App Users Unwittingly in the Spotlight

A Model of Privacy Protection in Mobile Apps

Wottrich, V.M.; van Reijmersdal, E.A.; Smit, E.G.

DOI
10.1111/joca.12218

Publication date
2019

Document Version
Final published version

Published in
Journal of Consumer Affairs

VERENA M. WOTTRICH, EVA A. VAN REIJMERSDAL, AND EDITH G. SMIT

App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps

Mobile apps are increasingly jeopardizing app users' online privacy by collecting, storing, and sharing personal data disclosed via apps. However, little is known about mobile app users' current privacy protection behavior and the factors that motivate it. Drawing on Roger's Protection Motivation Theory (PMT), this study develops and tests the App Privacy Protection Model among 1,593 Western European app users. The results demonstrate that, on the one hand, increased levels of perceived self-efficacy, vulnerability, and privacy concern enhance mobile app users' motivation to engage in risk-reducing behavior, while on the other hand, higher levels of knowledge of the data collection practices of mobile apps, app attitude, and perceived response costs diminish it. Being the first study that applies PMT in the mobile app context, this study offers several important implications regarding privacy protection in mobile apps.

Today, app users constantly, and often unwittingly, create quantifiable information online by downloading and using mobile apps (Buck et al. 2014; Perlroth and Bilton 2012; Sipior, Ward, and Volonino 2014). These data are regularly used by analytics companies to observe and identify patterns of consumer conduct, to aggregate consumer information into profiles, and to sell this information to marketers or other interested parties who, in turn, use these data for customized marketing or predictive analytics (Ashworth and Free 2006; Buck et al. 2014; Esposti 2014; Shklovski et al. 2014; Sipior, Ward, and Volonino 2014; van Dijck 2014). Despite the potentially positive outcomes of this kind of tracking, such as receiving targeted ads that fit ones interests (Aguirre et al. 2015), mobile app users may also experience direct negative consequences, such

Verena M. Wottrich (v.m.wottrich@uva.nl) is a PhD Candidate of Persuasive Communication, Eva A. van Reijmersdal (e.a.vanreijmersdal@uva.nl) is Associate Professor of Persuasive Communication, and Edith G. Smit (e.g.smit@uva.nl) is Full Professor of Persuasive Communication, all at the Amsterdam School of Communication Research, ASCoR, University of Amsterdam.

The Journal of Consumer Affairs, Fall 2019: 1056–1083
DOI: 10.1111/joca.12218

as discrimination in buying situations (Bauman and Lyon 2013; Esposti 2014), identity theft (Reyns 2013), fraud (Narayanan, Koo, and Cozzarin 2012), and unwanted commercial solicitations (Sutanto et al. 2013).

To better protect consumer data and regulate data collection practices, the European Union (EU) is currently taking the following measures. First, the EU introduced a comprehensive reform of data protection rules in May 2016, which aims, among others, to "give citizens back control over their personal data" (European Commission 2018). Second, the EU relies on a self-regulation principle, which is based on the assumption that consumers respond to businesses' data collection practices in a calculated and rational manner (Acquisti, John, and Loewenstein 2013) and that they take the necessary steps to protect their privacy. As becomes apparent from these two measures, the EU places the responsibility for the protection of personal data partly on consumers. Prior research, however, has shown that (mobile) Internet users currently do not seem to discharge their privacy protection responsibility, because they, for instance, barely read the privacy policies of apps (Liu 2014; Shklovski et al. 2014) or discount the value of their privacy for immediate gratifications associated with the information disclosure (e.g., gift cards) (Acquisti and Grossklags 2005, 2007; Acquisti, John, and Loewenstein 2013). Therefore, it is important to understand which factors motivate app users to protect their privacy in the mobile app context. It is necessary to focus on the mobile context in particular, because, in contrast to other digital devices, such as personal computers, mobile devices have become extensions to the self (Vishwanath and Chen 2008), which "are typically personal to an individual, almost always on, and with the user" (Federal Trade Commission [FTC], 2013, 2). More than other types of technology, mobile devices "can facilitate data collection and sharing among many entities, including […] application developers, analytics companies, and advertisers to a degree unprecedented in the desktop environment" (FTC, 2013, 2). Moreover, they can reveal precise information about a user's location "in ways not anticipated by consumers" (FTC, 2013, 3). Thus, mobile devices may compromise consumer privacy way more than other digital devices, which is why an independent study of privacy protection in the mobile app context is necessary.

This study aims to understand which factors motivate app users to protect their privacy in the mobile app context drawing on Protection Motivation Theory (PMT) (Rogers 1975, 1983), a theory that has been widely applied to consumer privacy and security issues (e.g., Boehmer et al. 2015; Milne and Culnan 2004), but not yet to the mobile app context. By surveying 1,593 mobile app users between 18 and 88 years old about the 12 most popular mobile apps in a Western European country, the

current study offers several important contributions. Theoretically, this study contributes to the growing body of literature using PMT to examine privacy behavior in the mobile app context (Boehmer et al. 2015; Milne, Labrecque, and Cromer 2009) by providing a theoretical refinement of PMT (Rogers 1975, 1983). More specifically, we show the need for including the concept of *knowledge* as an additional PMT construct. In doing so, we extend PMT and make it more applicable to the mobile app context. Moreover, we provide a more nuanced understanding of the factors that motivate app users to protect their privacy. Practically, the findings of this study offer important implications for public policy and consumer empowerment by showing that increased privacy concerns, vulnerability, and self-efficacy perceptions are positively related to privacy protection motivation. Thus, it might be beneficial for policymakers to concentrate their efforts on increasing mobile app users' awareness of potential privacy threats and their belief that they can protect their mobile privacy.

THEORETICAL BACKGROUND

Understanding Privacy Protection Behavior

Privacy, conceptualized by Altman (1975, 24) as "the selective control of access to the self," is characterized by a temporal, dynamic process, in which individuals attempt to protect their privacy by adjusting the boundaries of which information they disclose in their interaction with others. Whether individuals, in fact, adjust their privacy boundaries, is likely to depend on their "protection motivation," that is, their desire to protect themselves from threats (Rogers 1975). Applying this concept in the mobile app context, we define "protection motivation" as mobile app users' desire to engage in privacy-enhancing behavior, such as turning off GPS or Wi-Fi connections, reading privacy policies, or deleting apps that jeopardize privacy.

The term "protection motivation" is adapted from PMT, which was originally introduced by Rogers (1975, 1983) in an attempt to understand the effects of health-threat messages on health attitude change. PMT has become more and more relevant in the privacy and online safety context during the last decade (Boehmer et al. 2015; Cho, Rivera-Sánchez, and Lim 2009; Ifinedo 2012; Lee, LaRose, and Rifon 2008; Youn 2009). The original PMT model (Rogers 1975) posits that individuals' motivation to protect themselves from threats arises from three cognitive appraisal processes: (1) perceiving the threat to be noxious (i.e., perceived severity), (2) perceiving the threat to be likely to occur to oneself (i.e., perceived

vulnerability), and (3) perceiving the protective behavior to be effective in reducing the threat (i.e., perceived response efficacy).

In a later version, Rogers (1983) extended PMT to a more general theory of persuasive communication by adding three more cognitive appraisals that affect individuals' protection motivation. These are (4) individuals' belief to be able to perform the protective behavior (i.e., perceived self-efficacy), (5) any perceived costs (e.g., monetary, effort, time) associated with the protective behavior (i.e., response costs), and (6) the benefits (i.e., positive beliefs and attitudes) associated with the risky behavior. While the first four cognitive assessments increase individuals' motivation to engage in threat-reducing behavior, the last two appraisals diminish it. Taken together, these six constructs are important determinants of individuals' motivation to protect themselves from threats.

