to Malhotra et al. (2004), IUIPC serves as a "tool for analyzing online consumers' privacy concerns and reactions to various privacy threats on the Internet" (p. 348), which draws on the social contract and justice theories, identifying three dimensions of privacy concerns: *collection of personal information* (distributive justice), *control over personal information* (procedural justice), and *awareness of organizational information privacy practices* (interactional and informational justice).

Building on these privacy-related constructs, MUIPC draws on the communication privacy management theory and relates to information privacy concerns in a mobile user context, which is divided into three dimensions to measure mobile users' concerns: *perceived surveillance*, *perceived intrusion*, and *secondary use of personal information*. *Perceived surveillance* describes the tracking and profiling of mobile users through mobile technology capabilities (Xu, Gupta et al., 2012), which are equipped with environment sensors such as built-in cameras, proximity sensors, accelerometers, gyroscopes, and global positioning system (GPS) receivers (Enck, 2011; Lienhard & Legner, 2015). In a taxonomy of privacy, Solove (2006, p. 490) defines surveillance as "the watching, listening to, or recording of an individual's activities". The sensors in mobile devices allow diverse possibilities regarding users' environment, movement, orientation, and location, and thus, they enable to enhance mobile users' tasks; however, at the same time, the sensors may evoke privacy risks and can lead to information disclosure (Keith, Babb, Lowry, Furner, & Abdullat, 2015; Zhang, Adipat, & Mowafi, 2009), which is closely related to an *intrusion* of mobile users' privacy. Solove (2006, p. 549) defines intrusion as "invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy". For example, Google Maps or Apple Maps request access to the location of mobile users and as a result, users' location is exposed. While this function is fundamental for the functionality of the navigation system of these apps, access is requested unnecessarily in a number of cases by other apps (Enck, 2011), leading to privacy intrusion and malicious use of personal information such as secondary use. *Secondary use of personal information*, which is also a dimension of CFIP, is defined as "the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent" (Solove, 2006, p. 519). The collection of personal information enables companies to use the information for marketing purposes, for example, in order to target offers more accurately to individuals' interests (Culnan & Armstrong, 1999; Wang et al., 2016). Secondary use is described as an asymmetry of knowledge, because individuals are exposed to the uncertainty that they are likely to know little or nothing about the circumstances under which their personal information is captured, sold, or processed, which creates "a sense of powerlessness and vulnerability" (Solove, 2006, p. 520). One prominent example of secondary use of personal information is the recent Facebook privacy scandal, where approximately 87 million Facebook users' data were collected by political consulting firm Cambridge Analytica without the users' explicit consent to access their data (Hern, 2018). As a consequence, user growth on Facebook declined, for example, 3 million users in Europe abandoned Facebook, and Facebook shares decreased by 19%, which equaled a decline of $119 billion (Neate, 2018).

We choose the MUIPC construct as the focal variable of our study because our main interest are app permission requests and thus we focus on users in the mobile environment. Xu, Gupta et al. (2012, p. 13) arguably propose that "consumers' concerns for information privacy are not only different but more aggravated in the mobile environment". To that end, MUIPC is considered to be more suitable and a better-targeted instrument to address privacy concerns of mobile users (Keith, Babb, & Lowry, 2014; Lom, Thoo, Sulaiman, & Adam, 2018). The MUIPC instrument has been used in various studies. For example, Chen and Li (2017) conducted a survey with 284 mobile users and found that MUIPC has a significant impact on the intention to adopt security defensive software. Keith et al. (2014) designed a social geo-caching game, which they used for a field experiment with 568 participants to examine longitudinal behavior of actual information disclosure using the MUIPC instrument. Further studies use MUIPC to analyze the effects of privacy concerns on the sensitivity of mobile fitness data (Vitak, Liao, Kumar, Zimmer, & Kritikos, 2018), or address the moderating role of MUIPC in a mobile advertising context (Lom et al., 2018) and regarding the effect of app value as a privacy trade-off for mobile app downloads (Wottrich et al., 2018). The MUIPC instrument has also been used very recently in a study by Belanger and Crossler (2019), in which protective behaviors on mobile devices are in the focus of their analysis.

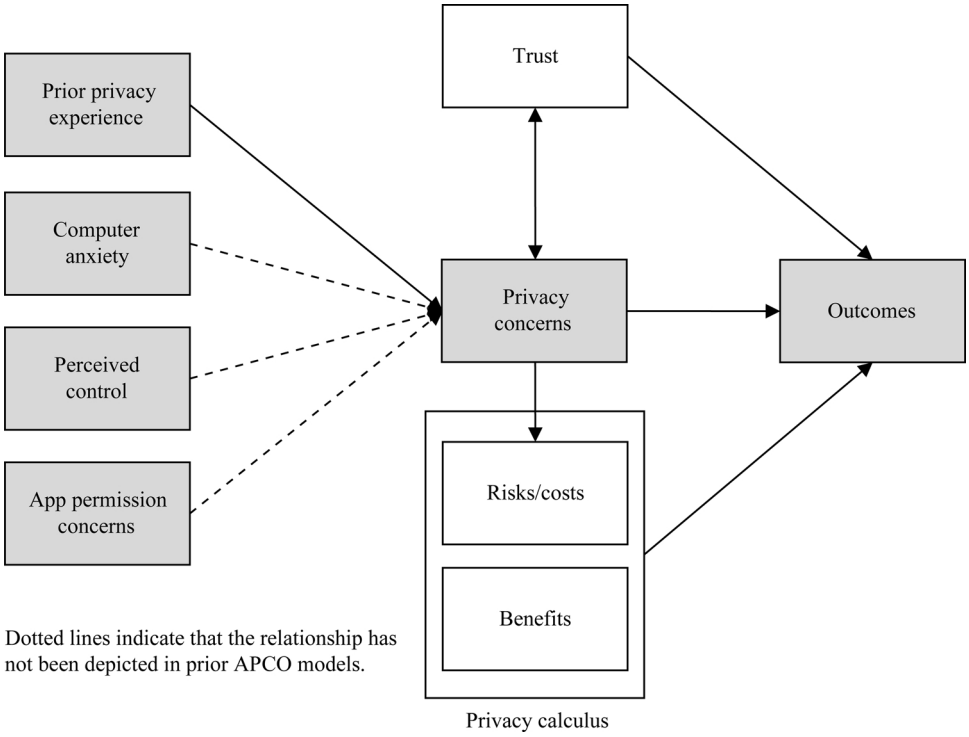


Fig. 1. APCO model in a mobile context and research focus of the study (shaded in gray).

2.2. Antecedents of information privacy concerns

Since our aim is to investigate the influence of app permission concerns on mobile users' information privacy concerns, we draw on the APCO model, which provides positivist privacy researchers with an overarching macro model that summarizes relationships of antecedents and outcomes of privacy concerns (Dinev et al., 2015; Smith et al., 2011). The APCO model is considered to be subject to a continuous process of optimization including "an expanded set of antecedents as well as an exhaustive set of outcomes," whereby the "ultimate objective should be a macro model that will prove useful across disciplines and contexts" (Smith et al., 2011, p. 1008). Following this recommendation, we present an APCO model in a mobile context in Fig. 1 with a focus on antecedents including prior privacy experience, computer anxiety, and perceived control, as well as app permission concerns as an antecedent of privacy concerns as the main focus of our study.

