The Impact of Data Privacy on Users' Smartphone App Adoption Decisions

FLORIAN BEMMANN, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany

Rich user information is gained through user tracking and power mobile smartphone applications. Apps thereby become aware of the user and their context, enabling intelligent and adaptive applications. However, such data poses severe privacy risks. Although users are only partially aware of them, awareness increases with the proliferation of privacy-enhancing technologies. How privacy literacy and raising privacy concerns affect app adoption is unclear; however, we hypothesize that it leads to a lower adoption rate of data-heavy smartphone apps, as non-usage often is the user's only option to protect themselves. We conducted a survey (N=100) to investigate the relationship between privacy-relevant app- and publisher characteristics with the users' intention to install and use it. We found that users are especially critical of contentful data types and apps with rights to perform actions on their behalf. On the other hand, the expectation of a productive benefit induced by the app can increase the app-adoption intention. Our findings show which aspects designers of privacy-enhancing technologies should focus on to meet the demand for more user-centered privacy.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → **Social aspects of security and privacy**.

Additional Key Words and Phrases: Privacy, app adoption, mobile devices

ACM Reference Format:
Florian Bemmann and Sven Mayer. 2024. The Impact of Data Privacy on Users' Smartphone App Adoption Decisions. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 278 (September 2024), 23 pages. https://doi.org/10.1145/3676525

1 Introduction

Mobile sensing data collected by smartphones is used for various purposes, such as fueling adaptive mobile applications or supporting research through the collected data. The better the device understands its user's behavior and context, the better an adaptive service is. Therefore, very detailed, contentful data types, such as detailed smartphone usage behavior or text contents, are especially interesting. As smartphones' current privacy-enhancing technologies (i.e., the permission system) cannot deal with such data sufficiently, privacy issues remain, making such data logging unacceptable for the user. Therefore, current operating systems restrict access to various functions (e.g., accessibility services), making it hardly usable for other use cases where users could benefit from Lee et al. [45], Naseri et al. [53]. Literature always says privacy is an issue for users, but we do not know which aspects contribute to how much. Yet, research does not understand the effects of individual data types, privacy-enhancing technologies, and other app characteristics concerning privacy decisions.

Authors' Contact Information: Florian Bemmann, LMU Munich, Munich, Germany, florian.bemmann@ifi.lmu.de; Sven Mayer, LMU Munich, Munich, Germany, info@sven-mayer.com.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM 2573-0142/2024/9-ART278
https://doi.org/10.1145/3676525

However, it would be important to understand how to build privacy-enhancing technologies that match the user's desires. We conducted an online survey to get quantitative insights into how specific app characteristics affect users' app adoption decisions. Depending on several app characteristics, we asked users about their willingness to install and use a new mobile app. We consider the data types used, privacy concerns, privacy-enhancing features around transparency and control, and the benefits that users expect from the app.

Our survey confirmed that users' main decision criteria for or against app adoption are the trade-off of privacy and expected benefit. Moreover, we uncovered more details on the specific data types and benefits. Using information about wallet- and account information induces most privacy concerns, followed by contentful datatypes such as text messages and microphone data. On the other hand, the expected benefits around productivity best mitigate these issues. Especially apps that help people pursue productive daily lives or offer a monetary incentive, which has a high likelihood of adoption.

Our findings show which app design settings designers and developers must be especially careful about, such as users' fears. We steer future work of privacy-enhancing technologies and underline the importance of better smartphone consent mechanisms, especially for contentful datatypes. Our work is of special relevance for designers of privacy-enhancing features in smartphone apps. Users' motivation to spend time in privacy is often limited. Thus, it is important to focus on the issues that raise the most concerns, such as the datatypes that users perceive as most privacy-sensitive in our study.