In this study, we propose a theoretical refinement of PMT. We argue that mobile app users' prior knowledge of the data collection and usage practices of apps should be added as an additional PMT construct. Prior literature on individuals' responses to fear appeal massages has often distinguished between objective knowledge (i.e., what you know) and subjective knowledge (i.e., what you think you know) (e.g., Morman 2000; Nabi, Roskos-Ewoldsen, and Carpentier 2008). A study by Morman (2000), for instance, has demonstrated that objective knowledge plays an important role in encouraging healthy behaviors, while subjective knowledge does not. His research showed that an objective knowledge gain on testicular cancer was positively associated with individuals' attitude toward and intention to perform the protective response (i.e., testicular self-exams). This was not the case for the subjective knowledge gain. In addition, So (2013) has postulated that information (or knowledge) of a threat plays an essential role in triggering fear or danger control processes. According to the author, adequate information on how to avert the danger is expected to increase self-efficacy and response efficacy perceptions, which is initiating a danger control process and forming protection motivation. Against this backdrop, we argue that the construct objective knowledge (i.e., app users' knowledge of the data collection and usage practices of mobile apps) is a prerequisite for motivating app users to protect their privacy in apps. In fact, prior research supports this assumption: According to Park (2011), a critical understanding of data flow and its implicit rules is necessary for users to be able to act. Moreover, it has been shown that to exercise appropriate measures of resistance against the potential abuse of personal information, users need to understand the data flow in cyberspace and its acceptable limits of exposure (Ball and Webster 2003). Based on

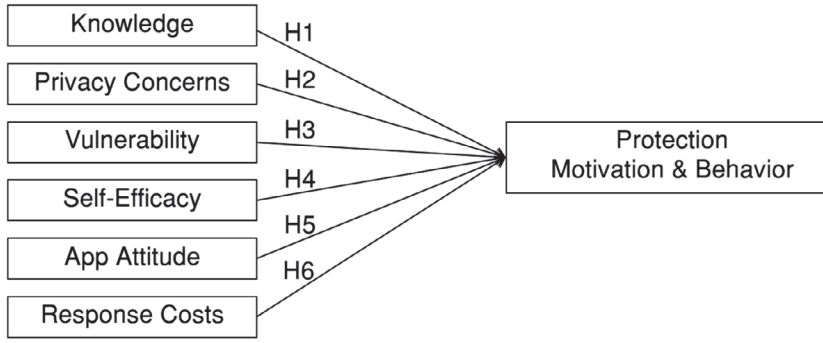
this argumentation we added the variable mobile app knowledge to our conceptual model.

Second, we did not differentiate between response efficacy and self-efficacy in this study, but rather we included an overall efficacy measure called privacy self-efficacy, due to the following reasons. At the moment, mobile app users do have a few options to respond to the data collection and usage practices of apps (e.g., using apps that restrict information disclosure), but these options are very limited and not commonly used. Compared to the general Internet environment, in which users are less constrained to disclose personal information, mobile app users mostly only have a "take it" (i.e., accept the terms, thereby jeopardizing privacy) or "leave it" (i.e., refuse to download the app) option when downloading apps. In other words, to use most apps, users have to make a conscious choice to first download the application and agree to the terms and conditions, which represents a higher investment than just visiting a Web site. When app users choose the "take it" option, they mostly do not have any leeway to influence how much personal data the app wants to access. Hence, there are currently not many real response options for mobile app users to protect their privacy except not installing privacy-invading apps. Letting users assess the response efficacy of the "not-installing-an-app-strategy" seems to be unnecessary, because an app that is not installed on a mobile device can obviously not invade consumer privacy and the strategy is, therefore, very effective. Another option to assess response efficacy would be to ask users about the efficacy of responses that do not exist yet or that are not commonly used; however, doing so would not only impair the ecological validity of our study but also the internal validity. The only option to get insights into response efficacy perceptions would be to ask people if they think that they are able to respond to the data collection practices of apps. Although there might not be an effective response, people might still have a feeling of whether they can influence the data collection or not. This feeling might not necessarily reflect reality, but it can still be there and it might influence individuals' privacy protection motivation. Hence, in the specific context of mobile apps, in this study we do not differentiate between response efficacy and self-efficacy but we rather include an overall efficacy measure called privacy self-efficacy. Taken together, this study introduces and tests the App Privacy Protection Model (APPM) as depicted in Figure 1.

Mobile App Knowledge

According to the EU ePrivacy Directive (2002), that is, a directive for the protection of personal data in the electronic communications

FIGURE 1
App Privacy Protection Model



sector, firms that wish to track Internet users need to provide them with clear and complete information on the purpose of the tracking and they need to obtain the data subject's consent, that is, "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (EU Data Protection Directive 1995, 39). These rules apply to many online technologies, including mobile apps (Zuiderveen Borgesius 2013).

Despite these legal regulations, currently, (mobile) Internet users seem to be far from giving an "*informed* indication of will" when they agree to privacy policies, because they barely read them (Liu 2014; Milne and Culnan 2004; Shklovski et al. 2014). In fact, (mobile) Internet users' level of knowledge regarding the data collection and usage practices of online services is rather low: As recent research showed, only few general Internet users understood the most basic surveillance practices of Web sites (Park 2011; Smit, van Noort, and Voorveld 2014) and mobile apps (Felt et al. 2012). Moreover, app users were surprised and hardly aware that apps access so much personal information (Lin et al. 2012) and many mistakenly believed that apps do not share personal information with the third parties when they have a privacy policy (Park and Jang 2014).

Existing research has shown that higher levels of objective knowledge on online phishing attacks enhances computer users' phishing threat avoidance behavior (Arachchilage and Love 2014). In addition, it has been demonstrated that Internet users' awareness of the presence of spyware is a key predictor of taking active measures to protect against spyware intrusion and clean spyware from infected systems (Hu and Dinev 2005). Based on these findings, we hypothesize that:

H1: Mobile app knowledge will be positively related to app users' privacy protection (1) motivation and (2) behavior.

Privacy Concerns and Perceived Severity

Information privacy is becoming more and more a shared concern in the mobile Internet context (Sipior, Ward, and Volonino 2014), because apps are dramatically increasing the amount of personal data released to service providers and other interested parties (Bettini and Riboni 2015). Privacy concerns are defined as "concerns about [the] possible loss of privacy as a result of information disclosure to a specific external agent" (Xu et al. 2012, 2). In this study, we use the construct privacy concerns to approach the PMT construct severity, that is, individuals' perception of the noxiousness of the threat (Rogers 1975). Although we acknowledge that the notion of perceived *severity* and *concern* are not exactly the same, we purposely use privacy concerns in this study given that this variable has shown to be a key variable affecting privacy protective behavior, such as fabricating personal information or using privacy-enhancing technologies (e.g., Wirtz, Lwin, and Williams 2007; Youn 2009).

Prior research has shown that levels of privacy concern are high and increasing. While an EU study (European Commission 2011) showed that many Europeans are fairly concerned about their behavior being recorded via mobile phone or mobile Internet (49%), a TRUSTe study (2014) revealed that 85% of respondents worried about using apps. The majority of the respondents indicated that businesses sharing personal information with other companies form the most prevalent cause of concern. In line with these findings, a study by Shklovski et al. (2014) revealed that app users express strong concerns regarding the data collection practices of apps.

According to PMT, the higher the perceived severity of the threat, the higher individuals' protection motivation and behavior will be (Rogers 1975). In a similar vein, prior research has shown that privacy concerns motivate protection behaviors in the general Internet context: A study by Youn (2009), for instance, has demonstrated that highly privacy-concerned adolescent Internet users are more inclined to engage in privacy protection behavior, such as seeking out interpersonal advice or refraining from using certain Web sites than less-concerned users (Youn 2009). In addition, it has been shown that privacy concerns led to protective behaviors such as fabricating personal information or using privacy-enhancing technologies (Wirtz, Lwin, and Williams 2007), limiting the visibility of social network site profiles (Chen and Chen 2015), or rejecting unnecessary cookies (Milne and Culnan 2004). Therefore, we hypothesize that:

H2: Privacy concerns will be positively related to app users' privacy protection (1) motivation and (2) behavior.