The APCO model suggests that privacy-related antecedents usually involve individual traits or contextual factors (Dinev et al., 2015). Individual traits refer to personality differences such as introversion versus extroversion or independent-self versus interdependent-self, whereas contextual factors describe the specific context that the factors depend on such as the industry to which an organization belongs or different types of information with different levels of sensitivity (Smith et al., 2011). In our study, we focus on individual traits, of which our main focus are app permission concerns. We suggest that other relevant individual factors for mobile users' privacy concerns regard prior privacy experience (privacy issues with mobile apps), computer anxiety (continuing automation through the ubiquity of mobile devices), and perceived control (privacy settings to control information retrieval through mobile apps). Due to the focus of our study, we view the APCO model from a mobile perspective and note that while prior privacy experience has been depicted in prior APCO models (Dinev et al., 2015; Smith et al., 2011), we integrate computer anxiety, perceived control, and app permission concerns as new relationships; whereby, computer anxiety and perceived control have been established in prior studies (Stewart & Segars, 2002; Xu, Gupta et al., 2012). In order to enable a comparison of app permission concerns with other relevant antecedents of privacy concerns, we refer to prior privacy experience, computer anxiety, and perceived control, which have been suggested to be important predictors in the information privacy literature (Dinev et al., 2015; Smith et al., 2011, 1996; Stewart & Segars, 2002; Xu, Gupta et al., 2012).

With regard to prior privacy experience, Smith et al. (1996, p. 186) describe that "individuals who had been exposed to, or been the victim of, personal information misuses should have stronger concerns regarding information privacy". In this regard, a distinction is made between personal experiences and indirect experiences, e.g., in the form of media messages about online privacy risks, which can be as effective as direct experiences because such messages may contain self-relevant information that exposes individuals' personal privacy risks in online environments (Cho, Lee, & Chung, 2010; Smith et al., 1996; Xu, Gupta et al., 2012). Computer anxiety is defined as "the tendency of individuals to be uneasy, apprehensive, or fearful about current or future use of computers" (Stewart & Segars, 2002, p. 44). Further, Thatcher and Perrewé (2002, p. 384) relate computer anxiety to "fears about the implications of computer use such as the loss of important data or fear of other possible mistakes". Such loss of important data can entail personal information that is tracked by using mobile applications, which may motivate mobile users "to avoid potential harm arising from ambiguous threat" (Yin, Bond, & Zhang, 2014, p. 542). In our context, mobile users could avoid potential harm by not accepting app permissions that require to access personal information such as mobile users' location, contacts, and other privacy-related data. The third antecedent, perceived control, refers to "perceived control over personal information as an individual's belief about the presence of factors that may increase or decrease the amount of control over the release and dissemination of personal information" (Xu, Gupta et al., 2012, p. 1346). Such factors may refer to consumers' choices about the amount of information collected, e.g., through opt-in and opt-out options (Caudill & Murphy, 2000). For example, in the context of location-based services, users are given the choice to turn off the location tracking from their mobile devices, and thus, opt out from having their personal information transmitted to the service provider. Finally, we add app permission concerns as a new antecedent, which we argue is becoming more and

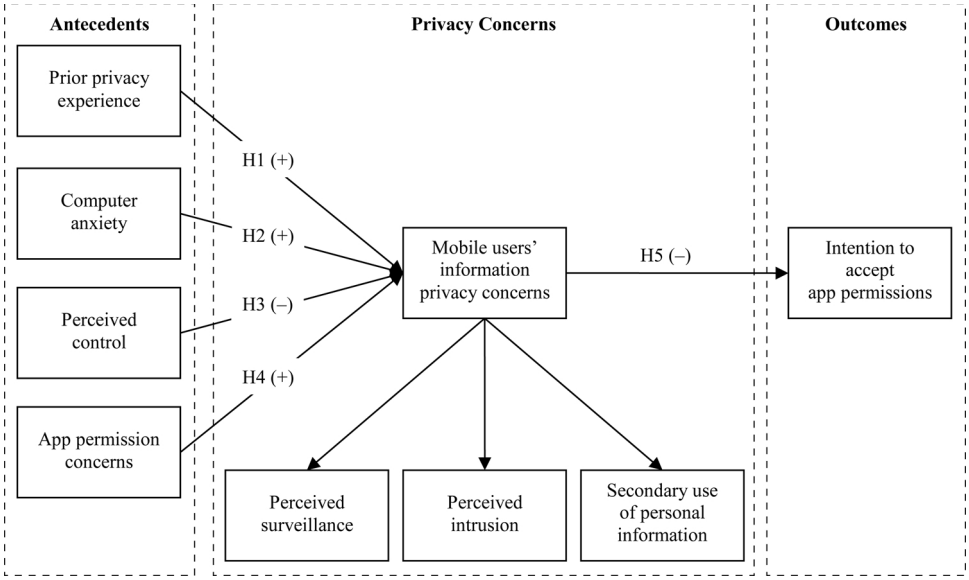


Fig. 2. APCO model of mobile users' information privacy concerns (MUIPC).

more important for information privacy concerns regarding the rapid growth of mobile apps and, subsequently, increasingly excessive app permissions. The justification for this addition will be provided in the next section, where we develop our hypotheses related to mobile users' information privacy concerns.

3. Research model and hypothesis generation

Based on the APCO model, we present our research model in Fig. 2, which includes antecedents of information privacy concerns, i.e., prior privacy experience, computer anxiety, perceived control, and app permission concerns, which we propose as an additional antecedent in a mobile user context. Privacy concerns are implemented in the model in the form of mobile users' information privacy concerns (MUIPC), which are formed by the dimensions of *perceived surveillance*, *perceived intrusion*, and *secondary use of personal information*. Finally, outcomes of privacy concerns are depicted through the intention to accept app permissions.

Considering the mobile context, MUIPC is in the heart of our research model, with prior privacy experience, computer anxiety, perceived control, and app permission concerns as its predictors. Prior privacy experience has been found to be a predictor of information privacy concerns in previous studies (Smith et al., 1996; Xu, Gupta et al., 2012; Xu, Gupta et al., 2012), and we expect that mobile users will have similar experiences with privacy-related issues, as recently supported by a study on mobile privacy concerns by Belanger and Crossler (2019). As such, mobile users will have stronger concerns regarding information privacy once their personal information has been misused in the past or they have heard or read about the use and potential misuse of the information collected from the Internet or through mobile applications. In such cases, mobile users perceive being a victim of personal information misuse, such as in the Facebook/Cambridge Analytica case described earlier, which leads to an increase of information privacy concerns (Borena, Belanger, Ejigu, & Anteneh, 2015; Zlatolas, Welzer, Heričko, & Hölbl, 2015). Thus, we propose the following hypothesis:

H1. Prior privacy experience positively influences mobile users' information privacy concerns.

As previous studies have shown the impact of computer anxiety on information privacy concerns (Osatuyi, 2015; Stewart & Segars, 2002), we further anticipate that MUIPC will be influenced by computer anxiety. The construct of computer anxiety suggests that it is formed in response to perceived threats from a technology, which leads individuals to experience tension when exposed to computers (Brown, Fuller, & Vician, 2004; Kummer, Recker, & Bick, 2017). Since computer anxiety refers to the loss of important data or fear of other possible mistakes (Thatcher & Perrewé, 2002), we reason that mobile users' computer anxiety will significantly affect their privacy concerns due to the high degree of sensitive data such as location information, contacts, photos, and other user-related data, which is transmitted through mobile devices. As computer anxiety increases, users may feel uncomfortable with excessive app permission requests and privacy concerns will increase. Therefore, we posit the following hypothesis:

H2. Computer anxiety positively influences mobile users' information privacy concerns.

