The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns

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

DOI
10.1016/j.dss.2017.12.003

Publication date
2018

Document Version
Final published version

Published in
Decision support systems

Decision Support Systems 106 (2018) 44–52

Contents lists available at ScienceDirect

Decision Support Systems

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

The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns

Verena M. Wottrich *, Eva A. van Reijmersdal, Edith G. Smit

Amsterdam School of Communication Research, ASCoR, University of Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 20 June 2017
Received in revised form 18 October 2017
Accepted 3 December 2017
Available online 6 December 2017

Keywords:
Mobile apps
Privacy trade-off
Privacy calculus
Decision-making
App permission requests

ABSTRACT

Today, mobile app users regularly "pay" for various mobile services, such as social networking or entertainment apps, by accepting app permission requests, thereby sharing personal data with apps. Privacy calculus theory has established that individuals disclose personal information based on a cost-benefit trade-off. In the mobile app context, however, this notion needs more support, because existing studies have only *measured* costs and benefits or *forced* a trade-off. Conducting two online experiments among Western European app users ($N_1 = 183$; $N_2 = 687$), this study replicates earlier findings and provides more-profound insights into the boundary conditions of the privacy calculus by showing that app value (i.e., benefits) trumps the costs (i.e., intrusiveness, privacy concerns) in the privacy trade-off.

1. Introduction

During the past few years, personal data have become *the* currency for mobile app users to pay for various mobile services, such as social networking, messaging, or entertainment apps [1–3]. Instead of paying for an app with "real" money, app users often (unwittingly) reimburse app developers by accepting their permission request, that is, an app's demand to control the mobile device and to access and use the personal information stored in the device [4]. By accepting permission requests, app users often share personal information with an app, such as their device ID, call log information, or address book contacts [5,6]. This might impose a threat to app users' privacy, because the shared information can be used to discriminate users in buying situations [56], to approach them with unwanted commercial solicitations [57], or for fraudulent behaviors, such as identity theft [58]. Thus, the decision to download an app might be risky. Therefore, it may be beneficial for app users to carefully consider the costs and benefits associated with the app download.

So far, the industry as well as prior research has predominantly considered privacy-related decision-making as a rational process in which consumers base their decision to share personal information on a careful analysis of the costs and benefits associated with the information trade [7–9]. This so-called *privacy trade-off* has been investigated in various contexts, including e-commerce [9], social network sites (SNS) [10], and mobile applications [11]. These studies, however, are vulnerable to criticism. Some of them only *measured* the concepts of costs and benefits, which makes drawing *causal* inferences regarding the privacy trade-off impossible [10–12]. Others *manipulated* the costs and benefits, but the experimental design of these studies *forced* participants to make a trade-off (e.g., [13]); hence, it is only logical that they also found it. It is therefore not enough to rely on earlier studies investigating the privacy trade-off in other contexts (e.g., [9]) to fully understand consumers' privacy decision-making process in the mobile app context.

Apart from that, there is a growing body of literature that criticizes the assumption of rationality in privacy decision-making (e.g., [14–16]). This stream of research states that even if individuals have access to comprehensive information on privacy risks and protection possibilities, they might not be able to process this information to formulate rational privacy-sensitive decisions [14]. Human rationality is bounded, which limits our ability to acquire and apply information [17]. Considering the limitations of earlier privacy trade-off studies as well as the emerging notion of bounded rationality in privacy decision-making, the question remains: do consumers engage in a privacy trade-off?

This study aims to shed light on this question by focusing on the mobile app context in particular, because mobile devices have become extensions of the self [18] and "are typically personal to an individual, almost always on, and with the user" ([19], p. 2). More than other types of digital devices, such as personal computers, 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" ([19], p. 2). Consequently, mobile devices may jeopardize consumer privacy more than

* Corresponding author at: Amsterdam School of Communication Research, University of Amsterdam, P.O. Box 15793, 1001 NG Amsterdam, The Netherlands.
E-mail address: v.m.wottrich@uva.nl (V.M. Wottrich).

https://doi.org/10.1016/j.dss.2017.12.003
0167-9236/

other digital devices, which is why an independent study of the privacy trade-off in the mobile app context is necessary. More specifically, we focus on app permission requests in the app download stage, because the download stage can be considered as "the first layer of defense against privacy invasive apps" ([4], p. 20).

In sum, this study seeks to answer the following research question: *Under which conditions do app users engage in a privacy trade-off when accepting app permission requests in the app download stage?*

Drawing on privacy calculus theory [8,9], we investigate the effects of users' *app intrusiveness* and *app value* perceptions on their intention to disclose personal information. In addition, we examine how these two factors interact with *privacy concerns*. Conducting two online experiments among app users in a Western European country ($N_1 = 183$; $N_2 = 687$), this study offers two substantive contributions. Theoretically, this study confirms the generalizability of the privacy calculus in the mobile app context, and it is the first to investigate the joint effects of app value, app intrusiveness, and privacy concerns on information disclosure intention. Therefore, it extends existing literature on the privacy calculus, in general, and on privacy decisions in the mobile app context, more specifically. Practically, this study offers valuable insights for policy makers into whether app users are currently empowered enough to make well-considered privacy decisions when downloading apps. Moreover, the knowledge gained from this study might be useful for app developers because it sheds more light on the conditions under which app users accept an app's terms of use.

2. Theoretical background

2.1. Accepting app permission requests: a privacy trade-off?

As a result of the advancements in information technology during the past few years, the collection and usage of personal data has become almost invisible to consumers [1,20]. In the mobile app context, for instance, consumers often unwittingly disclose personal information, such as their device ID, call log information, or address book contacts, by accepting an app's permission request – a necessary step for being able to download apps in the first place ([5,6]).

Whether app users intend to accept app permission requests depends on several factors. According to the theory of reasoned action (TRA) [21] and its later revision, the theory of planned behavior (TPB) [22], one of the most important factors driving behavioral intentions is an individual's belief and evaluation of the outcome of a behavior (i.e., behavioral beliefs). Translating this to the mobile app context, this means that an app user's belief about the consequences of accepting an app's permission request may determine his or her intention to do so. The TPB has already proven to be successful for predicting online safety behavior in the general Internet context [23]. It is therefore used in this study to understand privacy behavior in the mobile app context.

App users may experience contrary beliefs when considering the download of an app [24]. On the one hand, they can become aware of the potential risks to privacy associated with the download. On the other hand, they may think about the potential benefits, such as "staying connected" [25], that might come with a download. Either way, these contrary beliefs can exist at the same time, and they can, in conjunction, influence an app users' decision to accept an app's permission request, thereby sharing personal information with the app.