Vulnerability

Vulnerability indicates the extent to which an individual feels the threat will occur to him/herself (Lee, LaRose, and Rifon 2008; Rogers 1975). Translating this to the mobile app context, vulnerability can be understood as the extent to which an app user feels that the possible privacy invasion caused by mobile apps will occur to him/herself. Research on app users' perceived vulnerability is scarce. Only the study of Shklovski et al. (2014) showed so far that app users have the feeling to be vulnerable and helpless when it comes to privacy protection on mobile devices.

PMT posits that a higher perceived level of vulnerability leads to a higher protection motivation and behavior (Rogers 1975, 1983). Existing literature has found evidence for this assumption showing that higher perceived levels of vulnerability led to a higher intention to engage in virus protection behavior (Lee, LaRose, and Rifon 2008), a higher adoption of protective security behaviors, such as reading privacy statements on the web (Milne, Labrecque, and Cromer 2009), more privacy protection motivation (Youn 2009), and higher levels of online safety behavior, such as using a pop-up blocker (Boehmer et al. 2015). We were interested to examine whether higher perceived vulnerability levels would be positively related to higher levels of protection motivation and behavior in the mobile app context. Based on the literature we hypothesize that:

H3: Perceived vulnerability will be positively related to app users' privacy protection (1) motivation and (2) behavior.

Privacy Self-Efficacy

The term self-efficacy relates to individuals' belief that they are able to perform the protective behavior (Rogers 1983). In this study, we use the term *privacy self-efficacy* to describe mobile app users' perceived confidence in their own ability to control the disclosure and subsequent use of personal information collected via mobile apps. There are mixed findings with regard to the extent to which Internet users think they are able to protect their privacy online.

On the one hand, research suggests that Internet users do have the feeling that they are able to protect themselves online: A survey conducted by the Committee on the Internal Market and Consumer Protection of the European Parliament (IMCO 2011) demonstrated, for instance, that 68%

of European consumers feel they have control over the data they share online. Similarly, a survey conducted by the EU (European Commission 2011) showed that the majority of the Europeans think they have some control (79%) over the information they disclose on social networking sites (SNS) and sharing sites and 68% reported having control over personal information disclosed when shopping online. Finally, a study by Chen and Chen (2015) revealed that SNS users perceived their self-efficacy in privacy management to be high.

On the other hand, research has also pointed at low levels of perceived privacy self-efficacy, suggesting that Internet users perceived their level of personal information control to be consistently low (Park, 2011), that they are not able to limit information gathering via apps (Thurm and Kane 2010), and that they have the feeling that there is not much they can do about the data collection of apps (Shklovski et al. 2014).

According to PMT (Rogers 1975, 1983), higher perceived levels of self-efficacy lead to more protection motivation and behavior. In fact, research has shown that higher levels of self-efficacy led to more online protection measures, such as updating software protections and communicating safely with others online (Boehmer et al. 2015), a higher intention to adopt virus protection behavior (Lee, LaRose, and Rifon 2008), to more spyware deletion, and to less risky behavior such as setting browsers' safety settings to low and providing credit card information (Milne, Labrecque, and Cromer 2009). We were interested to examine whether higher perceived self-efficacy levels would be positively related to higher levels of protection motivation and behavior in the mobile app context. We hypothesize that:

H4: Perceived self-efficacy will be positively related to mobile app users' privacy (1) motivation and (2) behavior.

Perceived Benefits and Response Costs

Existing literature assumes that prior to disclosing personal information online, for instance via mobile apps, individuals act as rational economic agents performing an analysis of the costs and benefits associated with the information trade. Based on this trade-off, individuals are presumed to decide whether they disclose personal information or not (Acquisti and Grossklags 2005; Aguirre et al. 2015; Fife and Orjuela 2012; Keith et al. 2013; Li, Sarathy, and Xu 2010). In this study, the term *benefits* refers to individuals' expectation of acquiring positive outcomes when continuing the risky behavior and not engaging in protective behavior (Lee, LaRose, and Rifon 2008; Rogers 1975). In the mobile app context, this means

that app users tend to engage in risky behavior, because they perceive the benefits of using an app to be more attractive than the protective behavior. In fact, research has shown that app users decide to engage in risky behavior in exchange for convenience, functionality, or financial gains (Acquisti & Grossklags, 2007) and when they think the utility of the app is high enough (Good et al. 2005). As apps offer a heterogeneous range of benefits, we decided to measure benefits in terms of app attitude, that is, their overall evaluation of the app in question. App attitude resembles benefits on a more abstract benefits level and is easily applicable to all the different apps used in this study. Based on the reviewed literature, we hypothesize that:

H5: App attitude will be negatively related to app users' privacy protection (1) motivation and (2) behavior.

On the other hand, whether individuals engage in privacy protection behavior also depends on their perceived response costs. Response costs refer to individuals' perceived costs that are associated with the protective behavior (Rogers 1983). These costs may be related to money, time, or effort (Lee, LaRose, and Rifon 2008), but they can also be related to abstaining from the benefits of an app. App users do not have much leeway to protect their privacy in mobile apps, because only a few apps offer users the opportunity to change privacy settings. Therefore, the most effective way of protecting one's privacy in apps is to stop using a particular privacy-invading app. This might negatively influence app users' privacy protection motivation and behavior, because refraining from using a particular app service may lead to unwanted consequences such as not having access to certain information or people. It might be that if the perceived costs of the trade are too high, in other words, if mobile app users need to give up too much for protecting their privacy, their protection motivation and behavior is likely to be low. In fact, research has shown that response costs may have a negative effect on Internet users' motivation to engage in online safety behaviors (LeFebvre 2012). However, there were also recent studies that did not find an effect of response costs on online safety intentions (Boehmer et al. 2015; Shillair et al. 2015). In this study, we expect that response costs are negatively related to protection motivation and behavior in the mobile app context, because stopping to use a certain app for privacy reasons seems to be a big consequence for app users. Based on this, we hypothesize:

H6: Response costs will be negatively related to app users' privacy protection (1) motivation and (2) behavior.

METHOD

App Differences

Leading app stores comprise thousands of apps. While Android users can choose from 2.8 million apps in the Google Play store, Apple users can pick from 2.2 million apps in the Apple App store (Statista 2017). Given the fact that each of these apps offers different functions and handles different data collection and usage practices, it is important to investigate our main constructs on a more specific level, thus, for specific mobile apps. It might namely be that differences in apps lead to different outcomes. Therefore, we let our participants answer all our questions on *one specific app* and we examined whether we needed to take app differences into account in our analyses. At the beginning of the results section, we will present the results of these analyses. The 12 different apps used in this study were selected based on a pretest conducted among 28 Western European smartphone and tablet users (60.7% female; age: $M = 38.36$; $SD = 15.33$). In this pretest, participants were asked to indicate for a total of 75 apps derived from the app-popularity rankings of the Apple App Store and the Android Play Store (calendar week 25, 2015), whether they used these apps on their smartphone and/or tablet. Based on the results of the pretest, we selected the following most used, free apps for the final survey: WhatsApp (instant messenger), Facebook (SNS), Buienradar (weather app), GoogleMaps (mapping service), Gmail (e-mail service), YouTube (video platform), Nu.nl (news app), Skype (telecommunications app), Wordfeud (Scrabble gaming app), Dropbox (online cloud), 9292 (public transport app), and Spotify (music streaming app). We chose these 12 apps because they are currently the most used apps in the country where the study took place, which is why they represent a potential privacy danger to a lot of people.

Procedure

At the beginning of the actual survey, we obtained participants' informed consent and assessed demographics and general privacy concerns. Hereafter, we determined respondents' participation eligibility. Only respondents who owned a smartphone and/or a tablet and had downloaded at least one of the 12 most used free apps were allowed to participate. After the screening, *one* of the 12 apps was randomly chosen and respondents eligible for participating in the study answered questions *only about this specific app* in the subsequent part of the questionnaire. These questions measured: app attitude, privacy concerns,

mobile app knowledge, privacy self-efficacy, and perceived vulnerability. After these app-specific questions, respondents' smartphone or tablet use was assessed. Finally, the following variables were measured: privacy protection motivation, app download habit, response costs, protection behavior, prior experience of privacy infringement, and app use.