With regard to perceived control, we propose that mobile users will have similar fears about a potential misuse of personal data, e.g., through mobile apps that request access to users' location, although the information is not required by the app. In this regard, app stores allow mobile users to control the amount of personal information. For example, Apple changed the privacy settings with the release of iOS 6, which gives mobile users a higher amount of control over their personal information. The change implied that mobile users can turn off access to contacts, calendars, reminders, photos, Bluetooth sharing, as well as access to Twitter and Facebook accounts. Before this change, users were only allowed to turn off access to location. Later versions of iOS allowed mobile users to control further categories such as opting out of access to the microphone and built-in camera of mobile devices. For Android 5 or lower, it was not possible to control individual app permissions. Google also gave users more control over permissions with the release of Android 6. App stores and providers more and more face the challenge of considering privacy concerns of their users and implement privacy assurance approaches to alleviate those concerns, of which opt-out mechanisms are one such approach. In IS research, perceived control has been found to influence information privacy concerns, for example, in a study by Xu, Teo et al. (2012) or in another study by Wang et al. (2016). Several studies suggest that low levels of perceived control heightens individuals' risk perceptions, which in turn reduces their capabilities to affect changes in the environment in a desired direction (Du, Keil, Mathiassen, Shen, & Tiwana, 2007; Lang, Wiesche, & Krcmar, 2018). In a mobile environment, this implicates that users will not feel empowered to control their personal information, when app providers

do not provide them with possibilities such as turning the location of an app on and off, which will result in growing privacy concerns for users (Lang et al., 2018; Xu, 2007; Xu, Gupta et al., 2012). Based on these lines of logic, we propose the following hypothesis:

H3. Perceived control negatively influences mobile users' information privacy concerns.

In addition to prior privacy experience, computer anxiety, and perceived control, we propose app permission concerns as an antecedent of MUIPC. In a recent study by Gu et al. (2017), two factors related to app permission requests have been found to have a significant impact on information privacy concerns: (1) permission sensitivity in terms of the risk level of app permission requests (for example, "access to the vibrator" as a low-risk permission request, and "access to location information" as a high-risk permission request), and (2) permission justification regarding how collected information is used (for example, the justification for "access to the vibrator" is to "remind users when there is a new announcement"). While permission sensitivity and justification relate to distinct characteristics and designated purposes of app permission requests, in our study we focus on app permission requests that relate to the growing collection of personal information through mobile apps per se, which can result in the excessive collection of data and lead to information privacy concerns. Excessive app permission requests that "go beyond the necessary function of the app" (Harris et al., 2016, p. 445) are considered to be less likely accepted by mobile users due to privacy concerns about their personal information (Chin, Harris, & Brookshire, 2018). For example, it has been reported that more than 100,000 apps in Google's Play Store collected mobile users' data that was not consistent with their stated functions such as unnecessary location tracking or excessive access to contact lists (Robertson, 2012). We integrate app permission concerns in our research model for two reasons: first, in order to measure the impact of app permission concerns on MUIPC regardless of whether mobile users perceive permission requests to be sensitive or justified; and second, in order to compare app permission concerns to other privacy-related antecedents, i.e., prior privacy experience, computer anxiety, and perceived control. We hypothesize that growing concerns for app permission requests will lead to an increase of users' overall discomfort about their privacy. Thus, we propose the following hypothesis:

H4. App permission concerns positively influence mobile users' information privacy concerns.

Finally, following Wottrich et al.'s (2018) recent findings, we expect that a higher degree of privacy concerns will lead to the outcome that requested app permissions will be less likely accepted. We further base the hypothesis of the effect of privacy concerns on intention on numerous other studies (for example, Gu et al., 2017; Osatuyi, 2015; Smith et al., 1996; Stewart & Segars, 2002; Xu, Gupta et al., 2012). It is suggested that "individuals with higher levels of concern about information privacy practices may be more likely in the future to refuse to participate in activities that require the provision of personal information" (Smith et al., 1996, p. 187). We reason that as privacy concerns increase, users will less likely intent to accept app permissions, which will eventually lead to a decline to install an app. Since app permission acceptance usually involves the provision of personal information, we present the following hypothesis:

H5. Mobile users' information privacy concerns negatively influence the intention to accept app permissions.

Since we are not actually measuring an action, we refer to one well-known theory, the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980), which explains that one's *intention to act* actually leads to an *action*. Numerous studies have demonstrated this relationship in prior research including several studies in an information privacy context (Belanger & Crossler, 2019; Keith, Thompson, Hale, & Greer, 2012; Lowry, Cao, & Everard, 2011; Pavlou, Liang, & Xue, 2007; Wang & Herrando, 2019). Hence, we presume that with increasing intentions, there will be a growth of users' actual acceptance of app permissions.

4. Research design and measurements

To test the proposed hypotheses, we designed an online survey and recruited participants from an online social networking website. Due to accessibility, we targeted participants from the United States. We offered incentives in the form of three $50 Amazon gift cards, and participation in the survey was completely voluntary. In survey methodology, it is common practice to offer incentives in exchange for survey participation (Xu, Gupta et al., 2012). We recruited participants by posting announcements, which provided background information about the study. To reduce bias possibility regarding self-selection among survey respondents, we did not disclose in the announcements that privacy concerns were the focus of our study. In the announcements, we asked participants to give their opinion about a mobile social networking app. The subjects could easily participate by using the URL provided in the posting. A total of 918 subjects participated, with 775 producing usable data. Of the 775 participants, 68.3% were female, 39.1% were below 20 years and 36.3% were between 21 and 30 years. Most of the participants were from Georgia (7.2%), Pennsylvania (6.1%), and Texas (4.8%), 59.6% were students and 25.3% were employed, and mainly used Android (31.5%) or iOS (66.8%). A complete list of participant profiles is provided in Appendix A.

For the operationalization of the latent variables of our research model, we measured the core constructs using reflective multiple-item scales, drawn from pre-validated measures where possible. For the antecedents, we measured *prior privacy experience* with items adapted from Xu, Gupta et al. (2012) using a 7-point rating scale, which ranged from "not at all" to "very often". *Computer anxiety* was measured with a 7-point Likert scale from "strongly disagree" to "strongly agree" adapted from Stewart and Segars (2002), and *perceived control* with a 7-point rating scale from "no control" to "full control" adapted from Xu, Teo et al. (2012). To measure *app permission concerns*, we used a 7-point Likert scale ranging from "strongly disagree" to "strongly agree", which we adapted from Smith et al. (1996) who originally used the scale in a context where companies collected personal information from individuals. Their items were adapted to our mobile user context, more specifically, to our context where mobile users are requested to accept or decline app permissions. In order to allow participants to make sense of app permissions being requested, we presented a scenario in which a hypothetical social networking app required access to various types of information, of which three most common app permissions were presented: location, contacts, and photos. The scenario is provided in Appendix B. For the MUIPC construct, we used 7-point Likert scales ranging from "strongly disagree" to "strongly agree" for the dimensions of *perceived surveillance* (adapted from Xu, Gupta et al., 2012), *perceived intrusion* (Xu, Dinev, Smith, & Hart, 2008), and *secondary use of personal information* (Smith et al., 1996). For the outcomes, we measured *intention to accept app permissions* using a 7-point semantic differential scale with items adapted from Malhotra et al. (2004), who originally used the scale in an Internet user context. The survey instrument is provided in Appendix C.