In fact, multiple studies have assumed that individuals base their decision to share information on a rational cost-benefit trade-off (e.g., [1, 11]). Privacy calculus theory (PCT) [8,9] is one of the most commonly used theories to study the joint effect of opposing forces, such as costs and benefits, on privacy behaviors [26]. The theory suggests that people base their intention to disclose personal information on a privacy calculus, in which they weigh potentially competing factors, such as the costs and benefits of a trade, in light of possible outcomes, trying to maximize the positive and minimize the negative outcomes [8,9,26,27]. This sort of trade-off also seems to take place in the mobile app context: In a study by Eling et al. [24], for example, respondents reported weighing the perceived value of an app against the privacy intrusion caused by granting the app's permissions. In addition, Keith et al. [11] demonstrated that perceived privacy risk negatively affects app users' intent to disclose, while perceived benefit increases it. Moreover, a study by Kehr et al. [28] showed that a situation-specific evaluation of risks and benefits mediated the effect of information sensitivity and affect on information disclosure in apps. Although the studies of Eling et al. [24], Keith et al. [11], and Kehr et al. [28] point toward the presence of a cost-benefit trade-off when disclosing information via apps, they do not shed light on the conditions under which this trade-off takes place. Moreover, these studies only *measured* the costs and benefits, making it difficult to draw causal inferences. Other studies in the general Internet context, such as that conducted by Hann et al. [13], *manipulated* costs and benefits, but their experimental design forced participants to make a trade-off, which might explain why they found one. Considering these shortcomings and that earlier research has indicated that consumers do not always act as rationally as expected when it comes to privacy [14,20], the question remains: do consumers engage in a privacy trade-off?

This study sheds more light on the conditions under which app users engage in a cost-benefit trade-off when downloading apps. In the mobile app context, the costs of an app download are mainly related to the potential risk of losing freedom of choice and privacy due to the app's permission request, whereas the benefits of a download are often related to the perceived value of an app. Following earlier research (e.g., [24,29]), we use the concept of *app value* as an indicator for *benefits* and the concepts *app intrusiveness* and *privacy concerns* as indicators for *costs*.

2.2. Perceived app value

Value has generally been defined as "the perceived benefit of something (e.g., object, person, or activity) to an individual or group" ([30], p. 1). Mobile apps may offer different kinds of value to the user, which may be related, among others, to social interaction, information seeking, or entertainment [31]. Depending on how much value an app has to offer in general, app users may be more or less inclined to grant an app's permissions, thereby sharing personal information with it. According to Fife and Orjuela [1], an individual's concept of privacy indeed changes based on the benefits he/she expects for revealing personal information. Existing research supports this assumption, showing, for instance, that a higher perceived benefit of the information disclosure made consumers select riskier privacy settings in apps [11] and positively influenced their intention to download an app [24]. In addition, research has demonstrated that the immediate benefits from information disclosure (e.g., app use) may trump the delayed benefits (e.g., privacy protection), even among privacy-conscious users [20]. Moreover, recent research has demonstrated that the popularity of an app decreases privacy concerns and increases download intention [4]. Based on this line of research, we expect that:

H1. Perceived app value has a positive effect on app users' intention to accept permission requests.

2.3. App intrusiveness

One of the costs associated with downloading apps is that users have to accept the app's permission to be able to use it. This can be considered intrusive. Intrusiveness is a psychological construct that embraces the notion of "creating an imbalance between closeness and autonomy" ([32], p. 990), where closeness is related to the degree of interdependence between two parties and autonomy is related to the degree to which the personal identity of an individual can be safeguarded [33].

The concept of intrusiveness can also be applied to the mobile app context. Mobile apps usually only work properly when the user has accepted the app's permission request. As mentioned earlier, accepting an app's permission request often automatically implies sharing personal data with the app, which might jeopardize privacy ([6,34]). Consequently, whenever someone considers downloading an app, (s)he has to decide between two options: take it (i.e., accept the terms, thereby jeopardizing privacy) or leave it (i.e., refuse to download the app). When users choose the "take it" option, they mostly do not have any leeway to influence how much personal data the app wants to access. This creates an imbalance between closeness and autonomy, because the app restricts users in their autonomous decision to share information. This can be considered intrusive. Intrusiveness is distinct from privacy concern, because even though an app might be considered intrusive as it collects a lot of information, this does not necessarily have to mean that the app user perceives this as a privacy invasion.

According to psychological reactance theory [35], intruding on an individual's freedom of choice can lead to reactance, a state in which the individual is motivationally aroused to regain the lost freedom. Translating this notion to the mobile app context, it might be that when app users are confronted with a highly intrusive app, they show reactance by refusing to accept the app's permission request. This refusal does not have to be related to privacy concerns, it can also just occur due to the experienced loss of freedom. In fact, prior research supports this assumption, showing that consumers disclose less information when requests for personal information are highly intrusive (e.g., [24,29,36]). Additionally, a study by Gu et al. [4] showed that perceived permission sensitivity, that is, "the levels of discomfort users perceive when an app requests certain permissions to control their mobile device and use their personal information" (p. 20), exacerbated privacy concerns, which, in turn, had a negative influence on app download intention.

Based on this literature, we hypothesize that:

H2. App intrusiveness has a negative effect on app users' intention to accept permission requests.

2.4. The role of privacy concerns

App users may refuse to accept app permission requests not only because they want to show reactance against the intrusive request but also because they experience privacy concerns, here defined as individuals' "concerns about [the] possible loss of privacy as a result of information disclosure to a specific external agent" ([37], p. 2). Research on the antecedents and consequences of online privacy concerns has led to mixed results. On the one hand, several studies have shown that consumer privacy concerns lead to risk-reducing behavior, such as withholding or falsifying personal information, using privacy-enhancing techniques (e.g., encryption), or requesting removal from mailing lists [38,39]. Based on this body of literature, we expect that:

H3. Privacy concerns will be negatively related to app users' intention to accept permission requests.

On the other hand, prior research on privacy concerns has revealed the existence of a "privacy-paradox": although consumers are worried about their online privacy, they do not seem to apply these concerns to their online usage behavior correspondingly [16,40,41]. In this paper, we argue based on the framework of contextual integrity [42] that these mixed findings point toward the existence of different context-dependent privacy trade-offs, which are based on interactions of the variables app value, intrusiveness, and privacy concerns. Hereafter, we will elaborate more on the expected interactions.

Prior research has shown that individuals may differ widely in the extent to which they cope with and experience privacy concerns [43]. We assume that these different levels of privacy concerns may affect consumer responses toward the data collection practices of mobile apps. In fact, earlier research has demonstrated that different levels of privacy concerns may condition consumer responses toward various online marketing activities. For instance, highly privacy-concerned consumers responded more negatively (e.g., in terms of attitude, information disclosure) to online SNS campaigns [44], advergame features [45], and online behavioral advertising [46] than less-concerned individuals. Based on these findings, it is assumed that different levels of privacy concern may also condition the effect of app intrusiveness on users' intention to accept permission requests.

We expect that:

H4. The negative effect of app intrusiveness on intention to accept permission requests will be stronger when app users have high (as opposed to low) levels of privacy concerns.

