frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 09 September 2022
DOI 10.3389/fcomp.2022.986138

Check for updates

OPEN ACCESS

EDITED BY
Michele Ianni,
University of Calabria, Italy

REVIEWED BY
Raj Chaganti,
Toyota Research Institute (TRI),
United States
Matteo Dell'Amico,
University of Genoa, Italy

*CORRESPONDENCE
Vanessa Ayres-Pereira
vanessa.ayresp@gmail.com

SPECIALTY SECTION
This article was submitted to
Computer Security,
a section of the journal
Frontiers in Computer Science

RECEIVED 13 July 2022
ACCEPTED 17 August 2022
PUBLISHED 09 September 2022

CITATION
Ayres-Pereira V, Pirrone A,
Korbmacher M, Tjostheim I and
Böhm G (2022) The privacy and
control paradoxes in the context of
smartphone apps.
Front. Comput. Sci. 4:986138.
doi: 10.3389/fcomp.2022.986138

The privacy and control paradoxes in the context of smartphone apps

Vanessa Ayres-Pereira[1]*, Angelo Pirrone[1,2], Max Korbmacher[1], Ingvar Tjostheim[3] and Gisela Böhm[1,4]

[1]Department of Psychosocial Science, University of Bergen, Bergen, Norway, [2]Centre for Philosophy of Natural and Social Science, London School of Economics and Political Science, London, United Kingdom, [3]Norwegian Computing Center, Oslo, Norway, [4]Department of Psychology, Inland Norway University of Applied Sciences, Lillehammer, Norway

This research examines how various factors, such as the degree of e-privacy concerns and control over data access permissions, can influence a user's intention to install a smartphone app. We conducted two survey-based experiments with 441 participants. In each experiment, we manipulated the degree of control over the number and type of data access permissions granted to different fictional apps. In Study 1, participants were informed about the set of permissions the apps required. In Study 2, participants indicated which individual permissions they were willing to grant to the apps. In both experiments, we assessed the level of e-privacy concerns, perceived app importance, and the intention to install the apps. The results suggest that the type of app plays a central role in determining both the perceived benefit of installing the app and the level of e-privacy concerns. The intention to install an app is more strongly associated with perceived app importance than with e-privacy concerns (especially when app importance is high, and users have explicit control over which specific data access permissions they want to grant). The implications of these results are discussed regarding psychological factors involved in app installation decision-making process and the importance of promoting data protection by design.

KEYWORDS

control paradox, privacy paradox, e-privacy concerns, smartphone app, permission systems

Introduction

Installing an app on a smartphone is a common activity nowadays. In 2021, while the number of smartphone users worldwide was approximately 4.9 billion, the number of mobile application downloads reached a peak of 230 billion, an average of 47 apps per user (Statista, 2022). Most applications (also referred to as apps) require for their installation some extent of self-disclosure of private information. One issue of concern is that some app developers have collected excessive amounts of data from users for non-functional purposes, that is, for so-called secondary uses such as selling the data as a commodity (e.g., Spiekermann et al., 2015; Zang et al., 2015). This practice is ethically questionable because, usually, users are unaware of the amount of data collected and with whom the data are traded (e.g., Acquisti and Grossklags, 2007; Felt et al., 2012). Another issue is the risks for individuals and society that emerge due to data misuse. Such data have been used, for example, in cybercrimes, to charge different prices for the same product depending on the characteristics of the consumer (price discrimination) and to micro-regulate and persecute citizens in some countries (e.g., Acquisti and Varian, 2005; Zuboff, 2015).

In response to concerns about electronic data privacy (e-privacy), policymakers and technology companies have promoted solutions that involve giving consumers more control over the release of their information. Nowadays, data-access permission systems inform users and require them to provide consent for an app to read and write data from their devices. One problem, however, is that some researchers claimed that increased control might not be a solution to reduce users' vulnerability to the risks of data sharing. Brandimarte et al. (2012) observed that the greater the control individuals have over the release of personal information, the greater the likelihood that they engage in risky behavior, that is, that they intentionally disclose the data. This phenomenon is known as the control paradox. Another problem is that research has shown that, although users report increasing levels of concern about e-privacy, they tend to engage little in behaviors to protect their data. The inconsistency between a high degree of concern and yet a high probability of disclosing data was coined as the privacy paradox (Barnes, 2006). Due to the risks involved in app installation, scientists have argued that more research is needed to understand how users decide to install an app (e.g., Kokolakis, 2017).

Related work and own contribution

The literature indicates several factors that may influence e-privacy decisions, such as the degree of control over the release of personal information, benefits from data disclosure, and e-privacy concerns (e.g., Brandimarte et al., 2012; Felt et al., 2012; Egelman et al., 2013; Zafeiropoulou et al., 2013; Buck et al., 2014). So far, such factors have usually been studied in isolation and most studies focused on the context of social network sites (SNSs) and e-commerce (cf. Kokolakis, 2017). Furthermore, few of the studies on the context of apps compared how factors that influence installation intention can vary depending on the type of application (e.g., Gu et al., 2022). For example, while the request to share location data could be a factor that raises concerns that would decrease the intention to install a puzzle game app, the same request could not be a factor of concern for the installation of a map app. The objective of the present research is to add to a growing body of literature about how several factors interact in shaping people's decision to install different types of smartphone apps (e.g., Gu et al., 2022; Shahidi et al., 2022). The present research expands the literature by investigating how different factors (in particular, the degree of control and the degree of privacy concerns) can interact and shape psychological processes that influence the intention to install different types of smartphone applications. We conducted two survey-based experiments. For each study, we manipulated the degree of control of the user over the number and type of data access permissions granted to different fictional apps. In both studies, we assessed individuals' levels of e-privacy concerns, importance given to the app functionality, and the intention to install three different apps. In the next subsections, we discuss how these factors can influence the decision to install an app according to previous studies.

Degree of privacy concerns and the privacy paradox

Several studies reported the privacy paradox in the context of SNSs and e-commerce (for reviews, see Barth and de Jong, 2017; Kokolakis, 2017). However, some studies about the decision to install apps and allow them to access data produced mixed results regarding the privacy paradox. For example, polls conducted in the US found that Americans report avoiding apps due to privacy concerns; 54% of respondents reported that they decided not to install an app due to the amount of personal data needed to use it (Boyles et al., 2012). Besides, previous research suggests that users are concerned with their privacy and even willing to pay premiums for apps that are less likely to request access to personal data (Egelman et al., 2013).

The variability across studies can be due to several factors, including the fact that research on SNSs and e-commerce deals with decisions other than the decision to install apps. Moreover, e-privacy concern is a multidimensional concept. That is to say, there are many facets that people may be concerned about (e.g., Buck et al., 2018). In the context of smartphones, the degree of privacy concerns can vary, for example, according to the function served by the app and the type of data managed (e.g., Culnan, 1993). Regarding the type of data, much of past research on e-privacy has focused on users' attitudes and preferences toward sharing geolocation data (e.g., Barkuus and Dey, 2003; Sadeh et al., 2009; King et al., 2011; Lindqvist et al., 2011; Yigitoglu et al., 2018). Location is an important aspect of e-privacy (see Rowe, 2020, for an interesting discussion), but users may be less concerned about location than other types of data commonly accessed by apps (e.g., Egelman et al., 2013). Besides, the decision to share geolocation is heavily influenced by contextual factors such as the function of the app (Lin et al., 2012) and trust in the app (Zafeiropoulou et al., 2013). Therefore, it is relevant to investigate different facets of privacy concerns, including the level of sensitivity of different data types and how the decision to disclose them varies depending on the app.

We investigated the following aspects of e-privacy concerns in the present research: how concerned respondents are about their information privacy while using smartphones, how important they consider data security within different apps, and how uncomfortable they feel about granting data access permissions to different numbers and types of data. Considering the aforementioned results (e.g., Boyles et al., 2012; Egelman et al., 2013), we raised the following hypotheses:

H_1: The level of concern about information privacy while using smartphones has a negative effect on the intention to install all apps.

H_2: The level of importance assigned to data security in a specific app has a negative effect on the intention to install this app.

H_3: The level of discomfort arising from requesting access to certain types and amounts of data by a specific app has a negative effect on the intention to install this app.

Benefits from data disclosure and importance of app functionality

Previous research shows that users want applications to perform specific tasks (Egelman et al., 2013), and suggest that decisions to disclose data can be based on a trade-off where individuals choose to exchange their private data for benefits or services that they consider important (e.g., Hann et al., 2002; Hui et al., 2007; Acquisti, 2009). Privacy calculus theory postulates that the decision to disclose personal data is a function of the discount of the expected losses from the gains promised by the decision to disclose data (Dinev and Hart, 2006), where individuals decide to provide information when potential gains surpass potential losses (producing the privacy paradox).

Liu et al. (2015), Gu et al. (2022), and Shahidi et al. (2022), for example, produced evidence in favor of the privacy calculus theory by demonstrating that whether a user chooses to use an app is a result of the trade-off between the app's functionality (or usefulness) and the user's privacy concerns. However, some studies interested in decisions in the context of mobile applications have focused more on risks and not given as much attention to the relation between the degree of importance of different apps and the decision to disclose personal information (e.g., Felt et al., 2012; Egelman et al., 2013; Zafeiropoulou et al., 2013; Buck et al., 2014). Our research, therefore, aims to investigate how the perceived importance of apps for different purposes influences the intention to install the apps. We informed respondents about three different types of fictional apps (Puzzle Game, Messaging, and Weather Forecast). These apps were chosen because they are very common, generally installed by most people, and we expected they would have different levels of functionality importance. Considering the above results, we raised the following hypothesis:

H_4: The level of importance of the app has a positive effect on the intention to install the app.