Sample and Data Collection

The online survey was distributed among the international Esomar-certified online panel of the online market research institute PanelClix between July 24 and 31, 2015. PanelClix sent e-mails containing a link to the questionnaire to a representative sample of the country's population (18+). A total of 11,667 panel members were invited to participate in the study. Of these invitees, 2,684 people started the survey, resulting in a response rate of 23%. Of the 2,684 initial survey starts, 1,796 questionnaires were completed; hence, the completion rate was 67% and 203 completed questionnaires (11%) were removed from the sample, because these respondents had completed the whole questionnaire unusually fast and their response patterns indicated they had not read the survey questions properly. Hence, the net sample size was 1,593 (49% female; $M_{age} = 50.95$; $SD = 16.09$; range 18–88 years).

The sample approximated the country's population of 18 years and older (Centraal Bureau voor de Statistiek (CBS) 2015) with respect to gender (sample: 49.3% female; country population: 50.5% female). With regard to age and education, mean levels were slightly higher in the sample than in the population (age: $M_{sample} = 50.95$; $M_{CBS} = 41.3$; level of education: sample: 14% low, 49% medium, 36% high; country population: 30% low, 40% medium, 28% high). A total of 91.8% of the participants owned a smartphone and 79.9% a tablet. Android and iOS were the most prevalent operating systems on their smartphones and tablets. Respondents had an average of 40 ($SD = 35.96$) mobile apps on their smartphone and/or tablet, including preinstalled apps, and they had downloaded, on average, two ($SD = 5.69$) apps during the last month. Most of the respondents indicated using apps every now and then (43.8%) or often (34.5%) on a normal day. Moreover, they estimated that they had spent, on average, 64 minutes ($SD = 80.64$) on apps the day before participating in the survey. Respondents had downloaded, on average, 6 ($SD = 2.38$) of the 12 selected apps for this study. Of these 12 apps, the most popular apps were WhatsApp (83.9%), Facebook (71.0%), Buienradar (69.8%), YouTube (62.9%), GoogleMaps (60.8%), and Gmail (53.8%).

TABLE 1
Mobile App Knowledge: Example Measures

Construct	Statistics	
Mobile App Knowledge WhatsApp ($n = 270$)[a]	% Correct	% False
1. WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other WhatsApp users.	*29.3*	70.7
2. WhatsApp may share information on your app usage with interested third parties to assist them in understanding the usage patterns of WhatsApp users.	*18.9*	**81.1**
3. All personal information you transfer to WhatsApp are transferred to the United States.	*13.3*	**86.7**
4. Contents of messages that have been delivered by the WhatsApp service are not copied, kept, or achieved by WhatsApp in the normal course of business.	*29.6*	70.4
5. Files that are sent through the WhatsApp service will reside on WhatsApp servers after delivery for a short period of time.	*37.8*	62.2
6. When I use WhatsApp, I see the same ads as someone else using WhatsApp.	37.8	*62.2*
7. WhatsApp is only allowed to gather and store information about my app use when I gave them the permission to do so.	12.2	*87.8*
8. It is punishable for companies like WhatsApp to store information about the mobile app use of individuals.	23.0	*77.0*

[a]Note: Statements were presented in random order. Italicized percentage is the correct answer. Boldface percentage shows statements respondents were most often mistaken about. The first five statements are adapted from the privacy policy of WhatsApp (http://www.whatsapp.com/legal; last modified July 7, 2012) and the last three statements from McDonald and Cranor (2010).

Measures

Inspired by McDonald and Cranor (2010) and Smit, van Noort, and Voorveld (2014), *mobile app knowledge* was measured using eight untrue/true/do not know statements of which three were incorrect. The correct items were developed based on the privacy policies of the 12 mobile apps selected for this study. To construct knowledge items that were as comparable as possible for all 12 apps, we extracted three statements concerning the information collected by the app and two statements regarding with whom the information is shared from each privacy policy. According to Luzak (2014) and Shade and Shepherd (2013), this is the most important information for Internet users. In case we could not select two statements regarding with whom information is shared, we included another statement on what the app is doing with the collected information. One example of the constructed knowledge statements is provided in Table 1. All other knowledge statements are provided upon

request. Correlational analyses were performed to test whether the eight items per app were related to each other. The correlation coefficients of the correct statements varied from .20 to .60, suggesting that the items could be associated with each other. As done by Smit, van Noort, and Voorveld (2014) and Park and Jang (2014), a general mobile app knowledge scale was constructed by assigning a "1" for correct answers and a "0" for incorrect and "do not know" answers. Mobile app knowledge varied from "0" (no knowledge) to "8" (high knowledge) with an average score of 2.91 ($SD = 2.20$).

Privacy concerns were measured with 6-Likert scale items (1 = *strongly disagree* and 7 = *strongly agree*) adopted from Xu et al. (2012), for instance, "I am concerned that mobile app X is collecting too much information about me." Scale items were averaged to form one single index for mobile privacy concerns, with higher scores representing higher levels of concern ($M = 3.88$, $SD = 1.35$, $\alpha = .90$).

Perceived vulnerability was measured with 5-Likert scale items (1 = *strongly disagree* and 7 = *strongly agree*) adapted from Mohamed and Ahmad (2012), for example, "I feel my personal information in mobile app X could be misused." Scale items were averaged to form one susceptibility index ($M = 3.98$, $SD = 1.35$, $\alpha = .93$).

Perceived self-efficacy was measured using a combined 6-item Likert scale (1 = *strongly disagree* and 7 = *strongly agree*) consisting of two protection self-efficacy items adapted from Mohamed and Ahmad (2012) and four privacy control items of Xu et al. (2008), for example, "I believe I have control over who can get access to my personal information collected by mobile app X." As this scale was not yet constructed by earlier research, principal component analysis (PCA) was conducted, which yielded one component (EV = 4.37; $R^2 = .73$). Therefore, the items were averaged ($M = 3.64$, $SD = 1.36$, $\alpha = .92$).

App attitude was measured with four items on a 7-point semantic differential scale adapted from Ajzen (2006). After the fragment "In general, how do you evaluate mobile app X?" respondents could, for instance, choose between "bad/good." Scale items were averaged to form one app attitude index ($M = 5.25$, $SD = 1.17$, $\alpha = .86$).

Response costs were measured by 3-Likert scale items (1 = *strongly disagree* and 7 = *strongly agree*) inspired by Lee, LaRose, and Rifon (2008), for instance, "Deleting or not downloading an app brings about too many disadvantages for myself." Scale items were averaged ($M = 3.75$, $SD = 1.41$, $\alpha = .75$).

Privacy protection motivation was measured with 3-Likert scale items (1 = *very unlikely* and 7 = *very likely*) inspired by Ajzen (2006), for

example, "Over the next two weeks, I intend to protect my privacy in apps by controlling access to my personal information using the privacy settings." The scale items were averaged to form a single privacy protection motivation scale ($M = 4.02$, $SD = 1.71$, $\alpha = .90$).

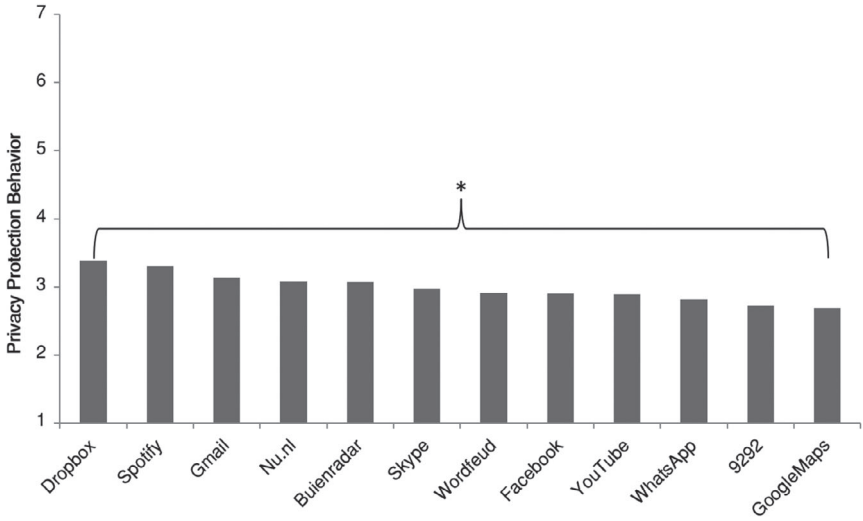
Privacy protection behavior was measured using six items borrowed from Park and Jang (2014). Respondents were asked to indicate on a 7-point Likert scale (1 = *not at all* and 7 = *all the time*) to what extent they perform several protection behaviors, for instance, "Read the privacy policy of mobile apps." Scale items were averaged to create one index for privacy protection behavior ($M = 2.95$, $SD = 1.35$, $\alpha = .80$).