Apart from that, the degree to which app users experience concern for privacy may also condition the effect of app value on users' intention to accept permission requests. Earlier research has shown that the perceived value or benefit can outweigh privacy concerns in the decision to disclose personal information, for instance, in e-commerce transactions [9] or on SNS [10]. Additionally, it has been found that consumers regularly discount the value of their privacy for immediate benefits associated with the information disclosure [14,47]. Translating these findings to the mobile app context, it is thus reasonable to assume that privacy concerns condition the effect of app value on users' intention to accept permission requests to a lesser extent when the app in question is of high value to users than when the app in question is of low value to users. Therefore, we hypothesize that:

H5. Privacy concerns will moderate the effect of app value on intention to accept permission requests such that more-concerned app users (as opposed to less-concerned) will have a lower intention to accept permission requests. This pattern will be more pronounced for low-value than high-value apps.

Finally, it might also be that app intrusiveness, app value, and privacy concerns, in conjunction, affect app users' intention to accept permission requests. Because there is insufficient literature available to convincingly hypothesize a three-way interaction between these variables, we pose the following research question:

RQ: To what extent do app intrusiveness, app value, and privacy concerns, in conjunction, influence app users' intention to accept permission requests?

3. Overview of studies

To test our hypotheses and answer our research question, we conducted two online experiments. Study 1 was conducted among 183 ($M_{age} = 21.18$, $SD = 2.01$) university students of a Western European country. To demonstrate the robustness of our findings, we replicated study 1 among a more generalizable sample of 687 mobile app users ($M_{age} = 52.40$, $SD = 15.87$). The sample of study 2 was representative for the Western European country where this study was conducted. The method and results of the two studies are presented below. To minimize the effects of common method variance (CMV) [48], we varied the anchors of our scales for different constructs. After collecting the data, Herman's single-factor test was conducted for both studies to test for CMV. If CMV were a serious problem in our studies, we would expect a single factor to emerge from an exploratory factor analysis or one general factor to account for most of the covariance in the independent and criterion variables. We conducted an exploratory factor analysis for each study on all items, extracting, for each study, four factors with eigenvalues greater one. Moreover, no general factor was apparent in the unrotated factor structure, with Factor 1 accounting for <23% of the variance in study 1 and <25% in study 2. Consequently, CMV was not of great concern in either study.

4. Study 1

4.1. Method

4.1.1. Participants, design, and stimulus material

A total of 183 students of a Western European university (M = 21.14, SD = 1.83; 82.7% female) participated in the experiment in exchange for partial course credit. One respondent was removed from the original sample because (s)he was significantly older than the rest of the participants. Of the participants, 100% owned a smartphone and/or 40.4% a tablet.

The experimental design was a 2 (intrusiveness: high vs. low) × 2 (app value: high vs. low) between subjects factorial design. Participants were randomly assigned to one of the following experimental conditions: high app value – high intrusiveness (N = 47); low app value – high intrusiveness (N = 48); high app value – low intrusiveness (N = 43); or low app value – low intrusiveness (N = 45). The factor privacy concern was measured.

To develop the stimulus material for the final experiment, we conducted a pre-test among 272 students. In this pre-test, participants rated how intrusive they perceived the different information inquiries of mobile apps to be. Based on these ratings, we developed an app permissions page in which the different types of information were presented in decreasing order of intrusiveness. The screenshot of the app permissions page strongly resembled a real Android permissions page, and it included a list of all the types of information the app requests access to (e.g., device ID, app history) as well as an "Agree" button. The following two factors were manipulated in the material.

App value served as a between subjects factor and could take a high or low value. To manipulate app value, participants were asked to write down in an open text field which app they would miss most (high value) or least (low value) if they had to delete it from their smartphone/tablet. The name of the app participants wrote down (e.g., XYZ) automatically appeared in a sentence above the screenshot of the app permissions page: "App XYZ needs access to…"

Intrusiveness was the second between subjects factor and could take high or low intrusiveness values. We manipulated intrusiveness by placing either the word "yes" (high intrusiveness) or "no" (low intrusiveness) behind every type of information listed on the app permissions page, suggesting that the app does or does not access it.

4.1.2. Procedure

Participants were recruited via the university's subject pool. Prior to participating in the study, informed consent was obtained. Hereafter, respondents were randomly assigned to one of the four conditions. Then, participants indicated in an open text field which app they would miss the most/least if they had to delete the app from their smartphone/tablet. Next, participants were asked to carefully read the following scenario: "For some mobile apps, the provisions for the protection of personal information have recently changed. These apps ask you to accept their terms of usage again. Imagine the [NAME OF THE APP] app asks you to accept its new terms of use. The [NAME OF THE APP] needs access to…[SCREENSHOT]." Hereafter, participants were asked to complete a questionnaire in which they answered questions on intention to accept the permission request, app attitude, privacy concerns, app use, prior experience of privacy invasion, manipulation checks, and demographics. At the end of the experiment, participants were thanked and debriefed.

4.1.3. Measures

4.1.3.1. App value. To check whether the app value manipulation was successful, we asked participants to indicate on a one-item scale (1 = *not at all* and 7 = *extremely*) how much they would miss app X if they had to delete it from their smartphone/tablet (M = 3.95, SD = 2.38). According to Rossiter [49], a single-item measure suffices when constructs are double concrete, meaning that the attribute of a construct has a clear singular meaning and that the object being rated is clear and unambiguous to the person doing the rating. A meta-analysis by Ang and Eisend [50] supports Rossiter's research, demonstrating that there was no difference in effect sizes when the double-concrete variables were measured with single or multiple items, indicating that data collection with single items is more efficient and less tedious. Based on this evidence and because we think that the value item used here is unambiguous, we decided to measure app value with a single item.

4.1.3.2. App intrusiveness. To check whether the intrusiveness manipulation was successful, we used three Likert scale items (1 = *strongly disagree* and 7 = *strongly agree*) inspired by Nowak and Phelps [51], for instance, "The information request of app X represents a serious invasion of my privacy" (M = 4.50, SD = 1.63, α = 0.86). A Principal component analysis (PCA) yielded one component (EV = 2.36; R^2 = 0.79).

4.1.3.3. Privacy concerns. Privacy concerns were measured with six Likert scale items (1 = *strongly disagree* and 7 = *strongly agree*) adopted from Xu et al. [37], 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 = 3.54, SD = 1.56, α = 0.92). The PCA yielded one component (EV = 4.38; R^2 = 0.72).

4.1.3.4. Permission acceptance intention. App users' intention to accept the app's permission request was measured with a self-constructed one-item scale inspired by Bernritter et al. [52]. Participants indicated on a 100-point slider scale (0 to 100%) their intention to accept the new terms of use of the app (M = 64.00, SD = 36.43). The higher the percentage, the more willing participants were to accept the permission request.

4.1.3.5. Control variables. A number of control variables were measured to ensure that the effects were not caused by other differences between groups. *App use* was measured by asking participants how often they use app X on their smartphone/tablet (1 = *never* and 5 = *a few times a day*; M = 3.38, SD = 1.71). *Prior experience with privacy infringement* was measured using three Likert scale items (1 = *not at all* and 7 = *all the time; don't know*) adapted from Xu et al. [37], for instance, "How often have you personally been the victim of what you felt was an improper invasion of privacy?" (M = 3.98, SD = 1.73). *Don't know* answers were categorized as missing values. Finally, participants' age, gender, and educational background were ascertained.