We considered evidence in favor of the privacy calculus, whether privacy concerns (H_1, H_2, H_3) and the importance given to the app (H_4) simultaneously predicted installation intention.

Degree of choice and the control paradox

Mobile operating system developers, such as Google and Apple, developed data access permission systems to allow users to control an application's access to the users' data. These systems, however, can present the opportunity to decide whether to disclose personal information differently. The system can present data access permission options as an "all-or-nothing" decision at installation time. That is, before the user presses the install button, the system shows the list of permissions that the app requests and prompts the user to consent (or not consent) to install and, therefore, grant all the requested permissions to the app. If the user does not consent to all permissions, the only option is to cancel the installation altogether (Android Developers: System Permissions, n.d.-a). Another way to present the options has emerged over the years and turned granting permissions into a more fine-grained decision to be made after installation. In this case, first, the app is installed, and while in use, the first time an app needs certain access, the system requests specific permissions. Declining permission to access certain data comes with the cost of not benefiting from certain functionalities (iOS human interface guidelines: Accessing user data and resources, n.d.-b).

Research shows that decisions can vary based on how the choices and the permission systems are designed (e.g., Lin et al., 2012). Some authors suggested that "presenting permission requests when the data is needed, rather than requiring all permissions to be granted at install time" could lead to better-informed decisions regarding privacy (Egelman et al., 2013, p. 213). However, a study conducted by Brandimarte et al. (2012) indicated that increased perceived control over the release of personal data can lead to increase in the willingness to disclose the information, a phenomenon coined as the control paradox. For Brandimarte et al., control is the "action of willingly sharing some private information with a set of recipients" (p. 341), considering the risks of other people accessing and using the data.

To our knowledge, the question of how the degree of control over the release of personal information affects the intention to install a smartphone app has not received sufficient attention in the e-privacy literature. Our studies, therefore, set out to investigate the occurrence of the control paradox in the context of smartphone apps. In order to vary the degree of control, we manipulated a specific aspect of control called volition, that is, the power of making a choice (Nordgren et al., 2007). Specifically, we manipulated information about the absence (Study 1) or presence (Study 2) of opportunity to choose the amount and type of data disclosed to applications.

Considering the results of Brandimarte et al. (2012), we raised the following hypothesis:

H$_5$: A condition that presents the opportunity for respondents to choose the exact amount and type of data disclosed to apps (Study 2) has a positive effect on the intention to install the apps, compared to a condition that does not present the opportunity to choose (Study 1).

Interactions between control and privacy concerns

The means by which increased control would increase the intention of data disclosure remains to be further explained. One possibility is that greater degrees of control reduce the degree of privacy concerns (e.g., Hoadley et al., 2010; Degirmenci, 2020) and then, tend to reflect a greater likelihood of data disclosure. However, the number of studies on the interactions between control and privacy concerns in digital contexts is still limited. Therefore, our objective was to expand the literature. Considering previous discussions (e.g., Hoadley et al., 2010; Degirmenci, 2020), we raised the following hypothesis:

H$_6$: A condition that gives respondents the opportunity to choose the amount and type of data disclosed to apps (Study 2) has a negative effect on privacy concerns levels compared to a condition that does not present the opportunity to choose (Study 1).

Study 1

In Study 1, we presented the installation decision as an "all or nothing" process, where installing an app implied granting access to a certain set of data types as required by the app. We observed if the perceived data security importance and the intention of installing an app varied across conditions that demanded different numbers of data access permissions. Finally, we assessed predictors of the intention to install an app.

Method

Participants

Participants were recruited in the canteen and through announcements at the beginning of lectures in the Faculty of Psychology of a university in Norway (October–November 2019). Two hundred and twenty-seven ($N = 227$) respondents finished the questionnaire (64.3% women, 33.0% men, 0.4% preferred not to say, 2.2% did not respond). Most of the sample (95.2%) were young adults, with ages ranging between 18 and 30 years (3.1% were 31–50 years old, 0.4% was 50 or older, and 1.3% preferred not to say). Consent to participate was considered as "given" if a participant returned a completed questionnaire. At the end of the survey, participants received a small chocolate bar as compensation. There were no other incentives for participation.

Design

The study was designed as a self-administered pen-and-paper questionnaire. Each participant answered questions about three fictional apps (Puzzle Game, Messaging, and Weather Forecast). The apps were presented in counterbalanced order across participants to minimize carryover effects. A block of questions was asked for each app. Chi-squared test[1] did not indicate a statistically significant effect of the order in which apps were presented on the dependent variable (intention to install the application) [Study 1: $\chi^2(N = 222) = 1.216, p = 0.544$].

A mixed (within- and between-subjects) design controlled for the number and type of data access permissions that were described as being required by the application. That is, participants were informed that "This app requires the following highlighted permission in order to work: internal storage (photos, files), microphone, location, contact". Every app could require access to zero, one, two, three, or four types of data (microphone; location; contacts; internal storage: photos and files). Therefore, Study 1 included five conditions: 0-, 1-, 2-, 3-, or 4-data access permissions. In the 0-data access permission condition, an app required access to no data. In the 1-data condition, an app required access to one type of data. In the 2-data condition, an app required access to two types of data (e.g., contacts and location; microphone and location) and so forth. All possible combinations of permissions requested are described in Table 1 together with the number of participants allocated per condition.

Procedure

A 4-page questionnaire was administered. The first page provided details of the research topic and informed consent, then asked participants to indicate their age group and gender. On the next pages, the survey focused on three fictional smartphone apps. For each app, participants were first asked about perceived app importance; they were informed about the number and type of data permissions requested by the app (in Study 1); inquired about app installation intention and perceived importance of data security within that app. On the last page, the questionnaire inquired about data sensitivity and privacy concerns when using smartphones. All items were presented in English.

[1] Readers unfamiliar with the statistical tests reported in this article can consult textbooks on statistical methods in psychology, such as Navarro and Foxcroft (2022).

TABLE 1 Number of participants per experimental condition.

Data access permissions requested	Puzzle app (n)	Weather app (n)	Messaging app (n)
Zero	16	22	12
One			
Contacts	18	14	13
Location	16	22	16
Microphone	16	13	25
Internal Storage	11	15	22
Two			
Contacts + Location	13	13	10
Microphone + Location	16	16	15
Microphone + Contacts	17	17	24
Internal Storage + Contacts	17	17	14
Internal Storage + Microphone	17	16	13
Internal Storage + Location	16	12	19
Three			
Microphone + Location + Contacts	14	12	8
Internal Storage + Microphone + Contacts	13	12	11
Internal Storage + Microphone + Location	10	14	10
Internal Storage + Location + Contacts[a]	1	3	1
Four	16	9	14

[a] An experimental error led to the small number of respondents in the condition where the app requested access to internal storage, location, and contacts.

Measures

Perceived app importance

The perceived importance of each app was assessed through one item: "How important is this app to you from 0 to 10, where 0 is 'not important at all' and 10 is 'very important'?".

Intention to install the app

One item assessed the intention to install each app: "How likely are you to install this app?". Responses to this question were given on a 7-point scale ranging from 1 (*very unlikely*) to 7 (*very likely*).

Perceived importance of data security

For each app, respondents indicated how important they thought data security was with respect to this app. This was measured with the following item: "How important do you think it is that such an app secures privacy, where 0 is 'not important at all' and 10 is 'very important'?".

Perceived data sensitivity

One question, consisting of four sub-items corresponding to four data access permissions, assessed perceived data sensitivity by asking**:** "Please indicate for each of the following permissions your degree of discomfort from 0 to 10 (where 0 is 'no discomfort at all' and 10 is 'extreme discomfort') when an app is requesting permission." The data types requested were internal storage (files and photos), microphone, location, and contacts.

It was presumed that the four items reflected a common latent *discomfort factor*. Therefore, for each app, an overall degree of discomfort arising from data access permissions was calculated as the sum of discomfort levels from access to each type of data multiplied by zero or 1 depending on whether (1) or not (0) the app required permission for this app (Study 1) / the user granted this permission for the app (Study 2). For example, a participant in Study 1 whose Puzzle app requested access to contacts and location, and with discomfort levels 10 and 9 when an app accesses contacts and location, respectively, would have an overall degree of discomfort of 19 when installing this app [$discomfort = (10 \times 1) + (9 \times 1)$]. Correspondingly, a participant in Study 2 who indicated a willingness to provide access only to contacts and location to the Puzzle app (in Study 2), and with discomfort levels 10 and 9 when granting access to contacts and location, respectively, would also have an overall degree of discomfort of 19.

Smartphone privacy concern

The last item measured the degree to which people were worried regarding their data privacy when using smartphones: "On a scale from 0 to 10 (where 0 is 'not concerned' and 10 is 'very concerned'), how concerned are you about your data privacy when using a smartphone?".

Results

In this section, we will focus on analyses that identify the impact of the conditions on the perceived importance of data security and installation intention across apps, and predictors of the intention to install the apps in Study 1.