2 Related Work

2.1 General Factors Influencing App Adoption

A large body of literature studies why people adopt or neglect smartphone apps. These are mostly survey studies where users are asked about their general willingness to adopt an app regarding multiple constructs, such as interaction-based benefits [4], consumer experience, disposition, and perception [29], various dimensions of benefits [68], or personality [70]. Other studies apply between-subject approaches where participants' behavior was observed or intention asked for different vignettes (e.g., [9, 32, 64]). Furthermore, a few more open methodologies were applied, such as exploratory over-the-shoulder and interview studies (e.g., [17]). Studies thereby often found an app's reputation and popularity (i.e., ratings and reviews) being a relevant factor [25, 64], alongside a good expected benefit and expected performance [30]. Perceived permission sensitivity and justification also play a role, although research is contradictory regarding whether privacy concerns significantly impact [17, 25, 32]. Privacy-related aspects have to be regarded in context carefully, as users judge privacy intrusive behavior depending on whether they see value in the use case and perceive the collected data as relevant, therefore [34]. Another issue that makes the effects of privacy perception hard to estimate is its two-sided effect: Increased transparency and control features, on the one hand, improve user privacy [9, 26], but on the other hand the increased risk awareness increases user concerns [7, 12] and finally can reduce granted data access and app adoption [9, 34]. When regarding app adoption, it is important to be aware of which adoption stage one is regarding [72]. Of major importance regarding the final app adoption is the first contact between the user and the app.

Overall, prior work has brought up a variety of factors that influence app adoption, for example, the expected benefit, perceived permission sensitivity, the presence of transparency and control features, and users' risk awareness. However, prior studies have not yet compared these factors' influence on app adoption. Related studies were conducted for individual factors or subsets only (e.g., [17, 32, 64]).

2.2 Effects of Privacy on App Adoption

Research on the effects of privacy on app adoption has yet brought up inconsistent results. Hsieh and Li [32] point out in their related work that literature concluding with both opposing directions exist, also Bemmann et al. [9] in their context of privacy dashboards found contradicting literature: While studies of Gu et al. [25] and Boyles et al. [10] argue for privacy issues throttling app adoption and [66] finding that them being tackled having a positive effect, others such as Barth et al. [8], Dogruel et al. [17], Karwatzki et al. [36] conclude that privacy is not a relevant factor in their studies. Meta-studies explain these diverging results with a high context-dependency of privacy [1, 32] and that current studies do not regard all relevant variables yet. Besides the social expectations [65] (explained e.g. by the theory of contextual integrity, see Nissenbaum [54]) and past experiences [1], which can hardly be controlled in the present studies, characteristics of the apps themselves seem relevant [1, 17]. Users rely more on reviews and word of mouth than reviewing app permissions themselves [17, 38]: Download times and average user ratings can affect consumers' adoption behavior [6], also reviews and graphic rating systems [20]. Such app characteristics are rather understudied in present papers [32]. Opinions and experiences, by nature, have a high effect on one's trust, which might explain these aspects' relevance [18]. While people-centric psychological traits, states, and opinions have been studied and brought up a variety of mental decision models (e.g., [29, 32, 33, 68]), research on the effect of app characteristics is relatively sparse yet. Some studies show that app characteristics like reviews and ratings are factors [6, 20] with strong effect. Overall, the literature advises future work to take more app characteristics into account in addition to personal traits [17, 32]. Measuring privacy concerns is difficult; users' answers highly depend on their awareness at the moment and survey content wording, e.g., Braunstein et al. [11]. Cultural differences also make up strong differences and thus may explain contradictory literature [56]. While when speaking about privacy, research mostly refers only to the privacy of the acting users, the privacy of third persons should also be regarded. However, as third-person privacy has shown less relevance to people than one's own privacy, we do not regard this factor in our study [50].

Regarding the factors that influence user app adoption, especially personal aspects such as personality traits, states, attitudes, and opinions have been studied (e.g., [29, 33]). Characteristics of an app, for example, which privacy-enhancing features it incorporates, are rather understudied yet. Results of present studies are diverging [32], as insights have to be joined from multiple individual studies. However, methodological and contextual differences do not allow for comparing factors across studies.