Moreover, we measured a number of control variables to make sure that our findings were not distorted by other variables. First, we measured demographic characteristics such as age, gender, and education. Moreover, we included a variable measuring participants' prior experience with privacy infringement, because we expected that participants who had already been the victim of a privacy invasion, would report different results that participants who had not had such experiences. *Prior experience privacy infringement* was measured using 3-Likert scale items (1 = *not at all* and 7 = *all the time; do not know*) adapted from Xu et al. (2012), for instance, "How often have you personally been the victim of what you felt was an improper invasion of privacy?" *Do not know* answers were categorized as missing values, which were imputed using the series mean to avoid listwise deletion of the cases with missing values ($n = 76$ cases). Items were averaged to form one prior experience privacy infringement scale ($M = 2.97$, $SD = 1.41$, $\alpha = .69$).

Data Analysis

First, Pearson correlations were computed to examine the relationship between the constructs proposed in this study. Then, we tested with an ANOVA whether levels of protection motivation and behavior would differ among apps. Finally, hypotheses were tested using multiple regression analyses. More specifically, the variables protection motivation and protection behavior were regressed in two separate regression analyses upon participants' background characteristics (gender, age, education, prior experience privacy infringement) and the theoretical protection determinants central in this study. These analyses allowed us to test for associations between mobile app knowledge, privacy concerns, perceived vulnerability, perceived self-efficacy, app attitude, response costs, and protection motivation and behavior while controlling for participants' background characteristics.

FIGURE 2
Privacy Protection Behavior Per App



Note: ANOVA comparisons showed that the Dropbox app ($M = 3.39$, $SD = 1.47$) differed significantly from the GoogleMaps app ($M = 2.69$, $SD = 1.23$), $F(11, 1{,}578) = 2.45$, $p < .01$, $\eta^2 = .02$. WhatsApp ($n = 270$), Facebook ($n = 240$), Buienradar ($n = 190$), GoogleMaps ($n = 173$), Gmail ($n = 156$), YouTube ($n = 147$), Nu.nl ($n = 109$), Skype ($n = 77$), Wordfeud ($n = 65$), Dropbox ($n = 64$), 9,292.nl ($n = 62$), Spotify ($n = 40$).

RESULTS

ANOVA analyses showed that levels of protection motivation did not differ among apps, $F_{\text{motivation}}(11,\ 1581) = 1.18$, $p = .30$. However, there were small significant differences between apps with regard to protection behavior, $F_{\text{behavior}}(11,\ 1581) = 2.46$, $p < .01$, $\eta^2 = .02$. As can be seen in Figure 2, there was a significant difference between the Dropbox and the GoogleMaps app. Participants' protection behavior was higher for the Dropbox app ($M = 3.39$, $SD = 1.47$) and lower for the GoogleMaps app ($M = 2.69$, $SD = 1.23$). However, as the effect size of this difference was very small ($\eta^2 = .02$), we did not analyze our data for each app separately.

Descriptive statistics suggested that participants' knowledge regarding the data collection and usage practices of mobile apps is limited ($M = 2.93$, $SD = 2.19$, range 0–8). Participants also experienced moderate levels (all variables measured on a 7-point scale) of perceived vulnerability ($M = 3.98$, $SD = 1.35$), perceived self-efficacy ($M = 3.64$, $SD = 1.36$), response costs ($M = 3.75$, $SD = 1.41$), and privacy concerns ($M = 3.89$, $SD = 1.35$). Moreover, participants reported a positive app

TABLE 2
Correlation Matrix

Variable	1	2	3	4	5	6	7	8
1. Knowledge	1							
2. Vulnerability	.20**	1						
3. Self-efficacy	−.17**	−.17**	1					
4. App attitude	−.14**	−.09**	.13**	1				
5. Response costs	.08**	.19**	−.18**	−.01	1			
6. Privacy concerns	.22**	.51**	−.14**	−.05*	.21**	1		
7. Protection motivation	−.10**	.25**	.16**	.04	.04	.28**	1	
8. Protection behavior	.01	.16**	.15**	−.06*	.01	.20**	.40**	1

Note: *Correlation is significant at the 0.05 level (two-tailed). **Correlation is significant at the 0.01 level (two-tailed).

attitude ($M = 5.25$, $SD = 1.17$). Finally, they reported moderate levels of protection motivation ($M = 4.02$, $SD = 1.71$) and rather low levels of privacy protection behavior ($M = 2.95$, $SD = 1.35$). Table 2 shows Pearson correlations between all variables.

Results of the two multiple regression models are presented in Table 3. The regression model with protection motivation as dependent variable was significant, $F(10, 1{,}582) = 36.80$, $p < .001$, and it explained 19% of the variance in protection motivation. Moreover, the regression model with protection behavior as dependent variable was significant, $F(10, 1{,}582) = 27.27$, $p < .001$, and it explained 15% of the variance in protection behavior. Contrary to our expectations, knowledge was negatively related to protection motivation ($\beta = -.14$, $p < .001$) and behavior ($\beta = -.08$, $p < .01$), hence H1 was not supported. Thus, the more app users know about the data collection and usage practices of mobile apps, the less their privacy protection motivation and behavior seems to be.

As proposed in H2, privacy concerns were positively related to protection motivation ($\beta = .22$, $p < .001$) and behavior ($\beta = .16$, $p < .001$), suggesting that as app users' concern about their privacy increases, they seem to be more motivated to engage in privacy protection and they do more to protect their privacy.

Moreover, as proposed in H3, perceived vulnerability was positively related to protection motivation ($\beta = .17$, $p < .001$) and behavior ($\beta = .06$, $p < .05$), supporting H3. This means that as app users believe that their chance of being a victim of a mobile privacy invasion increases, they are more likely to adopt measures to eliminate or reduce the harmful effects of mobile privacy invasions.

As predicted in H4, perceived self-efficacy was positively related to protection motivation ($\beta = .20$, $p < .001$) and behavior ($\beta = .20$, $p < .001$).

TABLE 3
Multiple Regression Analyses Predicting Protection Motivation and Behavior

	Protection Motivation, β	Protection Behavior, β	Hypothesis
Background characteristics			
Gender	.04	.01	
Age	$.10^{***}$	$-.10^{***}$	
Education	$-.05^{*}$	−.03	
Prior privacy infringement	$.10^{***}$	$.25^{***}$	
PMT determinants			
H1: Knowledge	$-.14^{***}$	$-.08^{**}$	Rejected
H2: Privacy concern	$.22^{***}$	$.16^{***}$	Confirmed
H3: Vulnerability	$.17^{***}$	.06 ∗	Confirmed
H4: Self-efficacy	$.20^{***}$	$.20^{***}$	Confirmed
H5: App attitude	.02	$-.05^{*}$	Partly confirmed
H6: Response costs	.00	$-.05^{*}$	Partly confirmed
R^2	.19	.15	

Note: All entries are standardized regression coefficients.
$^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

This suggests that as app users' believe in their ability to protect themselves from mobile privacy invasions, they seem to be more motivated to engage in privacy protection and they do more to protect their privacy.

Partly confirming H5, there was no relationship between attitude and protection motivation ($\beta = .02$, $p = .42$), but a small negative relationship between attitude and protection behavior ($\beta = -.05$, $p < .05$). This suggests that the more app users like the app, the less they engage in privacy protection behavior.