5. Data analysis and results

We conducted partial least squares structural equation modeling (PLS-SEM) with SmartPLS to analyze the collected data. All indicators were modeled as being reflective of their respective constructs. The measurement items loaded between 0.724 and 0.959 on their respective constructs, therefore exceeding the recommended threshold of 0.70 (Hair, Hult, Ringle, & Sarstedt, 2017) and the minimum criteria of 0.60 (Chin, 1998), thus demonstrating adequate indicator reliability and convergent validity. The internal consistency of the scales showed composite reliability (CR) ranging from 0.818 to 0.969, and Cronbach's

Table 1
Convergent validity of measurement model.

Construct	Items	Loadings	t-statistics	CR	Cronbach's α	AVE
Prior privacy experience (PPE)	PPE1	0.785	17.866	0.818	0.694	0.600
	PPE2	0.811	18.644			
	PPE3	0.724	13.656			
Computer anxiety (CA)	CA1	0.835	46.494	0.887	0.810	0.723
	CA2	0.897	86.509			
	CA3	0.818	41.369			
Perceived control (PC)	PC1	0.795	31.391	0.926	0.900	0.714
	PC2	0.868	61.064			
	PC3	0.854	53.178			
	PC4	0.816	37.583			
	PC5	0.888	80.825			
App permission concerns (APC)	APC1	0.901	82.439	0.942	0.907	0.843
	APC2	0.906	100.763			
	APC3	0.946	203.968			
Perceived surveillance (PS)	PS1	0.855	49.688	0.934	0.894	0.826
	PS2	0.929	140.343			
	PS3	0.941	191.321			
Perceived intrusion (PI)	PI1	0.944	159.090	0.965	0.946	0.902
	PI2	0.955	174.089			
	PI3	0.951	188.746			
Secondary use of personal information (SU)	SU1	0.955	144.912	0.969	0.952	0.913
	SU2	0.959	198.533			
	SU3	0.953	163.825			
Intention to accept app permissions (INT)	INT1	0.929	131.187	0.962	0.947	0.864
	INT2	0.949	195.591			
	INT3	0.946	142.892			
	INT4	0.893	97.125			

alpha ranging from 0.694 to 0.952, which were exceeding the recommended value for construct reliability of at least 0.60 (Hair et al., 2017), thus meeting criteria for internal consistency. Average variance extracted (AVE) ranged from 0.600 to 0.913, exceeding the recommended lower limit of 0.50 and thus indicating convergent validity (Fornell & Larcker, 1981). Table 1 provides an overview of the convergent validity of the measurement model.

For discriminant validity (Fornell & Larcker, 1981), we analyzed loadings and cross loadings of the measurement model (see Table 2). All items loaded higher on their constructs than any other constructs and the differences were greater than 0.117.

We further assessed discriminant validity in a latent variable correlation matrix (see Table 3). The square root of the AVE for each construct was larger than the correlation of the construct with any other constructs in the model, which demonstrated discriminant validity (Fornell & Larcker, 1981).

The correlation matrix also helped to determine if any of the correlations were above 0.90, which would indicate that common method bias (CMB) may exist (Pavlou et al., 2007). The observed correlations were below the 0.90 threshold (see Table 3). We further assessed CMB ex post through Harman's single-factor test. All items from the constructs were included in an unrotated exploratory factor analysis (EFA) to determine whether the majority of the variance could be ascribed to one general factor (Lowry & Gaskin, 2014; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Harman's single-factor test in this study produced 27 distinct factors, the largest of which explained only 37.24% of the variance of the model. Another ex post approach to examine CMB suggests to conduct a full collinearity test in order to ensure that all factor-level variance inflation factors (VIFs) are lower than 3.3, which is also an indication that a model can be considered free of CMB (Kock, 2015). While the common method factor technique is more common in covariance-based SEM (Lindell & Whitney, 2001), the full collinearity test is recommended for variance-based SEM (Kock & Lynn, 2012). To assess the structural model for collinearity issues, an examination of the

Table 2
Loadings and cross loadings of measures.

	PPE	CA	PC	APC	PS	PI	SU	INT
PPE1	**0.785**	0.201	–0.094	0.071	0.133	0.176	0.189	–0.083
PPE2	**0.811**	0.157	–0.149	0.154	0.253	0.242	0.277	–0.138
PPE3	**0.724**	0.217	–0.038	0.060	0.112	0.150	0.126	–0.093
CA1	0.241	**0.835**	–0.184	0.244	0.299	0.316	0.315	–0.147
CA2	0.180	**0.897**	–0.070	0.176	0.278	0.301	0.247	–0.157
CA3	0.171	**0.818**	–0.022	0.125	0.231	0.247	0.196	–0.138
PC1	–0.122	–0.096	**0.795**	–0.182	–0.149	–0.156	–0.185	0.147
PC2	–0.104	–0.102	**0.868**	–0.147	–0.142	–0.181	–0.217	0.141
PC3	–0.097	–0.097	**0.854**	–0.132	–0.140	–0.136	–0.172	0.132
PC4	–0.109	–0.110	**0.816**	–0.125	–0.124	–0.126	–0.167	0.126
PC5	–0.135	–0.096	**0.888**	–0.218	–0.203	–0.219	–0.239	0.202
APC1	0.114	0.189	–0.170	**0.901**	0.608	0.615	0.569	–0.465
APC2	0.133	0.210	–0.165	**0.906**	0.693	0.657	0.617	–0.466
APC3	0.129	0.206	–0.202	**0.946**	0.696	0.692	0.622	–0.555
PS1	0.210	0.247	–0.139	0.572	**0.855**	0.640	0.609	–0.332
PS2	0.206	0.300	–0.169	0.731	**0.929**	0.812	0.746	–0.479
PS3	0.226	0.323	–0.189	0.669	**0.941**	0.790	0.747	–0.445
PI1	0.261	0.326	–0.169	0.662	0.781	**0.944**	0.749	–0.516
PI2	0.228	0.300	–0.194	0.683	0.779	**0.955**	0.772	–0.501
PI3	0.241	0.352	–0.205	0.689	0.796	**0.951**	0.789	–0.511
SU1	0.259	0.300	–0.236	0.619	0.728	0.764	**0.955**	–0.426
SU2	0.274	0.301	–0.233	0.635	0.741	0.788	**0.959**	–0.438
SU3	0.255	0.270	–0.209	0.629	0.750	0.772	**0.953**	–0.427
INT1	–0.125	–0.182	0.214	–0.501	–0.443	–0.501	–0.428	**0.929**
INT2	–0.135	–0.177	0.163	–0.521	–0.445	–0.509	–0.421	**0.949**
INT3	–0.142	–0.152	0.160	–0.514	–0.441	–0.513	–0.419	**0.946**
INT4	–0.122	–0.133	0.135	–0.474	–0.397	–0.468	–0.408	**0.893**

Notes: PPE = Prior privacy experience, CA = Computer anxiety, PC = Perceived control, APC = App permission concerns, PS = Perceived surveillance, PI = Perceived intrusion, SU = Secondary use of personal information, INT = Intention to accept app permissions.