4.2. Results

4.2.1. Manipulation and confound checks

The intrusiveness manipulation was successful. Participants in the high intrusiveness condition perceived the app to be significantly more intrusive (M = 5.22, SD = 1.26) than participants in the low intrusiveness condition (M = 3.71, SD = 1.63), $t(163.37) = -6.91$, $p < 0.001$. The app value manipulation was also successful. Participants in the high app value condition perceived the app to be of significantly more value to them (M = 5.94, SD = 1.34) than respondents in the low app value condition (M = 2.02, SD = 1.34), $t(181) = -19.81$, $p < 0.001$. Additionally, participants in the high app value condition used the app more frequently (M = 4.89, SD = 0.55) than participants in the low app value condition (M = 1.93, SD = 1.05), $t(140.27) = -24.12$, $p < 0.001$. The experimental groups did not differ with respect to educational background (χ^2 (9) = 5.15, p = 0.82), gender (χ^2 (3) = 3.24, p = 0.36), or prior experience with privacy invasion ($F(3, 180) = 1.66$, p = 0.18). However, there was a significant age difference between groups, ($F(3, 179) = 4.09$, p = 0.01). Participants in conditions one (high value – high intrusiveness; N = 47; M = 21.57, SD = 1.71) and four (low value – low intrusiveness; N = 45; M = 21.63, SD =

2.02) were, on average, approximately one year older than participants in conditions two (low value – high intrusiveness; $N = 48$; $M = 20.77$, $SD = 1.75$) and three (high value – low intrusiveness; $N = 43$; $M = 20.58$, $SD = 1.67$). Therefore, we controlled for age in all further analyses. The apps participants filled in as part of the app value manipulation were all free apps (e.g., WhatsApp, Instagram), and hence, the costs of the app could not have played a confounding role in the analyses.

4.2.2. Testing hypotheses

The hypotheses were tested using hierarchical multiple regressions. The variables app value, intrusiveness, and privacy concerns were entered into the regression model as the first block (Step 1), followed by the interactions of privacy concerns with the other two variables in the second block (Step 2). Permission acceptance intention was included as a dependent variable. Before running the analyses, we applied main effects parameterization to the categorical independent variables to parameterize the model correctly, meaning that we coded the two levels of app value and intrusiveness using the codes −0.5 and +0.5 [53]. Furthermore, we mean-centered the variable privacy concerns Furthermore, we mean-centered the moderator variable privacy concerns, because this "renders the test of hypotheses and regression coefficients […] more meaningful and substantively interpretable" ([53], p. 289). Variance inflation factor (VIF) diagnostics did not point to multicollinearity problems (all <1.10).

Table 1 indicates that the regression model with permission acceptance intention as the dependent variable, with intrusiveness, app value, and privacy concerns as independent variables, and with age as a covariate was significant, $F(4, 178) = 20.45$, $p < 0.001$, and it explained 32% of the variance in permission acceptance intention. Moreover, the regression model containing the covariate age, the independent variables and their interaction terms with privacy concerns was significant too $F(8, 174) = 12.21$, $p < 0.001$, and it explained 36% of the variance in permission acceptance intention. In line with H1, app value had a positive effect on information disclosure intention ($\beta = 0.44$, $p < 0.001$). The more valuable an app was to app users, the more they were inclined to accept the permission request. Moreover, as predicted by H2, app intrusiveness had a negative effect on permission acceptance intention ($\beta = -0.23$, $p < 0.001$), meaning that the more information an app collected, the less app users were inclined to accept the permission request. Furthermore, supporting H3, privacy concerns were negatively related to permission acceptance intention ($\beta = -0.20$, $p = 0.002$), and hence, the more concerned app users were about their privacy, the less they were inclined to accept the permission request. Investigating the interaction effects, we did not find the expected two-way interaction of intrusiveness and privacy concerns, rejecting H4. Instead, the analysis yielded a two-way interaction of value and privacy concerns ($\beta = 0.13$, $p = 0.04$), partly confirming H5. As can be seen in Fig. 1, when privacy concerns were low, participants in the low app value condition were more willing to accept the permission request than when privacy concerns were high. In the high app value condition, however, there was no difference in permission acceptance intention between participants with higher or lower privacy concerns. Finally, answering our research question, we did not find a three-way interaction between app value, intrusiveness, and privacy concerns.

Table 1
Hierarchical multiple regression analyses predicting permission acceptance intention.

	Study 1		*Study 2*	
	Permission acceptance intention			
	R^2	β	R^2	β
Step 1	0.32***		0.29***	
Intrusiveness		−0.22***		−0.16***
Value		0.47***		0.42***
Privacy concern		−0.23***		−0.25***
Step 2	0.36***		0.30***	
Intrusiveness		−0.23***		−0.17***
Value		0.44***		0.42***
Privacy concern		−0.20**		−0.25***
Intrus × value		0.11		0.02
Intrus × PC		0.01		0.03
Value × PC		0.13*		−0.03
Intrus × value × PC		0.10		−0.08*
n		183		687

Note. Intrus = Intrusiveness, Value = App Value, PC = Privacy Concerns.
* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

5. Study 2

5.1. Method

A total of 687 respondents aged 18–87 years ($M = 52.40$, $SD = 15.87$) participated in the experiment in exchange for a small financial incentive. Participants were recruited among the international Esomar-certified online panel of the online market research institute PanelClix. PanelClix sent e-mails containing a link to our questionnaire to a representative sample of the Dutch population (18+). In total, 46.7% of the respondents were female. The majority had finished a medium (32.8%) or a higher level of education (24.3%). Moreover, 88.8% of the participants owned a smartphone and/or 65.9% a tablet. The experimental design, stimulus, material, measures, and procedure were identical to study 1.

5.2. Results

5.2.1. Manipulation and confound checks

As intended, participants in the high intrusiveness condition perceived the app to be significantly more intrusive ($M = 5.09$, $SD = 1.61$) than participants in the low intrusiveness condition ($M = 4.14$, $SD = 1.87$), $t(645.24) = -6.99$, $p < 0.001$; hence, the intrusiveness manipulation was successful. Moreover, participants in the high app value condition perceived the app to be of significantly more value to them ($M = 5.45$, $SD = 1.54$) than respondents in the low app value condition ($M = 1.85$, $SD = 1.32$), $t(661.43) = -32.57$, $p < 0.001$. Furthermore, participants in the high app value condition used the app more frequently ($M = 4.34$, $SD = 0.95$) than participants in the low app value condition ($M = 1.98$, $SD = 1.19$), $t(623.26) = -28.25$, $p < 0.001$. Therefore, the app value manipulation was successful as well. The experimental groups did not differ with respect to educational background ($\chi^2(18) = 14.38$, $p = 0.70$), gender ($\chi^2(3) = 4.16$, $p = 0.25$), age ($F(3, 683) = 0.09$, $p = 0.96$), or prior experience with privacy invasion ($F(3, 667) = 5.58$, $p = 0.19$). The apps participants filled in as part of the app value