Partly confirming H6, there was no relationship between response costs and protection motivation ($\beta = .00$, $p = .89$) but a small negative relationship between response costs and protection behavior ($\beta = -.05$, $p < .05$). This suggests that higher response costs are negatively related to protection behavior.

Finally, examining participants' background characteristics, the analysis revealed a positive relationship between participants' prior experience of privacy infringement and their protection motivation ($\beta = .10$, $p < .001$) and behavior ($\beta = .25$, $p < .001$). The more privacy infringement participants had experienced before, the higher their protection motivation and behavior was. Interestingly, we also found a positive association between age and protection motivation ($\beta = .10$, $p < .001$) but a negative association between age and protection behavior ($\beta = -.10$, $p < .001$). Hence, older people seem to be more motivated to protect their privacy in apps; however, they engage in less protection behavior. Finally, there was a negative relation between education and protection motivation ($\beta = -.05$, $p < .05$),

suggesting that higher educated people seem to be less motivated to protect their privacy.

CONCLUSION AND DISCUSSION

This study investigated mobile app users' current privacy protection behavior as well as the factors that motivate it. Results confirmed that the application of PMT in the context of mobile app privacy could be a promising theoretical framework for understanding privacy protection in apps. Consistent with PMT and earlier research on Internet users, we found that mobile app users' perceived vulnerability, self-efficacy, and privacy concerns were positively related to protection motivation and behavior (Boehmer et al. 2015; Lee, LaRose, and Rifon 2008; Milne, Labrecque, and Cromer 2009). This means that app users are more likely to engage in protection behavior if they feel vulnerable, concerned, and think that they are able to protect themselves from the data collection and usage practices of apps. Earlier studies that have used PMT as a theoretical framework (Boehmer et al. 2015; Lee, LaRose, and Rifon 2008; Milne, Labrecque, and Cromer 2009; Youn 2009) mainly focused on the general Internet context. Our study shows that PMT, and our extension of it, APPM, can also be used to tap into the mechanisms that explain protection motivation and behavior in the mobile app context. As such, the study represents a solid point of departure for future research investigating app privacy protection behavior in more detail.

Interestingly, although contrary to our expectations, higher levels of knowledge about the data collection and usage practices of mobile apps were not associated with more, but less protection motivation and behavior. One possible explanation is that app users with higher levels of knowledge simply have given up to protect their privacy, because they know that it is very difficult to tackle the threat. According to the extended parallel process model (EPPM) (Witte 1992), which is an extension of PMT, when individuals perceive a threat to be high, but efficacy to be low, they initiate a fear control process. In this process, the fear that has been evoked by the threat becomes intensified, because individuals believe that they are unable to effectively respond to the threat. As a result, individuals start to cope with the fear, for instance, by engaging in maladaptive responses (e.g., denial). The latter might explain the low protection motivation and behavior levels.

Contrary to our expectations, we also did not find a significant negative relationship between response costs and protection motivation but a small negative association between response costs and behavior, which has only little explanatory power. An explanation for this might be that the negative

consequences of safe behavior may not be that salient in the study's population. As our study demonstrated, overall, mobile app users' level of perceived self-efficacy is relatively low. This suggests that app users do not know how to protect their privacy in apps, which would explain, why they could not evaluate the response costs of protective behavior. If app users think that they are not able to engage in the protective behavior, it is, of course, difficult for them to evaluate the costs of it. Additional correlational analyses indeed show that self-efficacy and response costs are negatively correlated ($r = -.18$, $p < .001$).

Finally, contrary to our expectations, app attitude had only a small negative association with protection motivation, which has only little explanatory power. One explanation for this weak association might lie in our operationalization of the PMT construct benefits. We decided to measure the construct benefits by measuring app users' attitude toward the app, because we thought that this would be the only way to create one valence scale that is applicable to the 12 different apps we focused on in this study. If we had measured benefits in terms of different gratifications per app, it would have been impossible to create one benefits scale that applies to all apps. It might be that we simply did not capture the concept of benefits completely, which is why we do not find stronger associations. Future research should test to what extent another operationalization of the benefits construct yields the expected association.

Moreover, we found a positive relationship between age and protection motivation and a negative relationship between age and protection behavior. It seems as if older people would be more motivated to protect their privacy; however, they engage in less protection behavior. A reason for this conflicting finding might be that these people are concerned about their privacy and would also like to protect it; however, they simply do not know how to protect themselves. Thus, these people seem to have some kind of knowledge on the data collection practices of apps, but they do not have enough knowledge on *how* to tackle these practices.

Limitations and Future Research

Investigating current levels of privacy protection motivation and behavior in the mobile app context is very important, given that apps become more and more ingrained in our everyday lives. Such an investigation is, however, difficult and we, therefore, need to consider some limitations of our study, which call for future research. First of all, the surveyed sample only contained participants from one Western European country. More

international research is needed to validate our finding in other countries with other privacy regulations.

Second, we measured privacy protection behavior using self-report questions, which are always prone for socially desirable answers. Ideally, future research focuses on actual protection behavior, for instance, by tracking app users' behavior in apps. Apart from that, future research may want to investigate what the balance of the factors motivating protection behavior needs to look like so that app users really start protecting their privacy. A first step would be to investigate which trade-off app users make when deciding (not) to protect their privacy. Researchers might, for instance, want to conduct a conjoint experiment, which is able to separate an overall protection motivation judgment into several components. This separation, in turn, may provide valuable information on the relative importance of the distinct protection motivation determinants.

Third, it is necessary to note that the selection of apps focused on in this study might have had consequences for the results of this study. Participants of this study answered survey questions on apps they had already downloaded on their smartphone or tablet. This means that they had already made their privacy decision when they answered the survey questions, which is why the risks associated with the download were probably less salient among our participants. This might, for instance, explain the low privacy concerns and vulnerability levels. Moreover, due to the fact that participant had already downloaded the app in question, it might be that they experienced cognitive dissonance while answering our survey questions, which might have caused a positivity bias in our results. Future research might want to focus on a different, nonretrospective phase in the app downloading process to get more insights into privacy protection motivation and behavior. One could, for instance, let mobile app users download a fictive app and assess their protection motivation and behavior in the meantime by using tracking software and after the download by using self-report questions.

Fourth, this study focused only on mobile app users' objective knowledge. Prior research, however, has highlighted the importance of subjective knowledge rather than objective knowledge: A study by Nabi, Roskos-Ewoldsen, and Carpentier (2008) has demonstrated that individuals higher in perceived knowledge engage in more protective behavior (i.e., performing a testicular self-exam) than those low in perceived knowledge. Based on this evidence, future research should also focus on measuring app users' subjective knowledge to fully understand the impact of knowledge on protection behavior in the mobile app context.

Fifth, this study did not measure the PMT construct response efficacy. There are a few actions currently available to consumers to protect their privacy but these response options are very limited and not commonly used. To avoid ecological and internal validity issues, we did not ask users about these options. However, we acknowledge that neglecting the few response options that do exist is a limitation of this study. To get a better understanding of the factors that motivate privacy protection in the mobile app context, future research should, therefore, take into account the limited response options that are currently available to consumers (e.g., tools/apps to restrict the personal information disclosure in apps).

Theoretical and Practical Implications

Despite these limitations, the findings of this study have important theoretical and practical implications. Theoretically, our study contributes to existing online security literature, as it is, to our knowledge, the first to apply PMT in the mobile app context. As our results show, this was a fruitful application, because in line with earlier findings (e.g., Boehmer et al. 2015; Lee, LaRose, and Rifon 2008; Youn 2009) we find that mobile app users' perceived vulnerability, self-efficacy, and privacy concerns were positively related to protection motivation and behavior. Of these variables, the variable self-efficacy plays the most important role, because it has the strongest relationship with protection motivation and behavior. This is in line with earlier research, which demonstrated that self-efficacy has the most consistent impact on the enactment of safe behaviors and that it is the strongest predictor of online safe behaviors (Boehmer et al. 2015; Lee, LaRose, and Rifon 2008).