Table 3
Latent variable correlation matrix.

	PPE	CA	PC	APC	PS	PI	SU	INT
PPE	**0.775**							
CA	0.236	**0.850**						
PC	–0.136	–0.118	**0.845**					
APC	0.136	0.220	–0.195	**0.918**				
PS	0.235	0.321	–0.184	0.727	**0.909**			
PI	0.256	0.343	–0.200	0.714	0.827	**0.950**		
SU	0.275	0.304	–0.236	0.657	0.774	0.811	**0.956**	
INT	–0.141	–0.174	0.182	–0.541	–0.465	–0.536	–0.451	**0.930**

Notes: PPE = Prior privacy experience, CA = Computer anxiety, PC = Perceived control, APC = App permission concerns, PS = Perceived surveillance, PI = Perceived intrusion, SU = Secondary use of personal information, INT = Intention to accept app permissions; value on the diagonal (bold) is the square root of average variance extracted (AVE).

VIF values of the predictor constructs is considered to be an adequate approach (Hair et al., 2017). All VIFs of our model were lower than 1.377, further reducing concerns over CMB. The ex post controls suggested that the data did not suffer from CMB. To reduce CMB ex ante in the research design stage, the measures for the constructs were compiled from various sources (Chang, Van Witteloostuijn, & Eden, 2010). Furthermore, anonymity and confidentiality of the study were guaranteed in order to reduce the probability that respondents provided answers they believe were expected (Chang et al., 2010; Podsakoff et al., 2003).

Since the convergent and discriminant validity criteria for the measurement model were met and CMB was not likely to exist in our model, we proceeded with the path coefficient estimations of the PLS-SEM. As suggested by Xu, Gupta et al. (2012), we created a second-

Table 4
Path coefficients and effect sizes of the structural model.

Effect	Model 1 (without APC)			Model 2 (with APC)		
	R^2	*Path coefficient*	*Effect size (f^2)*	R^2	*Path coefficient*	*Effect size (f^2)*
Mobile users' information privacy concerns (MUIPC)	**0.185**			**0.617**		
Prior privacy experience (PPE)		0.185***	0.039		0.137***	0.044
Computer anxiety (CA)		0.283***	0.092		0.157***	0.057
Perceived control (PC)		–0.164***	0.032		–0.051*	0.005
App permission concerns (APC)					0.686***	1.128
Intention to accept app permissions (INT)	**0.270**			**0.270**		
MUIPC		–0.520***			–0.520***	

Notes: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; Cohen's f^2-statistics = [R^2incl. – R^2excl.] / [1- R^2incl.] with $f^2 \geq 0.02$ = small effect size, $f^2 \geq 0.15$ = medium effect size, and $f^2 \geq 0.35$ = large effect size (Cohen, 1988).

order construct for MUIPC and used the repeated indicator approach, which is favorable when the second-order construct is reflective (Lowry & Gaskin, 2014). The second-order reflective construct of MUIPC contained all indicators of its first-order subconstructs, i.e., *perceived surveillance*, *perceived intrusion*, and *secondary use of personal information*, which predicted the second-order construct. In addition to statistical significance, we also analyzed practical significance by using effect size calculation as per Cohen's f^2 statistics (Cohen, 1988). Measuring the effect size of empirical observations is considered a supplement to the statistical significance test, and it also determines the practical significance of the results (Kirk, 1996). Effect sizes have the advantage of being independent of the sample size, and the measures of the effect sizes allow a direct comparison of different quantities measured on different scales (Selya, Rose, Dierker, Hedeker, & Mermelstein, 2012). Table 4 shows the results of the path coefficient estimations and the effect sizes of the structural model, without app permission concerns included in the model (Model 1), and with app permission concerns included in the model (Model 2).

We found PPE and CA have direct positive effects on MUIPC with significance levels of $p < 0.001$ and small effect sizes, supporting H1 and H2. As hypothesized, results show that PC has a direct negative effect on MUIPC, supporting H3, however, the significance level decreases from $p < 0.001$ (Model 1) to $p < 0.05$ (Model 2) when APC is included in the model. Moreover, the small effect size of PC becomes very small after APC is included. Model 2 further reveals that APC has a direct positive effect on MUIPC with a path coefficient of $\beta = 0.686$ at a significance level of $p < 0.001$ and a very large effect size ($f^2 = 1.128$). Thus, H4 is supported. Finally, we found MUIPC has a direct negative effect on INT with a path coefficient of $\beta = -0.520$ at a significance level of $p < 0.001$, supporting H5. Overall, the percentage of variance explained for MUIPC increases from 18.5% (Model 1) to 61.7% (Model 2), when APC is included in the model. Fig. 3 shows the results of the structural equation modeling.

6. Discussion

6.1. Discussion of findings

This study aims to clarify the role of app permission requests regarding mobile users' information privacy concerns compared to prior privacy experience, computer anxiety, and perceived control. Results of a PLS-SEM analysis with 775 respondents indicated that all four antecedents influence users' privacy concerns, with app permission concerns having a major impact. Through our study, we confirm significant effects of prior privacy experience, computer anxiety, and perceived control on privacy concerns, as previously reported in prior studies (Osatuyi, 2015; Smith et al., 1996; Stewart & Segars, 2002; Xu, Gupta et al., 2012). However, the construct of app permission concerns has approximately twice as much predictive value than the other factors put together to explain mobile users' overall information privacy concerns. This implies that app permission concerns have an important effect on mobile users' concerns for information privacy and that researchers should not exclude it from future models. Following Wang et al.'s (2016) suggestion, our findings support the notion that the wired environment is critically different from the mobile environment, which we presume has made another major shift with the rising popularity of mobile apps and growing app permission requests. Accordingly, we suggest that future mobile privacy research should find new ways of alleviating concerns for app permission requests, which will provide practical implications for app stores and providers.

6.2. Contribution to theory

Our study contributes to existing privacy research in several ways. First, our primary contribution is to clarify the role of app permission requests regarding mobile users' concerns for information privacy. While prior studies have focused on distinct characteristics of app permission requests such as permission sensitivity, justification, or desensitization (Gu et al., 2017; Harris et al., 2016), in this research, we analyze mobile users' concerns for app permission requests per se and the impact on their overall information privacy concerns. While Gu et al. (2017) found sensitivity and justification to be significantly influencing privacy concerns, in Harris et al.'s (2016) study, desensitization of excessive permission requests had no significant impact on risk perceptions to install an app. The insights from these studies support the assumption that app providers should take the sensitivity of app permissions into account and provide reasonable justification whenever permissions are requested; however, users do not seem to become desensitized to excessive permissions, and our findings support that assumption given the major impact of app permission concerns on mobile users' privacy concerns. From this, we suggest that future mobile privacy research can build on our findings and extend the theory on privacy by seeking opportunities to mitigate app permission concerns, which will eventually further extend contributions to mobile users' information privacy concerns.