In general, respondents reported a moderate to high median (*Mdn*) level of smartphone privacy concern ($Mdn = 7.0$; on a scale from 0 to 10) and a moderate to high degree of discomfort from granting data access permission to all types of data ($Mdn = 7.00$; on a scale from 0 to 10). As shown in Figure 1, the Messaging app was perceived as more important than both, Puzzle and Weather Forecast apps, and the Weather app was more important than the Puzzle ($Mdn_{\text{Messaging}} = 9.0$; $Mdn_{\text{Weather}} = 7.0$; $Mdn_{\text{Puzzle}} = 1.0$; on a scale from 0 to 10). Data security was perceived to be more important in the Messaging than in the Puzzle and Weather apps ($Mdn_{\text{Messaging}} = 10.0$; $Mdn_{\text{Weather}} = 8.0$; $Mdn_{\text{Puzzle}} = 8.0$). The intention to install the Messaging app was greater than both the intention to

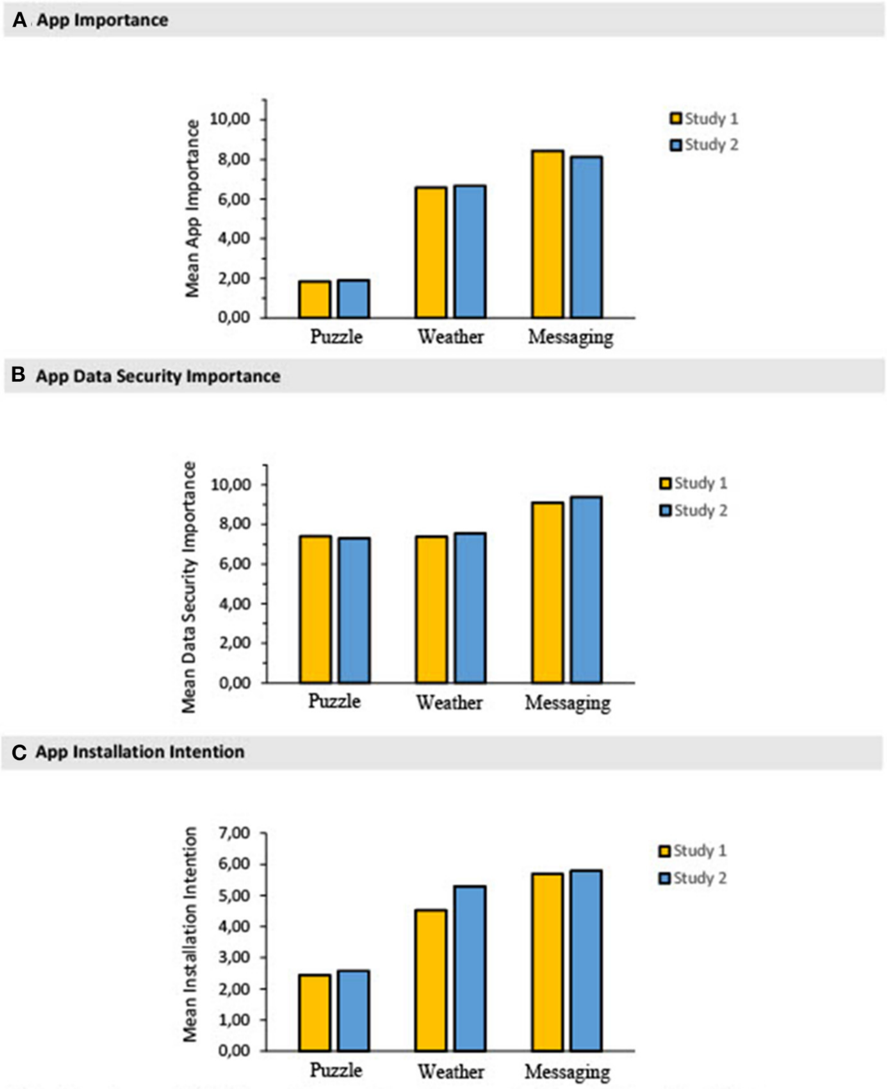

FIGURE 1
Mean perceived app importance **(A)**, app data security importance **(B)**, and app installation intention **(C)**. Error bars with 95% confidence intervals corrected for within-subject designs were omitted from the graphs because the bars were too narrow to be discernible.

install the Puzzle and Weather apps, while the intention to install the Weather app was greater than the Puzzle ($Mdn_{\text{Messaging}} = 6.0$; $Mdn_{\text{Weather}} = 5.0$; $Mdn_{\text{Puzzle}} = 2.0$; on a scale from 0 to 7). IBM SPSS® Statistics 25 software was used to perform the analyses.

Perceived app data security importance across conditions

Figure 2A presents the mean perceived data security importance across apps and conditions. A Kruskal-Wallis test showed that the number of permissions requested significantly affected the perceived importance of data security in the Puzzle app, $H(4) = 16.939$, $p = 0.002$. *Post-hoc* Mann-Whitney tests using a Bonferroni-adjusted alpha level of.005 (0.05/10) were used to compare all pairs of conditions. Perceived data security importance was significantly higher when the Puzzle app required access to 4-data types than to zero, $U(N_{0-\text{data}} = 16; N_{4-\text{data}} = 15) = 52.00$, $Z = -2.857$, $p = 0.004$, with a large effect ($r = -0.513$), or one, $U(N_{1-\text{data}} = 60; N_{4-\text{data}} = 15) = 223.50$, $Z = -3.090$, $p = 0.002$, with a medium effect ($r = -0.357$). There were no statistically significant differences between the other conditions. The number of permissions requested did not significantly affect the perceived importance of data security in the Weather, $H(4) = 0.728$, $p = 0.948$, and Messaging apps, $H(4) = 5.792$, $p = 0.215$.

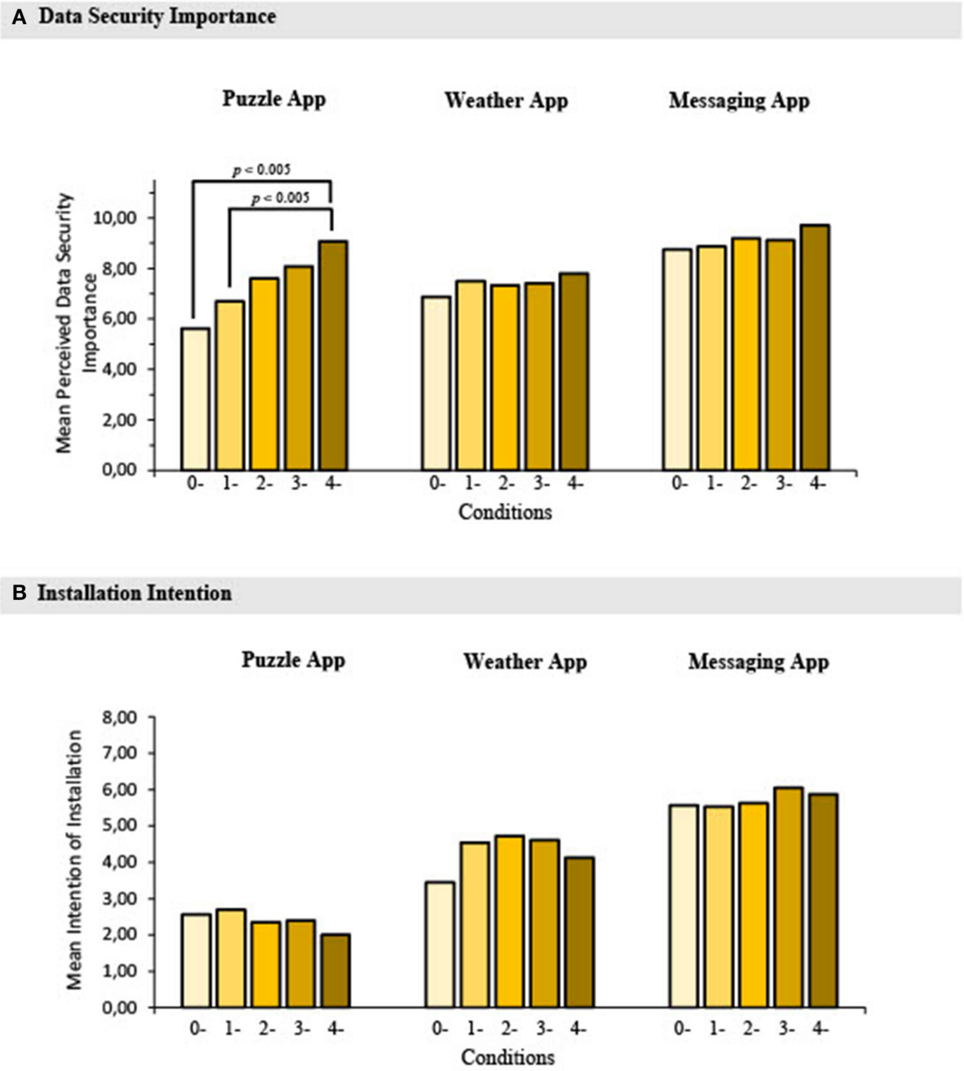

FIGURE 2
Mean data security importance **(A)** and installation intention **(B)** across apps and conditions with 0-, 1-, 2-, 3-, and 4-data access permissions required, study 1. Mann-Whitney tests, using Bonferroni adjusted p-value = 0.005 for ten comparisons. Error bars with 95% confidence intervals corrected for within-subject designs were omitted from the graphs because the bars were too narrow to be discernible.

Predictors of the intention to install an app in study 1

Multiple linear regressions were used to investigate whether the intention to install an app can be predicted from general smartphone privacy concern, perceived app importance, data security importance, and discomfort over data access. Our data, however, violated the parametric assumption of normality, and data transformations were not appropriate. Therefore, bootstrap regression (e.g., Davison and Hinkley, 1997) was used as an alternative (with a Bonferroni-adjusted alpha level of.017 = 0.05/3). Table 2 presents the results of bootstrapped multiple regression analysis for the three fictional apps.

In the Puzzle app, the model explained 29.9% of the variance in installation intention ($R^2_{\text{adjusted}} = 0.299$). App importance was a significant predictor of installation intention ($p = 0.001$, $B = 0.438$, 95% CI [0.326, 0.560]); an increase in one unit of importance of the app corresponded, on average, to an increase of.438 points in the intention to install the app. The degree of discomfort over data access was another significant predictor ($p = 0.002$, $B = -0.037$, 95% CI [-0.057, -0.018]). An increase in one unit of discomfort corresponded to a decrease in installation intention of.037 points. Smartphone privacy concern and perceived data security were not significant as predictors (see Table 2).