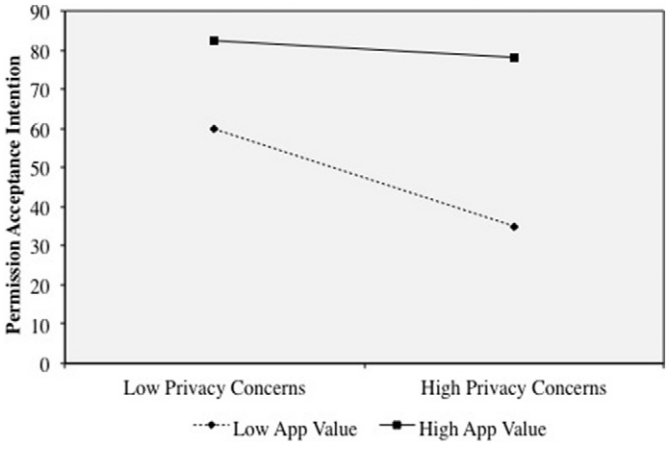

Fig. 1. Two-way interaction of app value and privacy concerns.

manipulation were all free apps (e.g., WhatsApp, Instagram), and hence, the costs of the app could not have played a confounding role in the analyses.

5.2.2. Testing hypotheses

As in study 1, the hypotheses were tested using hierarchical multiple regressions. As indicated in Table 1, the regression model with permission acceptance intention as a dependent variable and intrusiveness, app value, and privacy concerns as independent variables was significant, $F(3, 679) = 95.57$, $p < 0.001$, and it explained 29% of the variance in permission acceptance intention. Furthermore, the regression model containing the independent variables as well as their interaction terms with privacy concerns was significant, $F(7, 675) = 42.21$, $p < 0.001$, and it explained 30% of the variance in permission acceptance intention. Replicating our findings from study 1, the analysis revealed a positive effect of app value ($\beta = 0.42$, $p < 0.001$) and a negative effect of app intrusiveness ($\beta = -0.17$, $p < 0.001$) on permission acceptance intention, confirming H1 and H2. Additionally, as predicted by H3, we again found the negative relationship between privacy concerns and permission acceptance intention ($\beta = -0.25$, $p < 0.001$). Investigating the interaction effects, we again did not find a significant two-way interaction between app intrusiveness and privacy concerns, rejecting H4. Moreover, we did not replicate the two-way interaction between app value and privacy concerns found in study 1, rejecting H5. However, in contrast to study 1, study 2 revealed a small significant three-way interaction between app intrusiveness, app value, and privacy concerns ($\beta = -0.08$, $p = 0.02$). Thus, to answer our research question in a more generalizable sample, these three variables in conjunction seem to affect permission acceptance intention, although this effect is rather small. To investigate this interaction in more detail, we conducted moderation analyses using the PROCESS macro ([53], Model 3). This macro offers the possibility to probe three-way interactions using a pick-a-point approach, which estimates the conditional effect of the interaction of the independent variable *X* (i.e., intrusiveness) and the primary moderator *M* (i.e., value) on the dependent variable *Y* (i.e., disclosure intention) given certain values of the secondary moderator *W* (i.e., privacy concerns). It also conducts inferential tests for this interaction at that value of *W* [53]. This analysis revealed that the effect of app intrusiveness on permission acceptance intention is not moderated by app value when consumers experience medium, $\theta_{XM \rightarrow Y} = 2.36$, $t(679) = 0.51$, $p = 0.61$, or high levels of privacy concerns, $\theta_{XM \rightarrow Y} = -8.75$, $t(679) = -1.32$, $p = 0.19$. However, when app users experienced low levels of privacy concern, app value moderates the effect of intrusiveness on permission acceptance intention, $\theta_{XM \rightarrow Y} = 13.46$, $t(679) = 2.05$, $p = 0.04$. The results are graphically presented in Fig. 2, showing that when app users have low privacy concerns and when the app in question is of low value to them, they base their decision to accept the permission request on how intrusive the app is: The more information the app collects, the less the inclination of less-concerned users to accept the permission request. However, when the app in question is of high value to users, those with low privacy concern intend to accept the permission request regardless of how intrusive the app in question is.

6. Conclusion & discussion

6.1. Implications

This study tried to empirically answer the – so far unanswered – question do consumers engage in a privacy trade-off? By investigating consumers' privacy decisions in the pervasive, data-intensive, and potentially privacy-invading mobile app context, the current study offers three important findings. The first major finding is that the privacy calculus findings of past research can be replicated in the mobile app context. Hence, app users do indeed seem to engage in a privacy trade-off. A replication study focusing on the mobile app context was necessary for two reasons. First, mobile devices may compromise consumer privacy far more than other digital devices [19], which is why the privacy decision-making process is far more complex than, for instance, that of e-commerce transactions. It is therefore not enough to rely on earlier studies investigating the privacy trade-off in other contexts (e.g., [9]) to fully understand consumers' privacy decision-making processes. Second, earlier research often only *measured* the costs and benefits of the trade, making it impossible to draw causal inferences, or it *forced* participants to make a trade-off, which is why it is logical that these researchers also found a trade-off. Our study extends literature on the

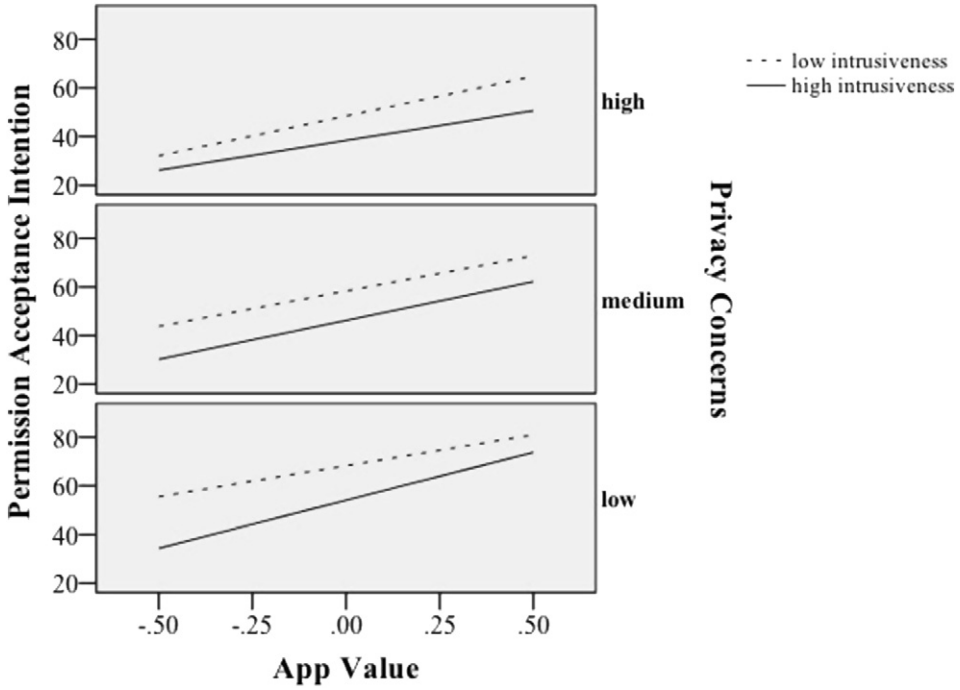

Fig. 2. Three-way interaction of app intrusiveness, app value, and privacy concerns.

privacy trade-off by manipulating the costs and benefits of the privacy trade-off without forcing participants to trade the costs against the benefits. In doing so, our study is, to our knowledge, the first to draw causal inferences on the interplay of costs and benefits in privacy decision-making. As our results demonstrate, app value has a positive effect on permission acceptance intention, which provides empirical evidence for earlier assumptions made in the mobile app context [11,24]. Moreover, we found that in line with earlier research on "normal" Internet users (e.g., [29,33,39]), perceived intrusiveness had a negative effect on mobile app users' intention to accept permission requests and that privacy concerns were negatively related to permission acceptance intention.