2.3 Impact of Data Tracking

In this section, we regard the factors *datatype* and *permission sensitivity* more in-depth. Literature does not come to a common opinion on the magnitude of the effect that data logging has on the willingness to install an app. Studies by Boyles et al. [10], Gustarini et al. [27], Revilla et al. [61] conclude that data access requests are a major factor hindering app adoption. However, other studies, such as from Kreuter et al. [41], did not observe differences when comparing cases with and without invasive data requests. Also, in the study of [13], privacy concerns made only 16% not participate, and practical reasons such as time, information, and cost overweigh [58]. These differences may again be explained by contextual factors: Privacy concerns are initially not on the user's radar. Thus, the presentation of the study plays a crucial role in the participants' responses and behavior. Boyles et al. [10], for example, reports on high user concerns only after users learn about what information an app collects and shares post hoc. Gustarini et al. [27] even report which datatype being logged having the strongest factor. The differences between individual datatypes, especially contentful datatypes, namely video, photo, and audio, were identified as the most sensitive. In interviews,

participants expressed that the collection of these mainly influenced their decision against opting in. Location, which is also of high importance, depends on the interestingness of places: Users expressed more concerns about their home or work location than rarely visited other places. They were especially against logging if they thought that their routine could be revealed. Revilla et al. [61] ranked several datatypes from the context of mobile sensing studies by users' installation acceptance. Regarding smartphone sensing data, visited websites, emotion, and location rank very low in acceptance (below 21%). Users show less concern about data types and permissions that they understand. They have difficulties understanding permissions [38, 47] and inferring which data is collected precisely and what purpose it is fulfilling [27]. Studies around more in-depth data types like detailed device usage or device access, such as those provided by Android's accessibility services, are rare. Only very specific studies, for example Naseri et al. [53], have regarded users' perceptions of these.

Overall, research on the specific effects of sensing data types is rare. Prior work agrees that data access and privacy are major factors in app adoption decisions [10, 27, 61], but detailed insights on specific datatypes or types of permissions are rare. Furthermore, when it comes to rich, contentful data that is currently on the rise and needed to fuel novel intelligent interface concepts, little is known about users' perceptions of that. We do not know users' moods about using deep activity data. Also, because it's hardly possible now, there are not many examples.

2.4 Impact of Personal Benefits

Harris et al. [29] define *perceived benefit* as *"the extent to which a consumer believes he or she will benefit from installing an app"*. Literature subdivides it into *hedonic, utilitarian* and *social-integrative* benefits [4, 68], with further more detailed categories being proposed in some papers, for example the subdivision of *utilitarian* into *learning* and *personal integrative*. A list of concrete personal benefits has been collected in a qualitative study of Jung [35]. Related are also constructs on expectations that users have towards an app, such as presented by Lin et al. [47]. Malik et al. [49] unravel factors influencing hedonic and utilitarian app adoption related to personal benefits, namely enjoyment and incentives. Personal benefits are of rather high importance to users. In a study of Fang et al. [19], user benefits show strong explanatory power on app engagement, Kim and Han [39] has similar results in the context of mobile service adoption. Regarding effect differences between the categories of benefits, the literature has no common opinion. While Fang et al. [19] state especially hedonic and social benefits to have the most explanatory power, Kim and Han [39] find hedonic values contributing less, but instead social and utilitarian to be the strongest. Also important, however not included in the four above-mentioned dimensions of benefits, are monetary values. According to studies of Hong and Tam [31], Lee et al. [46], monetary value plays an important role in service adoption.

We conclude from prior work that the benefit that a user expects from app usage is one of the largest determinants for app adoption [19, 39]. Literature that mostly stems from behavioral psychology and marketing research has come up with taxonomies that bring structure into the space of personal benefits [4, 68]. However, it has not been studied yet how different personal benefits vary in their effect on app adoption behavior.