TABLE 2 Results of bootstrapped multiple regression analysis with intention of installing the app as dependent variable, study 1.

Independent variables	***B***	***SE***	**Bias**	***p***	**BCa 95% CI**	
					Lower bound	**Upper bound**
Puzzle app (*n* = *209*)						
Smartphone privacy concern	−1.101	0.057	0.002	0.079	−0.209	0.019
App importance	0.438	0.056	0.002	0.001*	0.326	0.560
App data security importance	0.069	0.326	0.001	0.089	−0.013	0.152
App discomfort	−0.037	0.011	−0.001	0.002*	−0.057	−0.018
Weather app (*n* = 215)						
Smartphone privacy concern	0.017	0.047	−0.001	0.721	−0.077	0.104
App importance	0.390	0.045	−0.002	0.001*	0.296	0.470
App data security importance	−0.113	0.037	0.001	0.002*	−0.189	−0.040
App discomfort	−0.036	0.015	−0.001	0.023	−0.066	−0.009
Messaging app (*n* = 200[a])						
Smartphone privacy concern	−0.040	0.020	−0.001	0.049	−0.077	−0.004
App importance	0.522	0.033	0.000	0.001*	0.454	0.583
App data security importance	0.016	0.037	−0.001	0.663	−0.051	0.082
App discomfort	0.002	0.006	0.000	0.717	−0.010	0.014

Bootstrap results are based on 1,000 bootstrap samples. BCa, Bias-corrected and accelerated.

*p < 0.05.

[a] Results concerning the Messaging app were obtained after removing 14 outliers (case IDs 7, 26, 46, 60, 77, 81, 97, 150, 159, 170, 173, 183, 190, 210). The removal of outliers did not change the results (i.e., significant p values), however, it allowed to meet the assumptions of multiple regression analysis—absence of significant outliers and homoscedasticity.

In the Weather app, the model explained 29.7% of the variance in installation intention ($R^2_{\text{adjusted}} = 0.297$). App importance, $p = 0.001$, $B = 0.390$, 95% CI [0.296, 0.470], and app data security importance, $p = 0.002$, $B = -0.113$, 95% CI [−0.189, −0.040] were both significant predictors of the intention to install the Weather app. An increase in one unity of app importance corresponded, on average, to an increase in installation intention of.390 points, while an increase in one unity of app data security importance corresponded, on average, to a decrease in installation intention of 0.113 points.

In the Messaging app, the model explained 66.8% of the variance. App importance was the only predictor of the Messaging app installation intention ($p = 0.001$, $B = 0.522$, 95% CI [.454, 0.583]). An increase in one unity of app importance corresponded, on average, to an increase in installation intention of 0.522 points.

Discussion

The results from Study 1 suggest that the decision to install an app (and grant data access permissions as required) results from a trade-off between the app's functionality importance and the user's privacy concerns (e.g., Dinev and Hart, 2006; Liu et al., 2015; Shahidi et al., 2022). For our participants, when the functionality of the app was of great importance (Messaging app), there was a high intention to install it—despite high levels of concern about using smartphones, privacy security importance, and degree of discomfort over data access. In contrast, for apps with lower importance (Puzzle and Weather Forecast), privacy concerns were more likely to take precedence and predicted a decreased intention to install the app. The results of Study 1 show that different app-specific concerns are likely to predict a reduced intention to install different apps with low to moderate importance. The greater the discomfort over data access, the less participants intended to install the Puzzle app. The greater the importance of data security, the less participants intended to install the Weather app. Although data security was not a significant predictor of the Puzzle Game installation intention, only in this app data security importance was positively related to the number of requested permissions.

Previous research found that most participants do not pay attention to permission during installation (Egelman et al., 2013). We found that, for our respondents in Study 1, discomfort arisen from the number and type of permission requested by an app did not predict app installation (except the Puzzle app). These results confirm that, sometimes, information about the amount of data requested might not be crucial to many users. These results open up some follow-up questions. Considering that decisions can vary based on how the choices are structured (e.g., Egelman et al., 2013), could the degree of privacy concerns be reduced, and installation intention be increased if respondents had more control over the type of data access permissions granted to an app? Besides, could the lack of attention to the number of permissions requested be due to being unaware of which type of data is often needed for specific apps to work (e.g., Felt et al., 2012; Buck et al., 2014)?

Study 2

Study 2 served to replicate Study 1 with a condition in which participants have more detailed control over permissions (i.e., they have the freedom to decide which type of information the app can access on the mobile device).

Method

Participants

Participants were recruited at the University's canteens and through announcements at the beginning of lectures (October–November 2019) simultaneously with Study 1. Two hundred and fourteen (N = 214) respondents, who did not participate in Study 1, finished the questionnaire in Study 2 (81.2% women, 16.9% male, 0.9% preferred not to say, 0.9% did not respond). Most of Study 2 participants (96.7%) were again 18–30 years old (1.0% was 31–50 years old, 1.4% was 51 or older, and 0.9% did not respond).

Design

Study 2 was identical to Study 1 except that, instead of presenting which data permissions each app requested, respondents were asked to indicate which permissions they would be willing to grant to each app (the instructions were phrased as follows: "If you were asked to provide as many permissions as possible, which permissions would you be willing to provide to this app? Draw a circle around the permissions you decide to provide: internal storage (photos, files), microphone, location, contacts"). As in Study 1, we did not find a statistically significant effect of the order in which apps were presented on the dependent variable (intention to install the application) in Study 2: $\chi^2(N = 208) = 0.551, p = 0.759$).

Results

Comparison across studies 1 and 2

In this section, we report the analyses that were repeated across the two studies (see Appendix A1 for details).

Smartphone privacy concern

In general, respondents reported a moderate to high level of smartphone privacy concern (Mdn_{study1} = 7.0; Mdn_{study2} = 7.0; on a scale from 0 to 10), without statistically significant differences between studies, $U(N_{\text{study1}} = 223; N_{\text{study2}} = 210) = 22478.50, Z = -0.73, p = 0.467$.

Perceived sensitivity of information

Results of Mann-Whitney U tests (with Bonferroni adjusted p-value = 0.013, for four comparisons) indicated that data sensitivity did not differ significantly between studies for any of the data types: internal storage, $U(N_{\text{study1}} = 223; N_{\text{study2}} = 208) = 22737.00, Z = -0.35, p = 0.721$; location, $U(N_{\text{study1}} = 223; N_{\text{study2}} = 207) = 23046.50, Z = -0.03, p = 0.979$; contacts, $U(N_{\text{study1}} = 223; N_{\text{study2}} = 208) = 20516.00, Z = -2.09, p = 0.037$; and microphone, $U(N_{\text{study1}} = 221; N_{\text{study2}} = 208) = 19890.00, Z = -2.43, p = 0.015$.

A Friedman test—with Studies 1 and 2 datasets combined—evaluated differences in medians among the different types of data and rendered $\chi^2(2, N = 426) = 18.16$, which is significant ($p < 0.001$). Although participants reported a moderate to high degree of discomfort from granting data access permission to all types of data (Mdn = 7.00), *post-hoc* analysis with a Wilcoxon Signed-Rank test indicated that discomfort from granting access to internal storage was significantly higher than to contacts ($Z = -3.35, p = 0.001$), microphone ($Z = -3.18, p = 0.001$), and location ($Z = -3.07, p = 0.002$), with small effect sizes ($r = -0.161, r = -0.154, r = -0.149$, respectively).

App specific judgments: Perceived app importance, data security importance, and installation intention

Perceived app importance

Figure 1A presents mean perceived app importance in Studies 1 and 2. Results of Mann-Whitney U tests (with Bonferroni adjusted p value = 0.017) indicated that there was no statistically significant difference in perceived importance between studies for any of the apps: Puzzle, $U(N_{\text{study1}} = 220$; $\text{N}_{\text{study2}} = 205) = 22301.00, Z = -0.204$, p = 0.839; Weather Forecast, $U(N_{\text{study1}} = 221$; $\text{N}_{\text{study2}} = 209) = 22694.00, Z = -0.315$, p = 0.753; and Messaging, $U(N_{\text{study1}} = 222$; $\text{N}_{\text{study2}} = 212) = 21960.50, Z = -1.249$, p = 0.212.

A Friedman test—with Studies 1 and 2 datasets combined—evaluated differences in median importance across the apps and rendered $\chi^2(N = 410) = 570.19, p < 0.001$. Pairwise posthoc analysis with a Wilcoxon Signed-Ranks test indicated that the Messaging app was perceived to be significantly more important than both the Puzzle ($Z = -17.218, p < 0.001, r = -0.840$), and Weather Forecast apps ($Z = -10.349, p = 0.000, r = -0.503$). And the Weather app was significantly more important than the Puzzle ($Z = -16.283, p < 0.001, r = -0.800$).

Perceived importance of data security

Figure 1B presents the mean perceived data security importance across the apps in Studies 1 and 2. Results of Mann-Whitney U tests (with Bonferroni adjusted p-value = 0.017, 005/3) indicated that data security importance differed across studies neither for the Puzzle [$U(N_{\text{study1}} = 222; N_{\text{study2}} = 209) = 23{,}134.50$, $Z = -0.052$, $p = 0.959$] nor for the Weather app [$U(N_{\text{study1}} = 224; N_{\text{study2}} = 208) = 22{,}609.00$, $Z = -0.545$, $p = 0.586$]. For the Messaging app, in contrast, the perceived importance of data security was significantly smaller in Study 1 than in Study 2 [$U(N_{\text{study1}} = 224; N_{\text{study2}} = 210) = 20{,}564.50$, $Z = -2.945$, $p = 0.003$], with a small effect size ($r = -0.141$). The Messaging app had mean data security importance of 8.44 ($Mdn = 9.0$; SD = 2.12) in Study 1 and of 8.27 ($Mdn = 9.0$; SD = 2.22) in Study 2.