Considering the roles of app value, app intrusiveness, and privacy concerns in the privacy trade-off, our findings show that the effect of app value exceeds the association of privacy concerns, which in turn exceeds the effect of intrusiveness. In line with earlier research [14,20], this finding implies that the immediate value gained from information disclosure via mobile apps (e.g., the app use) trumps the costs (i.e., intrusiveness, privacy concerns) related to the information trade. Earlier research on consumer privacy aimed to establish rules that could help collect private information while pursuing consumer satisfaction, for instance, through fair information practices, or by providing consumers with more control over their data. These findings can be also linked to the main constructs of this study, app intrusiveness and app value using Nissenbaum's [42] framework of contextual integrity. Nissenbaum [42] proposed that only practices that are considered inappropriate flows of personal information disturb our sense of privacy. More specifically, only data collection practices that violate context-specific informational norms are problematic. Connecting this notion to our findings and earlier literature, it might be that once consumers perceive the value of an app as adequate, some degree of intrusiveness is perceived as appropriate as well.

Second, the current study is the first to investigate the joint effects of app value, intrusiveness, and privacy concerns on permission acceptance intention. In doing so, the study provides more profound insights into the boundary conditions of the privacy calculus than earlier research, and it sheds more light on the so-called "privacy paradox". The small three-way interaction found in study 2 revealed that when the app in question is of high value to users, those with low privacy concern intend to accept the permission request regardless of how intrusive the app in question is. However, when users are less concerned about their privacy and when the app is of low value to the user, app users seem to base their intention to accept the request on the intrusiveness levels of the app. These results imply that for apps that are of low value to users, less-concerned app users appear to use app intrusiveness as a cue based on which they decide to accept permission requests or not. Interestingly, what the three-way interaction also shows is that those with high privacy concerns still have disclosure values of 30% in the low value condition. These people are thus still relatively likely to accept permission requests, which points to the privacy paradox and might indicate that privacy concerns, for some people, might just be empty words or something very diffuse. The latter assumption is supported by the two-way interaction between app value and privacy concerns found in study 1. Here, no difference in permission acceptance intention between participants with higher or lower privacy concerns was found when the app in question was of high value to users. This supports the assumption that consumers discount their privacy for short-term benefits, such as the use of a valued app [20]. Notably, we only found the two-way interaction in study 1 and the three-way interaction in study 2. It might be that the relatively small three-way interaction only occurred in study 2 due to its large sample size, and hence, we should not overestimate it. The absence of the two-way interaction found in study 1 in replication study 2 might be explained by the different overall means of app value and privacy concern in both studies. The "older" sample of study 2 showed, on average, lower app value levels and higher privacy concern levels than the "younger" sample of study 1. It seems as if app value plays a less important role and privacy a more important role for older people than for younger people, which suggests that age might influence the outcome of the privacy trade-off. More research is needed to investigate the role of age in the privacy calculus.

Finally, the third major finding of this study is that the main effects of app value and app intrusiveness as well as the association of privacy concerns in the privacy trade-off are robust across different samples. The regression weights were very similar in both studies, which speak in favor of the robustness of our findings. This has important practical implications. An important and perseverative question in the consumer privacy context is whether consumer privacy can be protected through industry self-regulation, meaning that firms and consumers are responsible for taking the necessary means to protect their privacy, or whether policy makers need to intervene. The robust findings of our study show that although consumers do engage in a privacy trade-off, they still do not seem to be sufficiently equipped to make well-considered, self-regulated privacy decisions when downloading apps, because app value seems to overrule the influence of app intrusiveness and privacy concerns in the decision making process. Raising awareness of the intrusiveness of apps (e.g., via the app permissions screen) and evoking privacy concerns might decrease app users' permission acceptance intention, but this strategy does not seem to work well for highly valued apps. Given that app users probably first and foremost download apps that are of value to them, informing people about the costs of the trade might not be the best way to protect consumer privacy. This finding implies that the privacy self-regulation principle that is effective at the moment is not enough to protect consumer privacy in today's information age. It is about time that policy makers implement new laws that restrict mobile apps in their data collection and processing activities.

6.2. Limitations and future research

Investigating the conditions under which consumers withhold or surrender personal information is important, given that downloading mobile apps may have serious consequences for consumer privacy [6]. Such an investigation is, however, difficult, and we therefore need to consider some limitations of our study. First and most notably, the work presented here is purely experimental in nature, which might have consequences for the ecological validity of our findings. We did our best to design the experiments to be as realistic as possible, and according to our realism manipulation checks, it seems as if we succeeded in our aspiration. Nevertheless, our participants were exposed to an app permissions page and they were asked to think about whether they would accept these permissions or not. In practice, when app users download mobile apps, they often do not read the app permissions page, nor do they think about their decision to accept the terms of use as carefully as they had to during our study. In fact, research has shown that the majority of mobile Internet users never read privacy permissions when installing apps or visiting mobile websites [54]. Hence, it might be that the decisional calculus we show in this paper may look somewhat different in practice. To verify that our findings also hold in practice, future research could try to test the privacy trade-off in another context in which consumers are not that habituated to simply click on "accept."

Second, our choice to ask participants to rethink granting permissions for apps that were already installed on their mobile device might be vulnerable to criticism. In general, asking app users to re-accept the terms of use is something apps regularly do, for instance, because of changes in the app's privacy policy (e.g., WhatsApp privacy changes, cf., [55]). Hence, as far as realism is concerned, our scenario might be considered believable. However, it might be that asking participants about apps they already downloaded on their mobile device led to cognitive dissonance and a positivity bias in our results. Future researchers might want to investigate the privacy trade-off by manipulating app value in a more controlled way, for instance, by using fictive apps.

Third, the apps participants mentioned as part of the app value manipulation were all free, meaning that our findings are only applicable to apps that are at no charge. Compared to free apps, paid apps might be viewed differently in the eyes of users when considering privacy issues. In this vein, a fruitful next line of research may focus on comparing the privacy trade-off for free apps compared to that of paid apps.