Second, we respond to Smith et al.'s (2011) call for research to investigate an expanded set of antecedents across contexts in the APCO model. We chose the mobile environment as the context of our study and while prior privacy experience was introduced in prior APCO models (Dinev et al., 2015; Smith et al., 2011), we integrated further factors in our mobile-related APCO model including computer anxiety and perceived control drawn from prior privacy studies (Stewart & Segars, 2002; Xu, Gupta et al., 2012), as well as app permission concerns as a new antecedent. Our study extends the literature by proposing these factors as antecedents in the APCO model from a mobile perspective, because with the growing popularity and ubiquity of mobile apps there is not only an increase of privacy issues with mobile apps, but there is also a growing concern for the continuing automation which induces anxiety, an ambiguity of privacy settings leading to a loss of control, and an incremental increase of excessive app permission

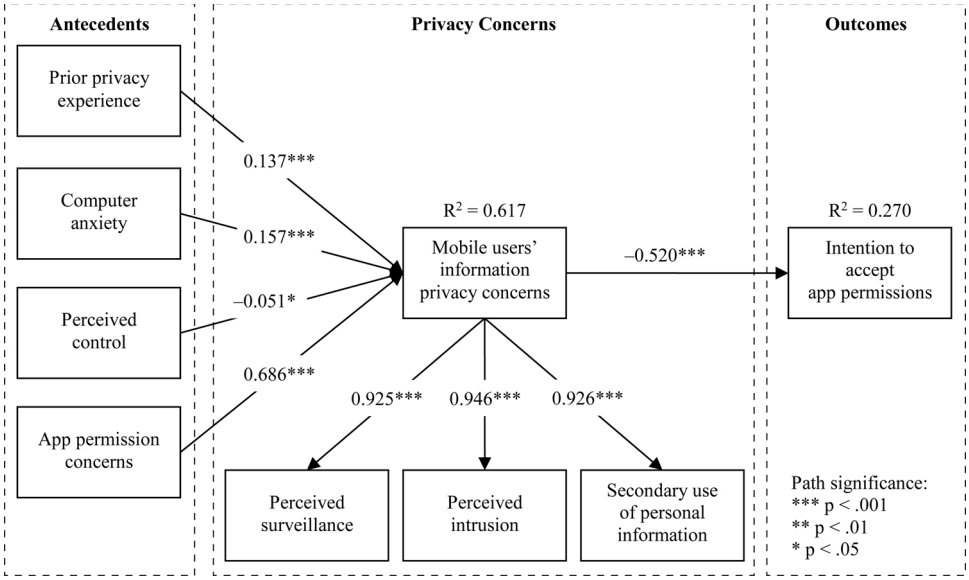


Fig. 3. Results of structural equation modeling.

requests. Based on our findings, which suggest that the construct of app permission concerns is the most important antecedent of mobile users' privacy concerns, it would be important for mobile privacy researchers to include app permission concerns in the examination of antecedents of privacy concerns in future mobile-related APCO models.

6.3. Implications for practice

From a practical perspective, app stores and providers should be alarmed that unnecessary and excessive app permission requests have a strong effect on users' privacy concerns, which can prevent users from installing mobile apps or make them feel uncomfortable with the result being that they uninstall an app (Boyles et al., 2012). As a consequence, app providers should ensure that they access personal information stored on mobile devices only if necessary and justified with value-added services, such as location tracking due to navigation purposes. As per our results show, app permission concerns have a highly significant impact on mobile users' overall information privacy concerns. Considering the large effect of app permission concerns, app providers should reduce permission requests to a required minimum. Due to this large effect, we further suggest that enhancements of the design and presentation of app permission requests are required to respond to the ever-growing privacy concerns of mobile users. For example, the ambiguity and uncertainty of the safety and necessity of app permissions could be resolved by user-generated ratings, which have become ubiquitous and influential on the Internet and the mobile app market (Chang, Ku, & Chen, in press; Gao, Greenwood, Agarwal, & McCullough, 2015; Liu, Au, & Choi, 2014), and which could also help to illuminate privacy assurances of mobile services. Results of this study lead to the recommendation that the mitigation of mobile users' privacy concerns is important more than ever due to the rapid growth of mobile apps and excessive app permission requests as a consequence thereof.

7. Conclusion

This study presented an empirical analysis of the influence of prior privacy experience, computer anxiety, perceived control, and app permission concerns on mobile users' overall information privacy concerns. While prior privacy experience, computer anxiety, and perceived control had a significant impact on mobile users' information privacy concerns, the predictive value of app permission concerns was approximately twice as much than the other factors put together. Our findings suggested that existing designs of app permission requests are problematic such that mobile users refuse to disclose their personal information mainly due to concerns for app permission requests. App stores and providers can leverage the findings of this study and rethink the design features of app permission requests to alleviate mobile users' concerns for app permission requests, which in turn decreases users' overall information privacy concerns, and eventually leads to an increase of the intention to accept app permissions.

7.1. Limitations

Our study is subject to the following limitations. First, the survey was conducted with participants from the United States. While various states within the United States were broadly covered in our study, a survey in other countries may lead to different results. According to Hofstede's cultural dimension index, the United States is a highly individualist culture (Hofstede, Hofstede, & Minkov, 2010). Thus, mobile users from the United States might have higher privacy concerns due to individual interests compared with users from collectivist cultures. Second, most of our participants were female students and up to the age of 30 years. Correlations of the demographic variables with other variables were very low in our sample, which indicated that there were no confounding effects. Nevertheless, other demographic user groups might present different concerns for information privacy. Third, we collected data through an online survey, which is liable to a self-selection bias (Kim, Lee, Han, & Lee, 2002). During participant recruiting, we asked participants to complete a survey about a social networking app. We did not mention that the focus of the survey is on information privacy concerns. Hence, the decision of the subjects to participate in the survey should not be related to their information privacy concern (Hui, Teo, & Lee, 2007). Fourth, for our scenario, we chose three most common app permissions: location, contacts, and photos. We acknowledge that these app permissions may be perceived as highly sensitive by mobile users compared to other permissions such as access to the vibrator or reminders. While perceived permission sensitivity has been analyzed in prior studies (Gu et al., 2017), in our study, we lay the focus on the overall impact of app permission concerns on mobile users' privacy concerns; however, we do suggest that other app permissions than location, contacts, and photos may lead to different results.

7.2. Future research directions

Against the backdrop of increasing privacy-related challenges for app stores and providers, our findings provide a basis for future research studies on mobile users' concerns for information privacy with a focus on app permission requests. Following the investigation by Gu et al. (2017) on permission sensitivity and justification, future research could explore effects of app permission requests on privacy concerns in more detail by addressing the following aspects. For example, effects of permission requests on privacy concerns might vary considering apps of different popularity (Gu et al., 2017) or reputation (Harris et al., 2016). It would be insightful to learn if the influence of permission requests on privacy concerns is alleviated the more popular or the more positive the reputation of an app is. Another focus of interest in this regard are privacy assurance approaches such as privacy statements, which ensure user privacy and data protection (Sutanto et al., 2013; Xu, Gupta et al., 2012). We suggest further research to analyze whether such privacy statements lose their effect the more app permissions are perceived to be of concern. Within these settings, we further suggest to consider perceived control in a future analysis, because control might provide a reinforcement or substitution effect, when (a) the popularity or reputation of an app is lower than other apps, (b) the app permissions are highly sensitive, (c) app permission requests are poorly or not at all justified, or (d) privacy statements on how safe the access to personal information is, are missing. As described earlier, user-generated ratings may also help to further alleviate privacy concerns. Future research could involve experimental surveys to evaluate the impact of such ratings on app permission concerns. For example, different scenarios could be presented in which app permissions are requested with various rating options. Questions could revolve around how safe it is for mobile users to share their personal information with the app and how necessary it is to request certain app permissions. We expect that further research on these proposed investigations will further contribute to a better understanding of mobile users' information privacy concerns.