2.5 Related Constructs and Mental Models

Many mental models exist that describe parts of the user's decision and opinion-building processes relevant to app adoption. The *privacy calculus* describes how users weigh the risks/costs and benefits of an action [14]. Fleischhauer et al. [21] study it in the smartphone context and categorize users into groups. A couple of similar constructs exist in different domains, such as risk-benefit analysis, as part of information boundary theory [52, 57], the *theory of consumption* which describes

informed decisions of customers, focusing on the interplay of value assessments and, intrinsic, and extrinsic motivation Kim et al. [40]. The construct of *service - privacy fit* is an antecedent to the privacy calculus. It describes whether the service of an app matches its requests Hsieh and Li [32], Hurwitz [34], and is thereby part of the user's risk assessment. Its mediating effects are mainly benefit expectancy and perceived privacy concern about whose trade-off users decide. It stems from the older construct of *task technology fit*[24]. A model of factors yielding user's perceived information privacy perception is described by Dinev et al. [16]. The particularly relevant correlates to information privacy are anonymity, secrecy, confidentiality, and control.

While the presented models all play a role in the huge and complex decision-making landscape, no overarching decision model for smartphone app adoption decisions has been proposed. Each study and model contributes one or a couple of aspects to the field, but an interconnection and work that puts the different aspects in relation to each other are yet missing. Therefore, it is currently hard to understand which factors decide app adoption behavior in the big picture.

2.6 Research Gap

What strategy users choose and how they weigh the multiple aspects depends on personal and app-specific characteristics [17]. The literature identified, among others, the expected personal benefit, permission sensitivity, and public opinions as relevant factors [4, 10, 30]. However, prior work hardly brings these in relation to each other. Thus, individual studies examine the influence of specific aspects but rarely investigate their influence in the big picture of app adoption behavior. To gain insights on how much the proposed factors from related work facilitate or hinder app adoption, we put up our first research question:

RQ1 *Which app characteristics hinder or facilitate the adoption of a mobile sensing app?*

Moreover, so far, prior work focused on studying personality traits, opinions, and situations with respect to app adoption. Here, they merely pointed out that data logging increases privacy concerns, which is a major factor hindering app adoption. At the same time, we see major apps relying on data-heavy tracking to support users in their daily routines utilizing sophisticated prediction applications and machine learning models. On the other hand, literature shows when users become aware of how apps work, users show a strong non-willingness to install data-heavy tracking apps [9, 10, 61]. While a few works study the influence of extensive data tracking in general, research lacks evidence of the effects of data types. Thus, we advocate studying which app characteristics reduce app adoption, such as tracked datatypes. We address this open question with our second research question:

RQ2 *Which datatypes stop people most from adopting a mobile sensing app?*

Our study stands out from prior work by assessing a) a diverse set of factors, especially including specific logged datatypes and provided benefits, regarding b) their quantitative effect on users' app adoption intention. By specifying which app aspects and datatypes raise the most privacy concerns, our insights enable researchers and app developers to focus on the most critical privacy-enhancing features first.

3 Methodology

To quantify the effects that app characteristics, especially required data access and contained transparency and control features, have on smartphone users' app adoption intention, we conducted a large-scale online survey. The questionnaire consisted of three phases: 1) demographics, 2) effects of app characteristics on app adoption, and 3) differences between individual datatypes. We provide the questionnaire in the Supplementary Material. We describe our results descriptively and run

comparative tests, and finally, we discuss the implications of our results on future human-centered smartphone app privacy design.

3.1 Survey Design

In this section, we show the structure of our survey and explain how we came up with our questions and assessed items. We include all questions in detail in the *Supplementary Material Appendix*.

3.1.1 Part 1 - Demographics. In the beginning, we asked for participants' smartphone usage to confirm their study eligibility and assessed demographics (country, gender, age, education, occupation). To classify our sample regarding their technology and privacy predisposition, we also assessed affinity for technology interaction (ATI) [23] and the IUIPC questionnaire [48].