In sum, this study is the first to examine the notion of the privacy calculus in the mobile app context using a rigorous experimental setting that allows solid causal inferences to be drawn. In two studies, we confirm the existence of the privacy calculus and show that the value of an app trumps the costs (i.e., intrusiveness, privacy concerns) in the privacy trade-off. Based on our findings, we call for more policy interventions that restrict the data collection and processing activities of mobile apps, because the current self-regulation principle does not seem to be sufficient to protect consumer privacy in today's information age.

References

[1] E. Fife, J. Orjuela, The privacy calculus: mobile apps and user perceptions of privacy and security, International Journal of Engineering Business Management 4 (2012) 1–10, https://doi.org/10.5772/51645.

[2] H.J. Smith, T. Dinev, Information privacy research: an interdisciplinary review, MIS Quarterly 35 (4) (2011) 989–1015 Retrieved from http://web.a.ebscohost.com/ehost/detail/detail?vid=1&sid=a25ecf2e-8031-4f26-b49f-46a2f040e602%40sessionmgr4007&hid=4002&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=67129829&db=buh.

[3] J. van Dijck, Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology, Surveillance Society 12 (2) (2014) 197–208 Retrieved from http://queens.scholarsportal.info/ojs/index.php/surveillance-andsociety/article/view/datafication.

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

[5] J. King, A. Lampinen, A. Smolen, Privacy: is there an app for that? Proceedings of the Seventh Symposium on Usable Privacy and Security. USA 2011, pp. 12:1–12:20, https://doi.org/10.1145/2078827.2078843.

[6] S. Thurm, Y.I. Kane, What they know: your apps are watching you, Wall Street Journal (2010) Retrieved from http://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

[7] A. Acquisti, L.K. John, G. Loewenstein, What is privacy worth? The Journal of Legal Studies 42 (2) (2013) 249–274, https://doi.org/10.1086/671754.

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

[9] T. Dinev, P. Hart, An extended privacy calculus model for E-commerce transactions, Information Systems Research 17 (1) (2006) 61–80, https://doi.org/10.1287/isre.1060.0080.

[10] T. Dienlin, M.J. Metzger, An extended privacy calculus model for SNSs: analyzing self-disclosure and self-withdrawal in a representative U.S. sample, Journal of Computer-Mediated Communication 21 (5) (2016) 368–383, https://doi.org/10.1111/jcc4.12163.

[11] M.J. Keith, S.C. Thompson, J. Hale, P.B. Lowry, C. Greer, Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior, International Journal of Human Computer Studies 71 (12) (2013) 1163–1173, https://doi.org/10.1016/j.ijhcs.2013.08.016.

[12] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems 22 (3) (2013) 295–316, https://doi.org/10.1057/ejis.2012.23.

[13] I.-H. Hann, K.-L. Hui, T. Lee, I. Png, Online information privacy: measuring the cost-benefit trade-off, ICIS 2002 Proceedings, Spain, 2002 Retrieved from http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf.

[14] A. Acquisti, J. Grossklags, Privacy and rationality in individual decision making, IEEE Security and Privacy Magazine 3 (1) (2005) 26–33, https://doi.org/10.1109/msp.2005.22.

[15] L.K. John, A. Acquisti, G. Loewenstein, Strangers on a plane: context-dependent willingness to divulge sensitive information, Journal of Consumer Research 37 (5) (2011) 858–873, https://doi.org/10.0.4.62/656423.

[16] S. Kokolakis, Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon, Computers & Security 64 (2017) 122–134, https://doi.org/10.1016/j.cose.2015.07.002.

[17] H.A. Simon, Models of Bounded Rationality, MIT Press, 1982.

[18] A. Vishwanath, H. Chen, 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) (2008) 1761–1775, https://doi.org/10.1002/asi.20892.

[19] Federal Trade Commission (FTC), Mobile privacy disclosures: building trust through transparencyRetrieved from www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf 2013.

[20] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science 347 (6221) (2015) 509–515, https://doi.org/10.2139/ssrn.2580411.

[21] I. Ajzen, M. Fishbein, Understanding Attitudes and Predicting Social Behaviour, Prentice-Hall, Englewood Cliffs, NJ, 1980.

[22] I. Ajzen, From intentions to actions: a theory of planned behavior, in: J. Kuhl, J. Beckmann (Eds.), Action Control: From Cognition to Behavior, Springer Berlin Heidelberg, Berlin, Heidelberg 1985, pp. 11–39, https://doi.org/10.1007/978-3-642-69746-3_2.

[23] S. Burns, L. Roberts, Applying the Theory of Planned Behaviour to predicting online safety behaviour, Crime Prevention and Community Safety 15 (1) (2013) 48–64, https://doi.org/10.1057/cpcs.2012.13.

[24] N. Eling, T. Widjaja, H. Krasnova, P. Buxmann, Will you accept an App? Empirical investigation of the decisional calculus behind the adoption of applications on Facebook, Proceedings of the Thirty Fourth International Conference on Information Systems, Italy 2013, pp. 1–20 Retrieved from https://www.researchgate.net/publication/258610799_Will_You_Accept_an_App_Empirical_Investigation_of_the_Decisional_Calculus_Behind_the_Adoption_of_Applications_on_Facebook.

[25] R. Wei, V.-H. Lo, Staying connected while on the move: cell phone use and social connectedness, New Media & Society 8 (1) (2006) 53–72, https://doi.org/10.1177/1461444806059870.

[26] Y. Li, Theories in online information privacy research: a critical review and an integrated framework, Decision Support Systems 54 (1) (2012) 471–481, https://doi.org/10.1016/j.dss.2012.06.010.

[27] V.H. Vroom, Work and Motivation, John Wiley & Sons, New York, 1964.

[28] F. Kehr, T. Kowatsch, D. Wentzel, E. Fleisch, Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus, Information Systems Journal 25 (6) (2015) 607–635, https://doi.org/10.1111/isj.12062.

[29] G. Cecere, F. Rochelandet, Privacy intrusiveness and web audiences: empirical evidence, Telecommunications Policy 37 (10) (2013) 1004–1014, https://doi.org/10.1016/j.telpol.2013.09.003.

[30] B. Figueiredo, D. Scaraboto, The systemic creation of value through circulation in collaborative consumer networks, Journal of Consumer Research 43 (4) (2016) 509–533 Retrieved from http://jcr.oxfordjournals.org/content/early/2016/08/18/jcr.ucw038.abstract.

[31] Y.-H. Lin, C.-H. Fang, C.-L. Hsu, Determining uses and gratifications for mobile phone apps, Future Information Technology, Springer 2014, pp. 661–668.

[32] S. Lavy, M. Mikulincer, P.R. Shaver, O. Gillath, Intrusiveness in romantic relationships: a cross-cultural perspective on imbalances between proximity and autonomy, Journal of Social and Personal Relationships 26 (6–7) (2009) 989–1008, https://doi.org/10.1177/0265407509347934.

[33] J. van Doorn, J.C. Hoekstra, Customization of online advertising: the role of intrusiveness, Marketing Letters 24 (4) (2013) 339–351, https://doi.org/10.1007/s11002-012-9222-1.