Acknowledgements

I wish to thank my wife, Tuba Degirmenci, for her support and encouragement. I also thank the two anonymous reviewers for their valuable comments and suggestions. This research was supported by a grant from the Australian Research Council (DP150100163).

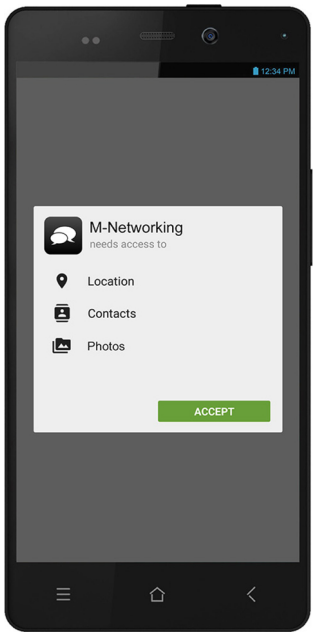
Appendix A. Participant profiles

Variable	Category	Frequency	Percentage
Gender	Female	529	68.3
	Male	195	25.2
	Missing	51	6.6
Age	≤ 20 years	303	39.1
	21-30 years	281	36.3
	31-40 years	72	9.3
	41-50 years	41	5.3
	> 50 years	29	3.7
	Missing	49	6.3
State	Georgia	56	7.2
	Pennsylvania	47	6.1
	Texas	37	4.8
	Illinois	36	4.6
	California	35	4.5
	New York	31	4.0
	New Hampshire	30	3.9
	Ohio	29	3.7
	Florida	28	3.6
	North Carolina	25	3.2
	Massachusetts	24	3.1
	New Jersey	24	3.1
	Connecticut	18	2.3
	Kentucky	16	2.1
	Michigan	16	2.1
	Indiana	15	1.9
	Virginia	13	1.7
	Washington	13	1.7
	Washington, D.C.	12	1.5
	Maryland	12	1.5
	Minnesota	11	1.4
	Other	76	9.8
	Missing	171	22.1
Profession	Employed	196	25.3
	Homemaker	4	0.5
	Self-employed	42	5.4
	Student	462	59.6
	Other	23	3.0
	Missing	48	6.2
Education	Less than high school	1	0.1
	High school degree	376	48.5
	College degree	113	14.6
	Undergraduate degree	138	17.8
	Graduate degree	87	11.2
	Other	11	1.4
	Missing	49	6.3

Yearly household net income	≤ $20,000	132	17.0
	$20,001-$40,000	79	10.2
	$40,001-$60,000	87	11.2
	$60,001-$100,000	107	13.8
	> $100,000	133	17.2
	Not specified	189	24.4
	Missing	48	6.2
Mobile operating system	Android	244	31.5
	iOS	518	66.8
	Other	13	1.8

Appendix B. Scenario

We provided a scenario to all participants in the survey. They were told that an online social networking service is providing a mobile application called “M-Networking”, and that their opinion about the app was being solicited. The survey included the following scenario: “An online social networking service provides M-Networking, which is a mobile application to connect with other users such as family, friends, and colleagues. Suppose you are considering whether you will install such M-Networking service on your mobile device, the app is requesting the following permissions: location (approximate location (network-based), precise location (GPS and network-based), and GPS access), contacts (read your contacts, modify or delete your contacts, and create contacts), and photos (access your photos, modify or delete your photos, and add photos)”.



Appendix C. Survey instrument

Core construct	Measurement items	Source
Prior privacy experience (PPE)	PPE1: How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce web site without your authorization? PPE2: How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet? PPE3: How often have you personally been the victim of what you felt was an improper invasion of privacy?	Xu, Gupta, et al. (2012)
Computer anxiety (CA)	CA1: Computers are a real threat to privacy in this country. CA2: I am anxious and concerned about the pace of automation in the world. CA3: I am sometimes frustrated by increasing automation in my home.	Stewart and Segars (2002)
Perceived control (PC)	PC1: How much control do you feel you have over your personal information that has been released? PC2: How much control do you feel you have over the amount of your personal information collected by mobile apps? PC3: Overall, how much in control do you feel you have over your personal information provided to mobile apps? PC4: How much control do you feel you have over who can get access your personal information? PC5: How much control do you feel you have over how your personal information is being used by mobile apps?	Xu, Teo, et al. (2012)
App permission concerns (APC)	If I would install this app on my mobile device… APC1: it would bother me when I am asked to accept these app permissions. APC2: I would think twice before accepting these app permissions. APC3: it would bother me to accept these app permissions.	Smith et al. (1996)
Perceived surveillance (PS)	If I would accept these app permissions… PS1: I believe that my mobile device would be monitored at least part of the time.	Xu, Gupta, et al. (2012)

	PS2: I would be concerned that the app is collecting too much information about me. PS3: I would be concerned that the app may monitor my activities on my mobile device.	
Perceived intrusion (PI)	If I would accept these app permissions… PI1: I feel that as a result, others would know about me more than I am comfortable with. PI2: I believe that as a result, information about me that I consider private would be more readily available to others than I would want. PI3: I feel that as a result, information about me would be out there that, if used, would invade my privacy.	Xu et al. (2008)
Secondary use of personal information (SU)	If I would accept these app permissions… SU1: I would be concerned that the app may use my personal information for other purposes without notifying me or getting my authorization. SU2: I would be concerned that the app may use my information for other purposes. SU3: I would be concerned that the app may share my personal information with other entities without getting my authorization.	Smith et al. (1996)
Intention to accept app permissions (INT)	Given these app permission requests, specify the extent to which you would accept these app permissions. INT1: unwilling–willing INT2: unlikely–likely INT3: not probable–probable INT4: impossible–possible	Malhotra et al. (2004)

References

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior.* Upper Saddle River, NJ: Prentice-Hall.

App Annie (2016). *Digital app economy forecast: App annie's app monetization report*Retrieved from. App Anniehttps://www.appannie.com/en/insights/market-data/app-monetization-report-2016/.

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems, 28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002.

Borena, B., Belanger, F., Ejigu, D., & Anteneh, S. (2015). Conceptualizing information privacy concern in low-income countries: An Ethiopian language instrument for social networks sites. *Paper Presented at the Americas Conference on Information Systems*.

Boyles, J. L., Smith, A., & Madden, M. (2012). *Apps and privacy: More than half of app users have uninstalled or decided to not install an app due to concerns about their personal information.* Internet & Technology. Retrieved fromPew Research Centerhttp://www.pewinternet.org/2012/09/05/main-findings-7/.

Brown, S. A., Fuller, R. M., & Vician, C. (2004). Who's afraid of the virtual world? Anxiety and computer-mediated communication. *Journal of the Association for Information Systems, 5*(2), 79–107. https://doi.org/10.17705/1jais.00046.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7–19. https://doi.org/10.1509/jppm.19.1.7.16951.

Chang, S.-J., Van Witteloostuijn, A., & Eden, L. (2010). From the editors: Common method variance in international business research. *Journal of International Business Studies, 41*(2), 178–184. https://doi.org/10.1057/jibs.2009.88.