Because the perceived data security importance varied statistically between studies for one of the apps (Messaging), Studies 1 and 2 datasets were not combined when evaluating differences in medians among the apps. Therefore, two Friedman tests were conducted, one for each study. The Friedman test—with Study 1 data—rendered $\chi^2(N = 219) = 113.784$, $p < 0.001$. This effect was replicated in a Friedman test with Study 2 data, rendering $\chi^2(N = 202) = 108.119$, $p < 0.001$. In Study 1, *post-hoc* analyses indicated that data security was perceived as significantly more important in the Messaging than in the Puzzle ($Z = -8.046$, $p < 0.001$, $r = -0.542$) and Weather apps ($Z = -8.380$, $p < 0.001$, $r = -0.562$), without significant difference between the Puzzle and Weather apps. As in Study 1, the analysis of Study 2 also indicated that data security was significantly more important in the Messaging than in the Puzzle ($Z = -8.407$, $p < 0.001$, $r = -0.584$) and Weather app ($Z = -7.942$, $p < 0.001$, $r = -0.556$), without significant difference between the Puzzle and Weather apps.

App installation intention

Figure 1C shows mean app installation intentions. Results of Mann-Whitney U tests (with Bonferroni adjusted p-value = 0.017) indicated that the intention to install the Puzzle, $U(N_{\text{study1}} = 226; N_{\text{study2}} = 210) = 22192.50$, $Z = -1.214$, $p = 0.225$, and the Messaging apps, $U(N_{\text{study1}} = 224; N_{\text{study2}} = 210) = 22873.00$, $Z = -0.522$, $p = 0.602$, were not significantly different between studies. The intention to install the Weather app in Study 1 ($M = 4.52$; SD = 1.98), however, was significantly lower than in Study 2 ($M = 5.89$; SD = 0.87); $U(N_{\text{study1}} = 226; N_{\text{study2}} = 212) = 18694.50$, $Z = -4.074$, $p < 0.001$, with a small effect size ($r = -0.195$).

Because the intention to install the Weather app varied statistically between studies, Study 1 and 2 datasets were not combined to evaluate differences in medians among the three apps. Two Friedman tests were conducted, one for each study. The Friedman test, with Study 1 data, rendered $\chi^2(N = 224) = 209.019$, $p < 0.001$. Results of the Friedman test, with Study 2 data, replicated Study 1 and rendered $\chi^2(N = 208) = 226.694$, $p < 0.001$. In both studies, *post-hoc* analysis with a Wilcoxon Signed-Ranks test indicated that the intention to install the Messaging app was significantly greater than both the intention to install the Puzzle ($Z_{\text{study1}} = -11.677$, $p_{\text{study1}} < 0.001$, $r_{\text{study1}} = -0.780$; $Z_{\text{study2}} = -11.397$, $p_{\text{study2}} < 0.001$, $r_{\text{study2}} = -0.788$) and the Weather app ($Z_{\text{study1}} = -7.032$, <0.001, $r_{\text{study1}} = -0.470$; $Z_{\text{study2}} = -3.877$, $p_{\text{study2}} < 0.001$, $r_{\text{study2}} = -0.268$). The intention to install the Weather app was greater than to install the Puzzle ($Z_{\text{study1}} = -9.475$, $p_{\text{study1}} = 0.000$, $r_{\text{study1}} = -0.630$; $Z_{\text{study2}} = -10.818$, $p_{\text{study2}} < 0.001$, $r_{\text{study2}} = -0.748$).

Number and type of data access permissions granted in study 2

Figure 3 presents the frequencies of numbers and types of data access permissions granted by respondents to the Puzzle, Weather, and Messaging apps in Study 2. For the Puzzle app, most participants reported willingness to grant access to none of the data types (on average, $M = 0.62$ permissions were granted). The most frequent number of permissions granted for the Weather app was one type of data ($M = 1.03$), namely, location (see Figures 3A,B). The number of permissions granted to the Messaging app was distributed almost equally from 1 to 4 ($M = 2.43$, see Figure 3A). In the Messaging app, access was granted most often to the location (156 times) and microphone (154 times), followed by internal storage (117), and somewhat less often to contacts (94).

Predicting the intention to install an app in study 2

Table 3 shows results of bootstrapped multiple regression analyses for the three apps in Study 2. In the Puzzle, Weather, and Messaging apps, the models explained 40.7, 29.5, and 60.5% of the variance in the installation intention, respectively. App importance was the only significant predictor of the intention in the three apps, Puzzle ($p = 0.001$, $B = 0.454$, 95% CI [0.379, 0.528]), Weather ($p = 0.001$, $B = 0.246$, 95% CI [0.182, 0.320]), and Messaging ($p = 0.001$, $B = 0.498$, 95% CI [0.413, 0.559]).

Discussion

Results of Study 2 confirmed that the decision to install an app is mostly determined by the perceived app importance, regardless of the permission format. Compared against Study 1, Study 2 also indicates that having more control over data access permissions can cancel the role of concerns in predicting the intention to install low to moderately important apps. Study 2 also shows that providing more control over data access permissions does not necessarily increase installation intention in comparison to Study 1. As shown, there was no significant difference between studies, except for a higher intention to install the Weather app in Study 2. Despite statistically significant, the difference was small and did not alter data trends across apps.

When respondents were presented with an explicit opportunity to choose specific data-access permissions in Study

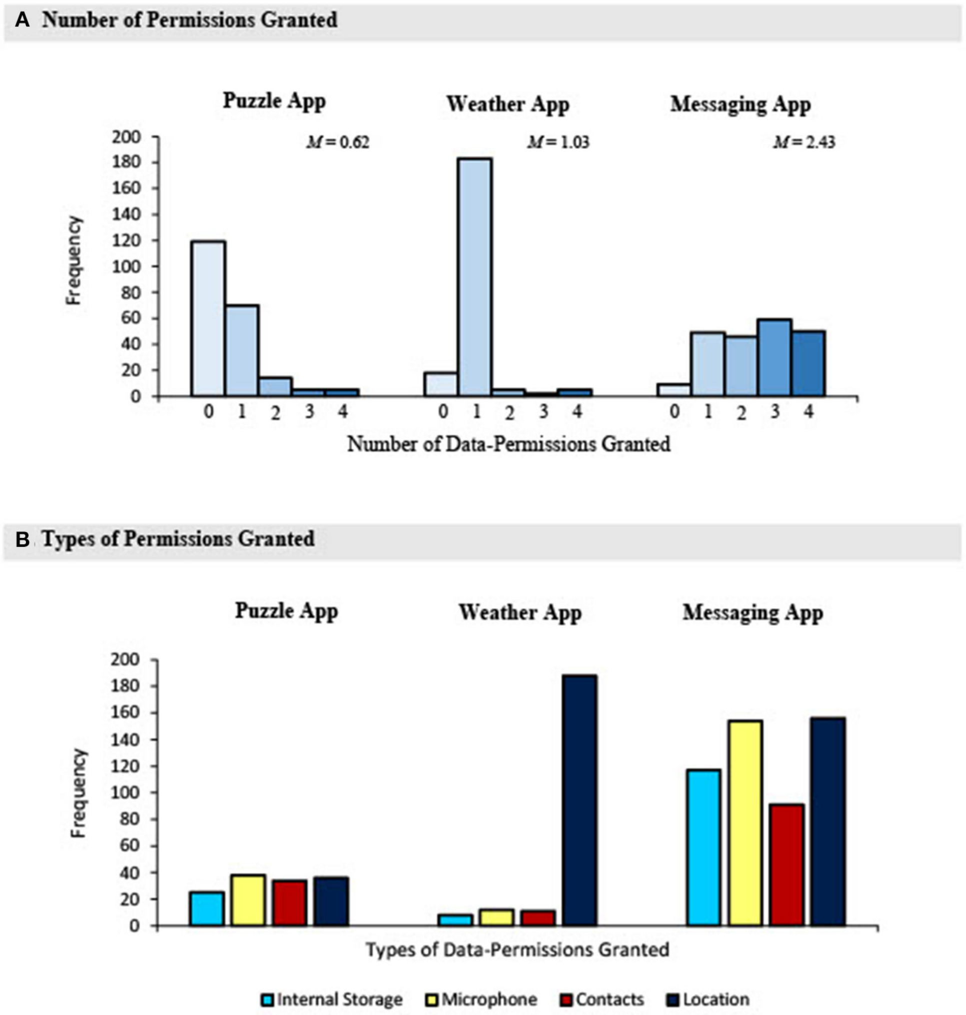

FIGURE 3
Frequency of number **(A)** and Type **(B)** of Permissions Granted per App, Study 2.

2, they tended to choose a small number of permissions which were consistent with the function of the app. Study 2 found that respondents tended to agree on which types of data were critical for the Puzzle and Weather apps to function (none for the Puzzle app, and location only for the Weather app). Participants differed yet in their understanding of what the Messaging app would require; the number of granted permissions was about equally distributed from one to four. In general, these results suggest that granting access to certain data seems to be more determined by the type of app than the degree of data sensitivity. For example, from our data from Study 2, it can be concluded that granting access to the location might be seen by the user as taking advantage of desirable location-sensitive features of a Weather app (Egelman et al., 2013; Zafeiropoulou et al., 2013), as well as photo storage can be an advantage of a Messaging app.