Additionally, this study contributes to the growing body of literature using PMT to examine privacy behavior in the mobile app context (Boehmer et al. 2015; Milne, Labrecque, and Cromer 2009) by showing the need for including the concept *knowledge* as an extra PMT variable. While knowledge is negatively associated with protection motivation and behavior, privacy concerns are positively associated with these outcome variables. It becomes clear, that in order to fully grasp mobile app users protection motivation and behavior, it is necessary to investigate the concept of knowledge, too. Thus, this study does not only extend PMT and make it more applicable to the mobile app context, but it also offers a more nuanced theoretical understanding of the factors that motivate app users to protect their privacy.

Practically, our study shows that mobile app users' knowledge on the data collection practices of mobile apps is currently limited. Obviously,

the current informed consent regulations do not seem to reach their aims, because app users barely have knowledge about the magnitude of the data collection and usage practices of apps and they are not really concerned about them. Without knowledge on the data collection practices of mobile apps, it is very difficult for users to arm themselves against these practices. Hence, they seem to be at the mercy of app providers and advertisers, and they do not see a way to protect their privacy, nor are they aware of the threats they are actually facing. However, our results also bring about potential ways to empower mobile app users. As our findings imply, it might be valuable to increase app users perceived self-efficacy, vulnerability, and privacy concern beliefs, as these are likely to increase privacy protection motivation. Based on this, policymakers should concentrate their efforts on (1) increasing mobile app users' awareness of potential privacy threats and (2) their belief that they can, in fact, protect their mobile privacy. In that regard, awareness creation should go beyond just informing consumers about the data collection practices of apps, for instance, by using privacy policies. This approach has been repeatedly proven ineffective (Liu 2014; Milne and Culnan 2004; Shklovski et al. 2014). Instead, policymakers might want to create awareness for the *concrete negative consequences* of the data collection and usage practices of apps (e.g., discrimination in buying situations, identity theft, fraud) by stimulating a public debate about the topic using mainstream media. In the Netherlands, for instance, a public TV channel recently broadcasted a successful privacy special, in which professionals uncovered how easy it is to access personal data (e.g., passwords, auto-fill forms) on mobile devices and how this information may be misused by others (NPO 2016). Using this way of informing consumers about the potential privacy threats caused by the data collection and usage practices of apps is probably more effective in creating awareness than the best privacy policy. Additionally, these kinds of programs may also help to increase consumers' belief that they can protect their privacy, which seems to play a very important role according to our findings. By offering consumers easy and concrete tools to restrict personal information disclosure via apps, as done in the NPO privacy special, consumers may feel savvier and less helpless, which might reduce privacy threatening behavior.

Although consumers might feel helpless when it comes to protecting their privacy, there are still some steps they can take. First and foremost, consumers can actively inform themselves about the data collection and usage practices of mobile apps and their consequences on educational Web sites, such as the Dutch Web site http://www.veiliginternetten.nl (translated: safely surfing on the Internet). This Web site creates awareness

for the different types of information apps usually want to access on mobile devices, it briefly discusses the pros and cons of each information access, and it stimulates consumers to read the privacy policy and to assess whether they find the information access acceptable or not. Second, app users could consider using alternative apps that offer the same service but access less personal information. The messaging service "Threema," for instance, offers a similar service as the popular messaging app "WhatsApp," but, in contrast to WhatsApp, Threema actively prevents the collection of meta data, thereby guaranteeing privacy (Threema 2018).

In sum, this study adds to the mobile app literature, as it is the first to examine the factors that motivate privacy protection in mobile apps. Results show that while increased levels of perceived self-efficacy, vulnerability, and privacy concern enhance mobile app users' motivation to engage in risk-reducing behavior, higher levels of knowledge of the data collection practices of mobile apps, app attitude, and perceived response costs diminish it. We can conclude that app users are unwittingly and defenselessly in the spotlight at the moment but once they start worrying about their privacy and feel able to protect it, the tables may turn.

REFERENCES

Acquisti, Alessandro and Jens Grossklags. 2005. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy Magazine*, 3 (1): 26–33. https://doi.org/10.1109/msp.2005.22.

Acquisti, Alessandro and Jens Grossklags. 2007. What Can Behavioral Economics Teach Us about Privacy. *Digital Privacy: Theory, Technologies and Practices*, 18: 363–377. https://doi.org/10.1201/9781420052183.ch18.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. What Is Privacy Worth? *The Journal of Legal Studies*, 42 (2): 249–274. https://doi.org/10.1086/671754.

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, and Martin Wetzels. 2015. Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, 91 (1): 34–49. https://doi.org/10.1016/j.jretai.2014.09.005.

Ajzen, Icek. 2006. Constructing a TpB Questionnaire: Conceptual and Methodological Considerations. http://www.unibielefeld.de/ikg/zick/ajzenconstruction a tpb questionnaire.pdf.

Altman, Irwin. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole.

Arachchilage, Nalin Asanka Gamagedara and Steve Love. 2014. Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior*, 38: 304–312. https://doi.org/10.1016/j.chb.2014.05.046.

Ashworth, Laurence and Clinton Free. 2006. Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics*, 67 (2): 107–123. http://www.jstor.org/stable/25123858.

Ball, Kirstie and Frank Webster. 2003. *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Era*. London: Pluto Press.

Bauman, Zygmunt and David Lyon. 2013. *Liquid Surveillance: A Conversation*. Cambridge, UK: John Wiley & Sons.

Bettini, Claudio and Daniele Riboni. 2015. Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges. *Pervasive and Mobile Computing*, 17: 159–174. https://doi.org/10.1016/j.pmcj.2014.09.010.

Boehmer, Jan, Robert LaRose, Nora Rifon, Saleem Alhabash, and Shelia Cotten. 2015. Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students. *Behaviour & Information Technology*, 34 (10): 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448.

Buck, Christoph, Chris Horbel, Tim Kessler, and Claas Christian. 2014. Mobile Consumer Apps: Big Data Brother Is Watching You. *Marketing Review St.Gallen*, 31 (1): 26–35. https://doi.org/10.1365/s11621-014-0318-2.

Centraal Bureau voor de Statistiek (CBS). 2015. Bevolking; Kerncijfers [Country Population; Core Statistics]. http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,%28l-1%29,l&HD=130605-0924&HDR=G1&STB=T.

Chen, Hsuan-Ting and Wenhong Chen. 2015. Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking*, 18 (1): 13–19. https://doi.org/10.1089/cyber.2014.0456.

Cho, Hichang, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. A Multinational Study on Online Privacy: Global Concerns and Local Responses. *New Media & Society*, 11 (3): 395–416. https://doi.org/10.1177/1461444808101618.

Esposti, Sara Degli. 2014. When Big Data Meets Dataveillance: The Hidden Side of Analytics. *Surveillance & Society*, 12 (2): 209–225. https://search.proquest.com/docview/1547988838?pq-origsite=gscholar.

EU Data Protection Directive. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Official Journal of the European Communities*, 38 (281): 31–50. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

EU ePrivacy Directive. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). *Official Journal of the European Communities*, 201: 37–47. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.

European Commission. 2011. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. https://data.europa.eu/euodp/en/data/dataset/S864_74_3_EBS359.

European Commission. 2018. Protection of Personal Data 2018. http://ec.europa.eu/justice/data-protection/.

Federal Trade Commission. 2013. Mobile Privacy Disclosures: Building Trust through Transparency. www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

Felt, Adrienne Porter, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security Article No. 3*. Washington, DC: ACM. https://doi.org/10.1145/2335356.2335360.

Fife, Elizabeth and Juan Orjuela. 2012. The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security. *International Journal of Engineering Business Management*, 4: 1–10. https://doi.org/10.5772/51645.

Good, Nathaniel, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw, Deirdre Mulligan, and Joseph Konstan. 2005. Stopping Spyware at the Gate. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (43–52). Pittsburgh, PA: ACM. https://doi.org/10.1145/1073001.1073006.

Hu, Qing and Tamara Dinev. 2005. Is Spyware an Internet Nuisance or Public Menace? *Communications of the ACM*, 48 (8): 61–66. https://doi.org/10.1145/1076211.1076241.