Chang Y.-C., Ku C.-H. and Chen C.-H., *Social media analytics: Extracting and visualizing Hilton hotel ratings and reviews from TripAdvisor*, International Journal of Information Management, 1–17, doi: 10.1016/j.ijinfomgt.2017.11.001 (in press).

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security, 25*(3), 330–344. https://doi.org/10.1108/ICS-04-2016-0027.

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management, 39*, 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), vii–xvi.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600.

Du, S., Keil, M., Mathiassen, L., Shen, Y., & Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in IT project risk assessment. *Decision Support Systems, 43*(1), 269–283. https://doi.org/10.1016/j.dss.2006.10.002.

eMarketer (2016). *Most mobile users will delete an app if concerned about security: Users are asked to share different types of information when downloading apps.* Retail & Ecommerce: Mobile. Retrieved fromeMarketerhttps://www.emarketer.com/Article/Most-Mobile-Users-Will-Delete-App-Concerned-About-Security/1013488.

Enck, W. (2011). Defending users against smartphone apps: Techniques and future directions. In S. Jajodia, & C. Mazumdar (Vol. Eds.), *Information systems security: Vol. 7093*, (pp. 49–70). Berlin: Springer. https://doi.org/10.1007/978-3-642-25560-1_3 Lecture Notes in Computer Science ed.

Federal Trade Commission (2013). *Path social networking app settles FTC charges it deceived consumers and improperly collected personal information from users' mobile address books.* Retrieved fromFederal Trade Commission: Protecting America's Consumershttps://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104.

Gao, G. G., Greenwood, B. N., Agarwal, R., & McCullough, J. S. (2015). Vocal minority and silent majority: How do online ratings reflect population perceptions of quality. *MIS Quarterly, 39*(3), 565–589. https://doi.org/10.25300/MISQ/2015/39.3.03.

Gu, J., Xu, J. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002.

Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks, CA: Sage Publications.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management, 36*(3), 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004.

Hern, A. (2018). *Far more than 87m Facebook users had data compromised, MPs told.* Retrieved fromThe Guardianhttps://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind – Intercultural cooperation and its importance for survival* (3rd ed.). New York: McGraw-Hill.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33. https://doi.org/10.2307/25148779.

Jung, Y., & Park, J. (2018). An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management, 43*, 15–24. https://doi.org/10.1016/j.ijinfomgt.2018.05.007.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29.

Keith, M. J., Babb, J. S., & Lowry, P. B. (2014). A longitudinal study of information privacy on mobile devices. *Paper Presented at the Hawaii International Conference on System Science*.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal, 25*(6), 637–667. https://doi.org/10.1111/isj.12082.

Keith, M. J., Thompson, S. C., Hale, J. E., & Greer, C. (2012). Examining the rationality of information disclosure through mobile devices. *Paper Presented at the International Conference on Information Systems*.

Kim, J., Lee, J., Han, K., & Lee, M. (2002). Businesses as buildings: Metrics for the architectural quality of Internet businesses. *Information Systems Research, 13*(3), 239–254. https://doi.org/10.1287/isre.13.3.239.79.

Kirk, R. E. (1996). Practical significance: A concept whose time has come. *Educational and Psychological Measurement, 56*(5), 746–759. https://doi.org/10.1177/0013164496056005002.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. https://doi.org/10.4018/ijec.2015100101.

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546–580.

Kuchler, H. (2018). *Software bug made millions of Facebook users' private posts public: As many as 14m users were affected by the error, which was not caught for 10 days.* Retrieved fromFinancial Timeshttps://www.ft.com/content/49749f5e-6a8b-11e8-b6eb-4acfcfb08c11.

Kummer, T.-F., Recker, J., & Bick, M. (2017). Technology-induced anxiety:

Manifestations, cultural influences, and its effect on the adoption of sensor-based technology in German and Australian hospitals. *Information & Management, 54*(1), 73–89. https://doi.org/10.1016/j.im.2016.04.002.
Lang, M., Wiesche, M., & Krcmar, H. (2018). Perceived control and privacy in a professional cloud environment. *Paper Presented at the Hawaii International Conference on System Sciences*.
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.
Lienhard, K., & Legner, C. (2015). The anatomy of context-aware mobile patient monitoring. *Paper Presented at the International Conference on Information Systems*.
Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *The Journal of Applied Psychology, 86*(1), 114–121.
Liu, C. Z., Au, Y. A., & Choi, H. S. (2014). Effects of freemium strategy in the mobile app market: An empirical study of Google Play. *Journal of Management Information Systems, 31*(3), 326–354. https://doi.org/10.1080/07421222.2014.995564.
Lom, H. S., Thoo, A. C., Sulaiman, Z., & Adam, S. (2018). Moderating role of mobile users' information privacy concerns towards behavioural intention and use behaviour in mobile advertising. *Advanced Science Letters, 24*(6), 4259–4264. https://doi.org/10.1166/asl.2018.11584.
Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200. https://doi.org/10.2753/MIS0742-1222270406.
Lowry, P. B., & Gaskin, J. E. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication, 57*(2), 123–146. https://doi.org/10.1109/TPC.2014.2312452.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032.
Neate, R. (2018). *Over $119bn wiped off Facebook's market cap after growth shock.* Retrieved fromThe Guardianhttps://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock.
Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior, 49*, 324–332. https://doi.org/10.1016/j.chb.2015.02.062.
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. *MIS Quarterly, 31*(1), 105–136. https://doi.org/10.2307/25148783.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.
Robertson, J. (2012). *Android apps collect too much user data, researcher says.* Technology: Security. Retrieved fromThe Sydney Morning Heraldhttps://www.smh.com.au/technology/android-apps-collect-too-much-user-data-researcher-says-20121102-28oie.html.
Selya, A. S., Rose, J. S., Dierker, L. C., Hedeker, D., & Mermelstein, R. J. (2012). A practical guide to calculating Cohen's f^2, a measure of local effect size, from PROC MIXED. *Frontiers in Psychology, 3*(111), 1–6. https://doi.org/10.3389/fpsyg.2012.00111.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196. https://doi.org/10.2307/249477.
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560. https://doi.org/10.2307/40041279.
Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97.
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 Quarterly, 37*(4), 1141–1164. https://doi.org/10.25300/misq/2013/37.4.07.
Thatcher, J. B., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26*(4), 381–396. https://doi.org/10.2307/4132314.
Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. In G. Chowdhury, J. McLeod, V. Gillet, & P. Willet (Vol. Eds.), *Transforming digital worlds: Vol. 10766*, (pp. 229–239). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-78105-1_27.
Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003.
Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? *International Journal of Information Management, 44*, 164–177. https://doi.org/10.1016/j.ijinfomgt.2018.10.016.
Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003.
Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *Paper Presented at the International Conference on Information Systems*.
Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *Paper Presented at the International Conference on Information Systems*.
Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *Paper Presented at the International Conference on Information Systems*.
Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135–173. https://doi.org/10.2753/MIS0742-1222260305.
Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416.
Yin, D., Bond, S. D., & Zhang, H. (2014). Anxious or angry? Effects of discrete emotions on the perceived helpfulness of online reviews. *MIS Quarterly, 38*(2), 539–560. https://doi.org/10.25300/misq/2014/38.2.10.
Zhang, D., Adipat, B., & Mowafi, Y. (2009). User-centered context-aware mobile applications—The next generation of personal mobile computing. *Communications of the Association for Information Systems, 24*(3), 27–46. https://doi.org/10.17705/1cais.02403.
Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012.