[34] N.J. King, P.W. Jessen, Profiling the mobile customer – privacy concerns when behavioural advertisers target mobile phones – part I, Computer Law & Security Review 26 (5) (2010) 455–478, https://doi.org/10.1016/j.clsr.2010.07.001.

[35] J.W. Brehm, A Theory of Psychological Reactance, Academic Press, Oxford, 1966.

[36] A. Acquisti, L. John, G. Loewenstein, The impact of relative standards on the propensity to disclose, Journal of Marketing Research 49 (2) (2012) 160–174, https://doi.org/10.1509/jmr.09.0215.

[37] H. Xu, S. Gupta, M.B. Rosson, J.M. Carroll, Measuring mobile users' concerns for information privacy, Proceedings of the Thirty Third International Conference on Information Systems, USA, 2012 Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1108&context=icis2012.

[38] K.B. Sheehan, M.G. Hoy, Flaming, complaining, abstaining: how online users respond to privacy concerns, Journal of Advertising 28 (3) (1999) 37–51, https://doi.org/10.1080/00913367.1999.10673588.

[39] J. Wirtz, M.O. Lwin, J.D. Williams, Causes and consequences of consumer online privacy concern, International Journal of Service Industry Management 18 (4) (2007) 326–348, https://doi.org/10.1108/09564230710778128.

[40] P.A. Norberg, D.R. Horne, D.A. Horne, The privacy paradox: personal information disclosure intentions versus behaviors, Journal of Consumer Affairs 41 (1) (2007) 100–126, https://doi.org/10.1111/j.1745-6606.2006.00070.x.

[41] M. Taddicken, The "privacy paradox" in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure, Journal of Computer-Mediated Communication 19 (2) (2014) 248–273, https://doi.org/10.1111/jcc4.12052.

[42] H. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009.

[43] B. Debatin, J.P. Lovejoy, A. Horn, B.N. Hughes, Facebook and online privacy: attitudes, behaviors, and unintended consequences, Journal of Computer-Mediated Communication 15 (1) (2009) 83–108, https://doi.org/10.1111/j.1083-6101.2009.01494.x.

[44] G. Van Noort, M.L. Antheunis, P.W.J. Verlegh, Enhancing the effects of social network site marketing campaigns: if you want consumers to like you, ask them about themselves, International Journal of Advertising 3 (2) (2014) 1–18, https://doi.org/10.2501/ija-33-2-235-252.

[45] V.M. Wottrich, P.W.J. Verlegh, E.G. Smit, The role of customization, brand trust, and privacy concerns in advergaming, International Journal of Advertising 36 (1) (2017) 60–81, https://doi.org/10.1080/02650487.2016.1186951.

[46] E.G. Smit, G. Van Noort, H.A.M. Voorveld, Understanding online behavioural advertising: user knowledge, privacy concerns and online coping behaviour in Europe, Computers in Human Behavior 32 (2014) 15–22, https://doi.org/10.1016/j.chb.2013.11.008.

[47] A. Acquisti, J. Grossklags, What can behavioral economics teach us about privacy, Digital Privacy: Theory, Technologies and Practices, 18, 2007, pp. 363–377, https://doi.org/10.1201/9781420052183.ch18.

[48] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, The Journal of Applied Psychology 88 (5) (2003) 879–903, https://doi.org/10.1037/0021-9010.88.5.879.
[49] J.R. Rossiter, Measurement for the Social Sciences: The C-OAR-SE Method and Why It Must Replace Psychometrics, Springer, Berlin, 2011.
[50] L. Ang, M. Eisend, Single versus multiple measurement of attitudes, Journal of Advertising Research (2017) Retrieved from http://www.journalofadvertisingresearch.com/content/early/2017/01/12/JAR-2017-001.abstract.
[51] G.J. Nowak, J. Phelps, Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs, Journal of Direct Marketing 6 (4) (1992) 28–39, https://doi.org/10.1002/dir.4000060407.
[52] S.F. Bernritter, P.W.J. Verlegh, E.G. Smit, Why nonprofits are easier to endorse on social media: the roles of warmth and brand symbolism, Journal of Interactive Marketing 33 (2016) 27–42, https://doi.org/10.1016/j.intmar.2015.10.002.
[53] A.F. Hayes, Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach, Guilford Press, New York, NY, 2013.
[54] Y. Liu, User control of personal information concerning mobile-app: notice and consent? Computer Law & Security Review 30 (5) (2014) 521–529, https://doi.org/10.1016/j.clsr.2014.07.008.
[55] D. McLaughlin, S. Bodoni, Facebook's WhatsApp Privacy Changes Raise EU, U.S. Concerns, Bloomberg, August 2016 Retrieved from https://www.bloomberg.com/news/articles/2016-08-29/whatsapp-privacy-changes-raise-eu-concern-over-user-data-control.
[56] S. Degli Esposti, When big data meets dataveillance: The hidden side of analytics, Surveillance & Society 12 (2) (2014) 209–225 Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/5113.
[57] J. Sutanto, E. Palme, Chuan-Hoo Tan, W.P. Chee, Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users, MIS Quarterly 37 (4) (2013) 1141–1164 Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3143&context=misq.
[58] B.W. Reyns, Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses, Journal of Research in Crime and Delinquency 50 (2) (2013) 216–238, https://doi.org/10.1177/0022427811425539.

Verena M. Wottrich (M.Sc.) is a PhD Candidate at the Amsterdam School of Communication Research ASCoR, Department of Communication Science, University of Amsterdam, The Netherlands. Her research focuses on the causes and consequences of Internet users' privacy decisions in (branded) mobile apps. Her work has appeared in the International Journal of Advertising, the sixth volume Advances in Advertising Research published by the European Advertising Academy (EAA), Advertising in new formats and media: Current research and implications for marketers, Emerald Publishing, and it has been acknowledged by awards from the International Communication Association and the European Advertising Academy.

Eva A. van Reijmersdal (Ph.D.) is Associate Professor at the Amsterdam School of Communication Science ASCoR, Department of Communication Science, University of Amsterdam, The Netherlands. Her research focuses on the effects of sponsored content on adults and children as well as on the effects of branded apps. She has published over 40 book chapters and articles in academic peer reviewed journals, including International Journal of Advertising, Computers in Human Behavior, Communication Theory, Psychology & Marketing, and Journal of Media Psychology. Her work has been acknowledged by awards from the International Communication Association, the National Communication Association, the European Advertising Academy, and the Dutch Flanders Communication Association.

Edith G. Smit (Ph.D.) is Full Professor at the Amsterdam School of Communication Research ASCoR, Department Communication Science, University of Amsterdam, The Netherlands. Her research is in persuasive communication with focus on processing of advertising and tailored health campaigns. She is also Dean of the Graduate School of Communication at the University of Amsterdam. Her work has appeared in academic peer reviewed journals, including Computers in Human Behavior, Journal of Advertising, International Journal of Advertising, and Journal of Advertising Research. Her work has been acknowledged among others by awards from the International Communication Association, the American Advertising Academy, and the European Advertising Academy.