Previous research suggested that most people are unaware of which type of data is often needed for specific apps to work (e.g., Felt et al., 2012; Buck et al., 2014). Our results contrast with the literature and suggest that our respondents had partial knowledge about the type of data needed for an app to function. Our samples, therefore, may possess a higher degree of smartphone literacy than the general population. Smartphone literacy is a type of privacy literacy that includes, among others, knowledge about the type of data needed for an app to function (Ketelaar and van Balen, 2018).

General discussion

This paper contributes to discussions regarding psychological factors and processes affecting the intention

TABLE 3 Results of bootstrapped multiple regression analyses with intention of installing the app as dependent variable, study 2.

Independent variables	*B*	*SE*	Bias	*p*	BCa 95% CI	
					Lower bound	Upper bound
Puzzle app ($n = 196$)						
Smartphone privacy concern	−0.066	0.034	0.001	0.055	−0.135	0.005
App importance	0.454	0.038	−0.001	0.001*	0.379	0.528
App data security importance	0.004	0.028	0.000	0.902	−0.053	0.057
App discomfort	0.023	0.021	0.002	0.257	−0.012	0.069
Weather app ($n = 179^a$)						
Smartphone privacy concern	−0.021	0.027	−0.001	0.448	−0.075	0.031
App importance	0.246	0.031	0.003	0.001*	0.182	0.320
App data security importance	−0.018	0.023	0.000	0.458	−0.059	0.025
App discomfort	0.000	0.017	0.001	0.989	−0.034	0.034
Messaging App ($n = 197^b$)						
Smartphone privacy concern	−0.047	0.027	0.002	0.085	−0.103	0.014
App importance	0.498	0.036	−0.001	0.001*	0.413	0.559
App data security importance	−0.034	0.062	0.000	0.573	−0.190	0.088
App discomfort	0.003	0.006	0.000	0.625	−0.009	0.016

Bootstrap results are based on 1,000 bootstrap samples. BCa, Bias-corrected and accelerated.

*p < 0.05.

[a] Results concerning the Weather App were obtained after removing 18 outliers (case IDs 266, 276, 302, 306, 321, 328, 342, 363, 379, 382, 441, 264, 281, 286, 307, 308, 320, 332, 380, 392, 438). The removal of outliers did not change significant p-values, however, it allowed meeting the assumptions of multiple regression analysis—absence of significant outliers and homoscedasticity.

[b] Results concerning the Messaging App were obtained after removing 4 outliers (case IDs 379, 290, 363, and 388). The removal of outliers did not change significant p-values, but it allowed meeting the assumptions required by multiple regression analysis.

to install smartphone apps. First, the present research demonstrates that the importance given to the app's functionality is the strongest predictor of the intention to install it. The predictive value of app functionality on app installation is independent of permission design, whether the app predefines permissions (Study 1) or allows respondents to select them (Study 2). Therefore, the results of Studies 1 and 2 confirm the hypothesis that app perceived importance has a positive effect on app installation intention (H_4), replicating previous studies (e.g., Egelman et al., 2013; Shahidi et al., 2022).

Privacy concerns and the privacy paradox

Second, the present study demonstrates that e-privacy concerns are a sensitive measure and that both the levels of privacy concerns and their correlation with the decision to install an app vary depending on various parameters. Overall, respondents reported moderate to high levels of privacy concerns across all three dimensions measured. One dimension, the level of importance given to data security, varied depending on the number of data accessed and the type of app: the greater the number of data accessed, the greater the importance given to security in the Puzzle app. Another dimension, the level of discomfort, varied depending on data type: respondents considered access to photos and files more sensitive than access to location, microphone, and contacts. Together, these results are consistent with previous research indicating that certain dimensions of privacy concerns are affected by context (in this case, the type of app) as well as the type of data managed (e.g., Culnan, 1993; Anic et al., 2019).

Our research also demonstrated that the presence of correlations between privacy concerns and the decision to install an app varies across the different dimensions of privacy concerns. The level of concern related to smartphone use never correlated to installation intention (refuting H_1). However, other dimensions of privacy concerns—namely, the level of importance placed on data security within a certain app and the level of discomfort arising from the request for data access by an application—lowered the intention to install the Puzzle and Weather apps when respondents had less control, that is, when they could not choose the type of data accessed (in Study 1). These results supported hypotheses 2 and 3 (H_2 e H_3) that these other dimensions of e-privacy concerns may reduce installation intention. These results are relevant because they demonstrate that different facets of privacy concerns can interfere with the decision to install different apps. The variation in correlations regarding the different facets suggests that the use of different instruments to measure privacy concerns can contribute to variations in terms of conclusions across studies, sometimes showing the so-called privacy paradox, sometimes contradicting its existence (e.g., Acquisti and Grossklags, 2003; Egelman et al., 2013). Furthermore, these results are relevant because they suggest that contextualizing the construct of e-privacy concerns—within specific apps—can be a methodological strategy to optimize the detection of privacy concerns as a factor for installation. This finding is consistent with methodological research showing that presenting input information in questionnaire items similar to that available at the time of the actual decision (in this case, the app of interest) tends to increase attitude-behavior consistency (Schwarz, 2007).

Overall, the results suggested that app-specific privacy concerns (not general concerns regarding smartphone use) can have a negative effect on app installation intention under two particular conditions: when the user does not have fine-grained explicit control over which data access permissions they may grant (Study 1) and second, when the app is considered of low to moderate importance (Puzzle and Weather apps in our studies).

A note on the nature of benefits

As previously discussed, our results suggested that the degree of importance (or the degree of perceived benefit) of an app can affect the influence of privacy concerns on installation intention. Privacy concerns would be more likely to influence the intention to install apps with low to moderate perceived benefits. However, a study published recently (Gu et al., 2022) argued that not only the degree of benefits—but the nature of the benefits—produced by an app would influence the installation decision-making process (or the information processing mode, in the author's terminology). They argue that utilitarian apps trigger an analytical information processing mode in which individuals examine all available clues to form a privacy concern before balancing risks and benefits. Hedonic apps, in contrast, are assumed to elicit imagery processing, in which attention is governed only by obvious (or explicitly stated) privacy cues. In our study, the fictional apps Puzzle Game and Weather Forecast could be defined as hedonic and utilitarian, respectively. Evidence that privacy concerns have a stronger effect on the decision to install utilitarian than hedonic apps would support Gu et al.'s (2022) theory. In fact, we observed in Study 1 that the levels of privacy concerns had stronger negative effects on the intention to install the Weather Forecast (utilitarian) than the Puzzle Game (hedonic) app. On average, one degree of data security importance decreased the intention to install the utilitarian app (Weather Forecast) by 0.113 points. A degree of discomfort arising from granting data access permissions decreased the intention to install the hedonic app (Puzzle Game) by only 0.037 points. Therefore, privacy concerns had a stronger negative effect on the intention to install the utilitarian app than the hedonic app. These results support that categorizing the benefits produced by apps as hedonic or utilitarian might be useful for predicting the strength of the effects of privacy concerns on the intention to install the apps (e.g., Gu et al., 2022) in certain conditions. It is noteworthy that our results indicate that in the case of a Messaging app, privacy concerns are not related to installation intention. Messaging apps can hold both hedonic and utilitarian functions. Future research should determine whether the Messaging app affected responses differently from the other apps because of the high level of importance of the app's functionality or the nature of the benefits produced (both functional and hedonic).

Decision framing and the control paradox

Together, these results support the view that the decision to install an app may result from a privacy calculus, that is, the trade-off between the app's functionality and the user's privacy concerns (e.g., Dinev and Hart, 2006). The decision to install an app arises when the perceived potential benefits outweigh the potential risks of data disclosure. However, privacy concerns tend to be particularly less influential on users' decisions about whether or not to install an app, compared to benefits (Liu et al., 2015)—especially when individuals have greater control over which data can be accessed by the app. The psychological mechanisms through which a condition of increased control affects the decision-making process when installing apps remain to be explained. Some researchers argued that increased control could increase the intention to disclose personal data (H_5) by reducing the degrees of privacy concerns (H_6) (e.g., Hoadley et al., 2010; Brandimarte et al., 2012). In our study, a permission design, which gave respondents more control over permissions in Study 2, produced a small, albeit statistically significant, increase in the intention to install a medium-importance app (Weather). A condition of increased control (Study 2) did not affect the intention to install apps with extreme (very high or low) degrees of importance, such as our Puzzle and Messaging apps. Furthermore, we observed that in Study 2, respondents tended to choose to grant a small number of permissions that were consistent with the app function (especially for the Puzzle and Weather apps). Naturally, when installing an app, not granting access to any data type implies disclosing less information than granting access to multiple data types. Therefore, together, these results weakly support hypothesis 5 (H_5), that increased control (Study 2) would increase intention to install an app or disclose personal data, compared to a situation of less control (Study 1). Consequently, our findings limit the generalization of Brandimarte et al. (2012).