Ifinedo, Princely. 2012. Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31 (1): 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

IMCO. 2011. Consumer Behaviour in a Digital Environment. Study. http://www.europarl.europa.eu/document/activities/cont/201108/20110825ATT25258/20110825ATT25258EN.pdf.

Keith, Mark J., Samuel C. Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior. *International Journal of Human-Computer Studies*, 71 (12): 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016.

Lee, Doohwang, Robert LaRose, and Nora Rifon. 2008. Keeping Oour Network Safe: A Model of Online Protection Behaviour. *Behaviour & Information Technology*, 27 (5): 445–454. https://doi.org/10.1080/01449290600879344.

LeFebvre, Rebecca. 2012. The Human Element in Cyber Security: A Study on Student Motivation to Act. In *Proceedings of the 2012 Information Security Curriculum Development Conference* (1–8). Kennesaw, GA: ACM. https://doi.org/10.1145/2390317.2390318.

Li, Han, Rathindra Sarathy, and Heng Xu. 2010. Understanding Situational Online Information Disclosure as a Privacy Calculus. *Journal of Computer Information Systems*, 51 (1): 62–71. http://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=54525529&site=ehost-live.

Lin, Jialiu, Norman Sadeh, Shahriyar Amini, Janne Lindqvist, Jason I. Hong, and Joy Zhang. 2012. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (501–510). Pittsburgh, PA: ACM. https://doi.org/10.1145/2370216.2370290.

Liu, Yue. 2014. User Control of Personal Information Concerning Mobile-App: Notice and Consent? *Computer Law & Security Review*, 30 (5): 521–529. https://doi.org/10.1016/j.clsr.2014.07.008.

Luzak, Joasia. 2014. Privacy Notice for Dummies? Towards European Guidelines on How to Give 'Clear and Comprehensive Information' on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy. *Journal of Consumer Policy*, 37 (4): 547–559. https://doi.org/10.1007/s10603-014-9263-3.

McDonald, Aleecia M. and Lorrie Faith Cranor. 2010. Americans' Attitudes about Internet Behavioral Advertising Practices. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (63–72). Chicago, IL: ACM. https://doi.org/10.1145/1866919.1866929.

Milne, George R. and Mary J. Culnan. 2004. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing*, 18 (3): 15–29. https://doi.org/10.1002/dir.20009.

Milne, George R., Lauren I. Labrecque, and Cory Cromer. 2009. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43 (3): 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x.

Mohamed, Norshidah and Ili Hawa Ahmad. 2012. Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia. *Computers in Human Behavior*, 28 (6): 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008.

Morman, Mark T. 2000. The Influence of Fear Appeals, Message Design, and Masculinity on Men's Motivation to Perform the Testicular Self-Exam. *Journal of Applied Communication Research*, 28 (2): 91–116. https://doi.org/10.1080/00909880009365558.

Nabi, Robin L., David Roskos-Ewoldsen, and Francesca Dillman Carpentier. 2008. Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. *Health Communication*, 23 (2): 191–201. https://doi.org/10.1080/10410230701808327.

Narayanan, Meyyappan, Bonwoo Koo, and Brian Paul Cozzarin. 2012. Fear of Fraud and Internet Purchasing. *Applied Economics Letters*, 19 (16): 1615–1619. https://doi.org/10.1080/13504851.2011.648313.

NPO. 2016. Jongeren Vertrouwen Facebook En Google Niet [Young People Don't Trust Facebook and Google]. http://jij.eenvandaag.nl/uitslagen/69830/jongeren_vertrouwen_facebook_en_google_niet.

Park, Yong J. 2011. Digital Literacy and Privacy Behavior Online. *Communication Research*, 40 (2): 215–236. https://doi.org/10.1177/0093650211418338.

Park, Yong J. and Seung Mo Jang. 2014. Understanding Privacy Knowledge and Skill in Mobile Communication. *Computers in Human Behavior*, 38: 296–303. https://doi.org/10.1016/j.chb.2014.05.041.

Perlroth, Nicole, and Nick Bilton. 2012. Mobile Apps Take Data without Permission. *The New York Times*, February 15. https://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/.

Reyns, Bradford W. 2013. Online Routines and Identity Theft Victimization. *Journal of Research in Crime and Delinquency*, 50 (2): 216–238. https://doi.org/10.1177/0022427811425539.

Rogers, Ronald W. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91 (1): 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Rogers, Ronald W. 1983. Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In *Social Psychophysiology: A Sourcebook*. Social Psychophysiology, edited by John T. Cacioppo and Richard Petty (153–176). New York, NY: Guilford.

Shade, Leslie R. and Tamara Shepherd. 2013. Viewing Youth and Mobile Privacy through a Digital Policy Literacy Framework. *First Monday*, 18 (12). https://doi.org/10.5210/fm.v18i12.4807.

Shillair, Ruth, Shelia R. Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J. Rifon. 2015. Online Safety Begins with You and Me: Convincing Internet Users to Protect Themselves. *Computers in Human Behavior*, 48: 199–207. https://doi.org/10.1016/j.chb.2015.01.046.

Shklovski, Irina, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems* (2347–2356). Seoul: ACM. https://doi.org/10.1145/2556288.2557421.

Sipior, Janice C., Burke T. Ward, and Linda Volonino. 2014. Privacy Concerns Associated with Smartphone Use. *Journal of Internet Commerce*, 13 (3–4): 177–193. https://doi.org/10.1080/15332861.2014.947902.

Smit, Edith G., Guda van Noort, and Hilde A.M. Voorveld. 2014. Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe. *Computers in Human Behavior*, 32: 15–22. https://doi.org/10.1016/j.chb.2013.11.008.

So, Jiyeon. 2013. A Further Extension of the Extended Parallel Process Model (E-EPPM): Implications of Cognitive Appraisal Theory of Emotion and Dispositional Coping Style. *Health Communication*, 28 (1): 72–83. https://doi.org/10.1080/10410236.2012.708633.

Statista. 2017. Number of Apps Available in Leading App Stores as of March 2017. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Wei Phang Chee. 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, 37 (4): 1141–1164. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=91906295&site=ehost-live.

Threema. 2018. Threema Rigorously Protects Your Privacy. https://threema.ch/en/.

Thurm, Scott, and Yukari I. Kane. 2010. What They Know: Your Apps Are Watching You. *The Wall Street Journal*, December 17. http://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

TRUSTe. 2014. TRUSTe Privacy Index. 2014 Consumer Confidence Edition. https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2014/.

van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society*, 12 (2): 197–208. https://search.proquest.com/docview/1547988865?pq-origsite=gscholar.

Vishwanath, Arun and Hao Chen. 2008. Personal Communication Technologies as an Extension of the Self: A Cross-Cultural Comparison of People's Associations with Technology and Their Symbolic

Proximity with Others. *Journal of the Association for Information Science and Technology*, 59 (11): 1761–1775. https://doi.org/10.1002/asi.20892.

Wirtz, Jochen, May O. Lwin, and Jerome D. Williams. 2007. Causes and Consequences of Consumer Online Privacy Concern. *International Journal of Service Industry Management*, 18 (4): 326–348. https://doi.org/10.1108/09564230710778128.

Witte, Kim. 1992. Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59 (4): 329–349. http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=9301100383&site=ehost-live.

Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart. 2008. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. In *Proceedings of the 29th International Conference on Information Systems (ICIS) Paper 6*. Paris: AISeL. http://aisel.aisnet.org/icis2008/6.

Xu, Heng, Sumeet Gupta, Mary Beth Rosson, and John M. Carroll. 2012. Measuring Mobile Users' Concerns for Information Privacy. In *Proceedings of the 33rd International Conference on Information Systems (ICIS) Paper 10*. Orlando, FL: AISeL. http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10/.

Youn, Seounmi. 2009. Determinants of Online Privacy Concern and its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*, 43 (3): 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x.

Zuiderveen Borgesius, Frederik J. 2013. Behavioral Targeting: A European Legal Perspective. *IEEE Security & Privacy*, 11 (1): 82–85. https://doi.org/10.1109/msp.2013.5.