In our study, the design that gave respondents more control over permissions (Study 2) tended to reduce only one aspect of data privacy concerns: the discomfort triggered by granting data access permissions (especially for our Puzzle and Weather apps). That is, not merely having control, but exerting that control and not giving access permissions, reduced the level of discomfort. However, a condition of greater control did not affect the other aspects, the respondents' privacy concerns when using

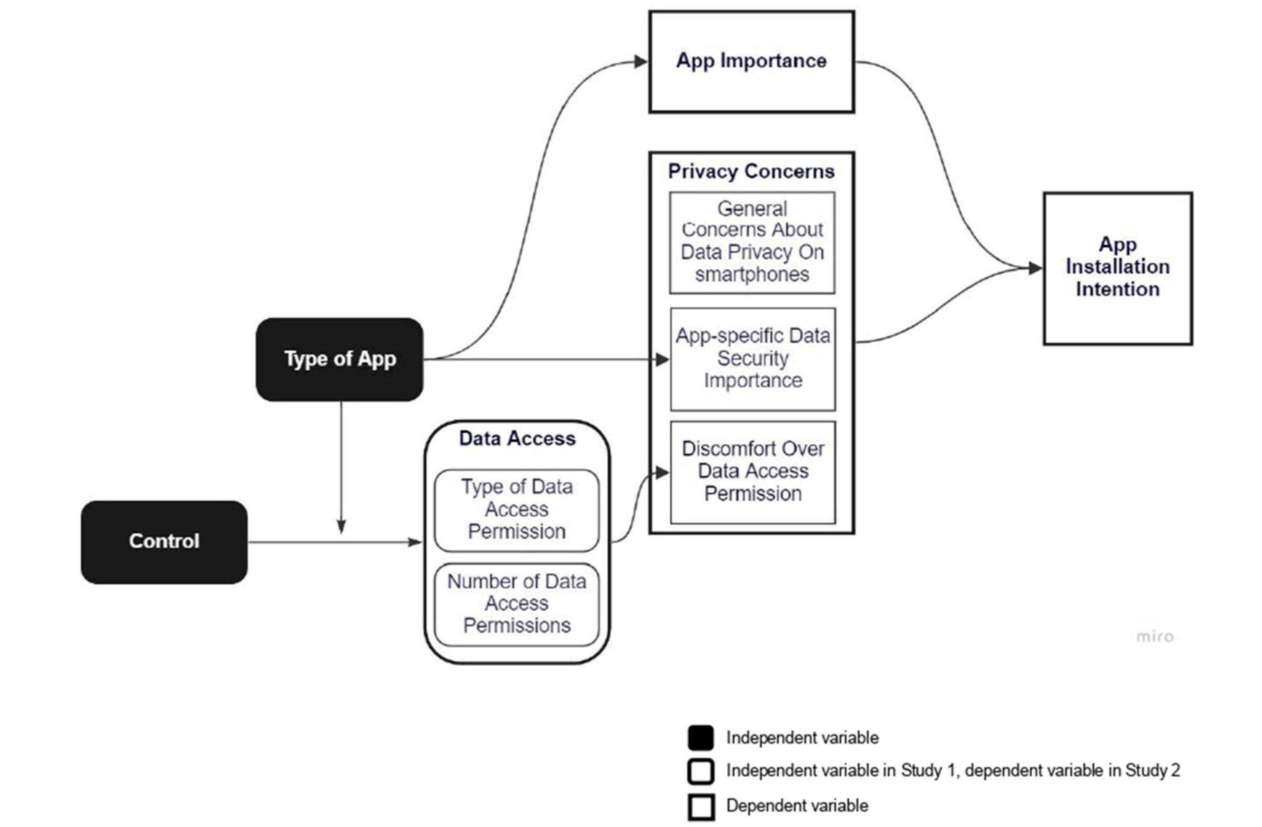
App Importance
Privacy Concerns
General Concerns About Data Privacy On smartphones
App-specific Data Security Importance
Discomfort Over Data Access Permission
App Installation Intention
Type of App
Control
Data Access
Type of Data Access Permission
Number of Data Access Permissions
miro
Independent variable
Independent variable in Study 1, dependent variable in Study 2
Dependent variable

FIGURE 4
Diagram of the relationships between the variables as indicated by the results. Privacy concerns dimensions that influenced app installation varied as a function of the type of app and degree of control over data access permissions (see Summary for details).

smartphones or the importance they gave to data security. These results support that higher control can reduce certain types of privacy concerns (Hoadley et al., 2010)—partially corroborating hypothesis 6 (H_6).

An interesting finding was that in Study 2—although there was no reduction in the level of importance attributed to data security—we no longer observed a correlation between this dimension of privacy concerns and the intention to install any app (unlike Study 1). These results expand the literature by suggesting that greater control can simply rule out the influence of concerns over the intention to install apps without necessarily reducing its level. While preliminary, these findings create an avenue for further theorizing and researching the conditions that shape the control paradox.

Although still limited, our results suggest that a condition of increased control can alter the decision-making process by decreasing certain concerns or the strength of their influence on the decision, compared to an "all-or-nothing" condition. However, this change in the decision-making process does not necessarily imply a change in the outcome of this process (i.e., the intention to install the app). It is possible that the resulting installation intention is less susceptible to variations in the level of control when the benefits of the app are perceived as extreme, that is, of very high or low importance. As previously discussed, we presume that this is because the benefits tend to dominate installation decisions. Therefore, our results contribute to the literature by suggesting that control effects on disclosure decisions—similar to the ones observed by Brandimarte et al. (2012)—are more likely to be observed in medium importance apps.

Summary

Figure 4 summarizes and illustrates how the analyzed variables seem to interact. The results indicate that the type of app plays a central role in determining both the perceived benefit of installing an app and the level of concern for data privacy, supporting recent studies (Gu et al., 2022). In the present study, the fictional Messaging, Weather, and Puzzle apps had functionalities considered of high, moderate, and low importance, respectively. The perceived benefit (or importance) of installing an app predicted the intention to install all apps. The type of app affected the degree of data security importance. Here, the Messaging app was perceived with a significantly higher degree of data security importance. The type of app also moderated the number and type of data access permissions granted (when participants had control over this decision in Study 2). In Study 2, a Game app correlated to granting access to no data, while a Weather app correlated to the disclosure of location data only. The number and type of data access permissions granted, in turn, determined the level of discomfort over data access. In the present research, both the level of discomfort over data access permissions and importance given to data security are considered facets of privacy concerns. These facets of privacy concerns decreased installation intention of low or moderate importance apps (Game and Weather) when the user had less control over the number and type of data accessed by the app (Study 1).

Implications

In general, our results suggest that it is important for policymakers to consider that consumers do not make choices as entirely free agents; their choices are highly influenced by contextual factors. High functionality apps can bias users toward installing the apps and disclosing their data. In particular, we found that—when the decision to install the app is coupled with the decision to grant several data access permissions ("all-or-nothing" decision frame)—users will install the app regardless of the number of data access permissions required as long as the app's utility is high enough. It seems to be a risk, then, that apps whose functions are considered extremely important may inadvertently lead users to disclose more data than they should and would want to. Therefore, this study adds to a body of research suggesting that it is relevant for commercial parties and policymakers to consider that just delegating responsibility to users may not necessarily reduce their vulnerability to the risks of data disclosure. Our results add to a body of research that supports the necessity of policies and principles such as privacy-by-design and privacy-by-default (cf. Schaar, 2010).

The contextual effects reported in this article could support the development of design-aware privacy policies that limit the use of design features that increase the chances of consenting to non-functional data collection (e.g., "all-or-nothing" decision frame) (e.g., Lin et al., 2012; Tsavli et al., 2015). While preliminary, our results, seem to suggest that increasing control over permissions can indeed function as a protective factor, as most of our respondents reported a preference for granting few (functional) data access permissions when they could. However, our results suggest indirectly that prior learning that provides a good understanding of the type of data needed for an app to function is a necessary condition for an informed decision to grant a few data permissions.

Limitations and further research opportunities

An important note regarding this study is about the sample. Participants in the present research were all recruited within the psychological faculty at the university campus in Norway. They can thus be expected to have a high educational level. Educational level has been positively correlated with the level of privacy literacy (e.g., Weinberger et al., 2017). Besides, we infer that our respondents had some knowledge about the type of data often needed by an app to function because they had the intention to disclose function-consistent data access permissions to some of the apps. Thus, our results may be specific to respondents with a certain level of expertise and knowledge. So, it may be necessary to consider demographic characteristics such as age, educational level and background when trying to generalize our findings to other populations. Future studies should expand the samples to people recruited in different contexts and include scales of privacy literacy (e.g., Trepte et al., 2015) or awareness about data collection techniques (e.g., Arpetti and Delmastro, 2021).

Another methodological limitation of the present research is that the chosen lower importance apps had functionalities that often require only few data access permissions to work. For example, in the case of the Puzzle app, a puzzle might be solved without access to personal files, contacts, microphone, or location. On the other hand, the chosen high-importance app was such with functionalities that might require access to multiple data for functional purposes. In the case of the Messaging app, access to both contacts and microphone is important. In practice, this correspondence between the nature of the benefits, the degree of importance, and data requirements is also observed in the real environment: Apps with more functionalities tend to be more popular, but also need more data to function. In theoretical terms, it is important for future studies to disentangle the relationships between the degree of importance of an app and the number of data needed by varying these aspects orthogonally. For example, in Study 1 we found that the discomfort produced by the number of permissions requested increased privacy concerns and decreased the intention to install an app considered to be of little importance; on the other hand, the discomfort produced by the permissions granted did not affect the intention to install an app considered highly important. It is unknown whether the number of permission requests raises concerns only for low-important apps or if the concerns were triggered by the request for access to non-functional data. To answer this question, future studies should include low-importance apps that request multiple functional permissions as well as high-importance apps that require few non-functional permissions. Similarly, future studies should disentangle the relationships between the degree of perceived benefit and the nature of the benefit provided by an app (hedonic, utilitarian or both).

Finally, we used fictitious apps and presented them in a questionnaire. This setting may not completely emulate the situation of granting permissions on smartphones in real life. An experimental study could recreate a more realistic context and observe users while operating real mobile devices.

Conclusion

Respondents tend to have moderate-high levels of privacy concerns. However, concerns are more likely to decrease the intention to install an app when the benefits are perceived as low or medium, and individuals do not have detailed control over the number and type of permissions granted (Study 1). These results support the existence of the privacy paradox (Barnes, 2006) in the context of apps, extending and generalizing the results reported by other studies about privacy decisions (e.g., Hann et al., 2002; Hui et al., 2007; Acquisti, 2009). These results also expand the literature by suggesting that the occurrence of a privacy calculus (Dinev and Hart, 2006) may be influenced by the user's level of control over data disclosure, although further research is needed. Our study produced mixed results regarding the control paradox (Brandimarte et al., 2012). A condition of increased control led to a small increase in the intention to install a medium-importance app, but it also tended to lead to a restriction in the amount of data shared with that app. We hope that the results presented in this article will inspire future research into the effects of control and concerns on app installation and other data sharing decisions.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

The study was registered in the university system of risk and compliance in the processing of personal data in research projects (RETTE). The methods were acknowledged by the Norwegian Center for Research Data (NSD; notification form 695287). The patients/participants provided their written informed consent to participate in this study.

Author contributions

VA-P processed the experimental data, performed the analysis, interpreted the results, drafted the manuscript, and designed the figures. AP conceived and planned the experiments and supervised the data collection. MK was involved in planning and conducting the data collection together with two other research assistants. GB and IT supervised the project. All authors discussed the results and commented on the manuscript.

Funding

This work was funded by the Research Council of Norway (project number 270969).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fcomp.2022.986138/full#supplementary-material

References

(n.d.-a). *Android Developers: System Permissions*, n.d.-a. Available online at: http://android.cn-mirrors.com/guide/topics/security/permissions.html (accessed August 26, 2022).

(n.d.-b). *iOS human interface guidelines: Accessing user data and resources*, n.d.-b. Available online at: https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/accessing-user-data/

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *Secur Privacy Econ.* 7, 82–85. doi: 10.1109/MSP.2009.163

Acquisti, A., and Grossklags, J. (2003). "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior," in *2nd Annual Workshop on Economics and Information Security,* 1–27.

Acquisti, A., and Grossklags, J. (2007). What can behavioral economics teach us about privacy?, in *Digital Privacy: Theory, Technologies, and Practices[eBook]*, eds. A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. and di Vimercati (Boca Raton, FL: CRC Press), 363–377

Acquisti, A., and Varian, H. R. (2005). Conditioning prices on purchase history. *Mark. Sci.* 24, 367–381. doi: 10.1287/mksc.1040.0103

Anic, I. D., Škare, V., and Milaković, I. K. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electron. Commer. Res. Appl.* 36. doi: 10.1016/j.elerap.2019.100868

Arpetti, J., and Delmastro, M. (2021). The privacy paradox: A challenge to decision theory? *J. Indus. Bus. Econ.* 48, 505–525. doi: 10.1007/s40812-021-00192-z

Barkuus, L., and Dey, A. (2003). "Location-based services for mobile telephony: A study of users' privacy concerns," in *Proceedings of the 8th International Conference on Human-Computer Interaction*, 1–4.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First *Monday* 11. doi: 10.5210/fm.v11i9.1394

Barth, S., and de Jong, M. D. T. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telemat. Inf.* 34, 1038–1058. doi: 10.1016/j.tele.2017.04.013

Boyles, J. L., Smith, A., and Madden, M. (2012). *Privacy and Data Management on Mobile Devices.* Washington, DC: Pew Research Center

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Soc. Psychol. Pers. Sci.* 4, 340–347. doi: 10.1177/1948550612455931

Buck, C., Burster, S., and Eymann, T. (2018). "An experiment series on app information privacy concerns," *Proceedings of the European Conference on Information Systems*, 178.

Buck, C., Horbel, C., Germelmann, C. C., and Torsten, E. (2014). "The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers," in *Proceedings of the 22nd European Conference on Information Systems*, 1–14.

Culnan, M. J. (1993). "How did they get my name?": an exploratory investigation of consumer attitudes toward secondary information use. *MIS Q.* 17, 341–363. doi: 10.2307/249775

Davison, A. C., and Hinkley, D. V. (1997). *Bootstrap Methods and their Application, 1*. Cambridge: Cambridge University Press.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *Int. J. Inf. Manage.* 50, 261–272. doi: 10.1016/j.ijinfomgt.2019.05.010

Dinev, T., and Hart, P. (2006). An extended Privacy Calculus Model for e-commercer transactions. *Inf. Syst. Res.* 17, 61–80. doi: 10.1287/isre.1060.0080

Egelman, S., Felt, A. P., and Wagner, D. (2013). "Choice architecture and smartphone privacy: There's a price for that," in *The Economics of Information Security and Privacy[eBook]*, ed R. Böhme (Berlin: Springer), 211–236.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., et al. (2012). "Android permissions: User attention, comprehension, and behavior," *Proceedings of the 8th Symposium on Usable Privacy and Security*, 1–14.

Gu, J., Tian, J., and Xu, Y. C. (2022). Private or not? The categorical differences in mobile users' privacy decision-making. *Electron. Commer. Res. Appl.* 52, 1–12. doi: 10.1016/j.elerap.2022.101122

Hann, I. H., Hui, K. L., Lee, T. S., and Png, I. P. L. (2002). "Online information privacy: measuring the cost-benefit trade-off," in *Proceedings of the 23th International Conference on Information Systems*, 1, 1–10.

Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. (2010). Privacy as information access and illusory control: the case of the Facebook News Feed privacy outcry. *Electron. Commer. Res. Appl.* 9, 50–60. doi: 10.1016/j.elerap.2009.05.001

Hui, K. L., Teo, H. H., and Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Q.* 31, 19–33. doi: 10.2307/25148779

Ketelaar, P. E., and van Balen, M. (2018). The smartphone as your follower: the role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Comput. Human Behav.* 78, 174–182. doi: 10.1016/j.chb.2017.09.034

King, J., Lampinen, A., and Smolen, A. (2011). "Privacy: Is there an app for that?," in *Proceedings of the Symposium on Usable Privacy and Security* (*SOUPS*). Pittsburgh: Symposium on Usable Privacy and Security.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Comput Secur.* 64, 122–134. doi: 10.1016/j.cose.2015.07.002

Lin, J., Amini, S., Hong, J., Sadeh, N., Lindqvist, J., Zhang, J., et al. (2012). "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. Pittsburgh, USA.

Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., and Zimmerman, J. (2011). "I'm the mayor of my house: examining why people use Foursquare—a social-driven location sharing application," *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*, 2409–2418.

Liu, B., Kong, D., Cen, L., Gong, N. Z., Jin, H., Xiong, H., et al. (2015). "Personalized mobile app recommendation: Reconciling app functionality and user privacy preference," *Proceedings of the 8th Association for Computing Machinery International Conference on Web Search and Data Mining*, 315–324.

Navarro, D. J., and Foxcroft, D. R. (2022). *Learning statistics with Jamovi: A tutorial for psychology students and other beginners* (*Version 0, 75.).* Available online at: https://www.learnstatswithjamovi.com

Nordgren, L. F., van der Pligt, J., and van Harreveld, F. (2007). Unpacking perceived control in risk perception: The mediating role of anticipated regret. *J. Behav. Dec. Making* 20, 533–544. doi: 10.1002/bdm.565

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *Int. J. Inf. Manage.* 55, 1–5. doi: 10.1016/j.ijinfomgt.2020.102178

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., et al. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Comput.* 13, 401–412. doi: 10.1007/s00779-008-0214-3

Schaar, P. (2010). Privacy by design. *Identity Inf. Soc.* 3, 267–274. doi: 10.1007/s12394-010-0055-x

Schwarz, N. (2007). Attitude construction: evaluation in context. *Soc. Cogn.* 25, 638–656. doi: 10.1521/soco.2007.25.5.638

Shahidi, N., Tossan, V., Bourliataux-Lajoinie, S., and Cacho-Elizondo, S. (2022). Behavioural intention to use a contact tracing application: the case of StopCovid in France. *J. Retail. Consum. Serv.* 68, 1–12. doi: 10.1016/j.jretconser.2022.102998

Spiekermann, S., Böhme, R., and Acquisti, A. (2015). Personal data markets. *Electron. Mark.* 25, 91–93. doi: 10.1007/s12525-015-0190-1

Statista. (2022). *Number of mobile app downloads worldwide from 2016 to 2021*(*in billions)* (2022). Available online at: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Trepte, S., Teutsch, D., Masur, P. K., Eichler, C., Fisher, M., Hennhöfer, A., et al. (2015). "Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)," in *Reforming European Data Protection Law,* eds S. Gutwirth, R., Leenes, and P.d, Hert (Netherlands: Springer).

Tsavli, M., Efraimidis, P., Katos, V., and Mitrou, L. (2015). Reengineering the user: Privacy concerns about personal data on smartphones. *Inf. Comput. Secur.* 23, 394–405. doi: 10.1108/ICS-10-2014-0071

Weinberger, M., Zhitomirsky-Geffet, M., and Bouhnik, D. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Inf. Rev.* 41, 655–671. doi: 10.1108/OIR-05-2016-0127

Yigitoglu, E., Gursoy, M. E., Liu, L., Loper, M., Bamba, B., Lee, K., et al. (2018). "PrivacyZone: a novel approach to protecting location privacy of mobile users," *2018 IEEE International Conference on Big Data* (*Big Data)*, 1238–1247.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., and O'Hara, K. (2013). "Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions?," *Proceedings of the 5th Annual Association for Computing Machinery Web Science Conference*, 463–472.

Zang, J., Dummit, K., Graves, J., Lisker, P., and Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technol. Sci.* 1–53. Available online at: https://techscience.org/a/2015103001/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30, 75–89. doi: 10.1057/jit.2015.5