3.1.2 Part 2 - Factors on App Adoption. In part 2, we assessed participants' app adoption intention, depending on several app characteristics and perceptions. We assessed each aspect with multiple items that we derived from literature-based constructs (see breakdown in the bullet point list below) and calculated a score value for each aspect. We introduced the participants by telling them that we were interested in their decisions about installing and using a new smartphone app. All questions began with *I usually install an app on my personal smartphone...* following the adapted item. For example, *...if I feel I have control over my personal information that has been released* (one of the three items on transparency), or *... that requests sensitive personal information* as one of three items constituting permission sensitivity. Where appropriate, we opted for the more extreme wording of an item (i.e., using reinforcements such as "very"), as people in general agree that data is sensitive and risk-related. Thus, an extreme formulation yields better distribution in the responses [15]. We presented all statement questions using a slider ranging from *Strongly disagree* to *Strongly agree* on a 100-point scale without ticks and default selection (c.f. [51, 60] who have shown that sliders lead to more precise responses). To ensure high data quality, we included attention checks as a slider item, which had to be moved to the very left or right at the end of each phase. We assessed the following potential factors of app adoption:

- **Perceived Permission Sensitivity** Perceived permission sensitivity describes *"the level of discomfort users perceive when an app requests certain permission to control their mobile devices and use of their personal information"* [25]. We use this construct to estimate how much impact mobile sensing data access overall has on the app adoption intention. We adopted the items of Gu et al. [25] (SENS1 - SENS3), which they developed and validated with a confirmatory factor analysis (CFA) [22].
- **Benefit Expectancy** We measure the extent to which a user believes they will benefit from installing an app with the construct of *benefit expectancy*. We use three items that Hsieh and Li [32] adapted from Venkatesh et al. [67] and Lai and Shi [43], and adapted them to our context's wording.
- **Transparency Features** Privacy-enhancing technologies that offer transparency to the users are known to affect users' app adoption decisions [9]. We assess the three transparency aspects *data collection*, *process transparency*, and *data use transparency* through three subscales from Agozie and Kaya [2].
- **Control Features** Equivalent to transparency, we also assess the impact of control features. We base five items on those of Xu et al. [69].
- **Service - Privacy Fit** It describes whether the service of an app matches its requests Hsieh and Li [32], Hurwitz [34], from a user's perception. To assess the effect of the service-privacy fit on app adoption, we adapted the items used by Hsieh and Li [32], who adapted items on task-technology fit [24] from Yang et al. [71] and Laugesen and Hassanein [44].

- **Privacy** We assess the effect that potential privacy concerns have on app adoption with four items adapted from Gu et al. [25].
- **User Ratings** We create an item that asks for the relevance of app store ratings.
- **Trust in Publisher** We assess trust in the app and its publisher with adapted items from Duan and Deng [18], who adapted items on trust in system [55] and trust in organization [5].

3.1.3 Part 3 - Effects of Specific Characteristics. In the third part of our survey, we regard (1) datatypes, (2) publisher, and (3) personal benefits in more detail. We gathered a list of datatypes (respectively publisher types and personal benefits) from related work, and let participants rate them individually. Thereby, we create a more nuanced understanding of how these three factors affect an app adoption decision in detail.

Data Access. To compile a list of data accesses, we reviewed all Android permissions[1], accessibility service event types[2], and iOS permissions[3], and grouped them into human-understandable data types. We distinguish between read access and permissions that request write access or the ability to perform actions. For each data access, we ask users about (1) its perceived sensitivity and (2) potential risk. All data accesses are listed in the Supplementary materials.

Publisher. We let our participants rank four types of app publishers by how much they trust them to protect their privacy. We reviewed publishers in the Android and iOS app stores and found it comprehensive to cover *university*, *governmental organizations*, *companies*, and *non-profit organizations*.

Benefit. To break the expected benefits down in more detail, we collected specific benefits from related work. We used items based on Jung [35], formulated based on their code name and examples. We added *monetary incentive*, which is mentioned by Malik et al. [49] but not included in the codes of Jung [35]. We report on this rating separately and do not include it in the score on benefit expectancy.

3.1.4 Open Question. As the last element, we added an open-text question where participants could enter any feedback about the survey.

3.2 Pilot Testing

We piloted the study with 20 participants. We ensured that we received an appropriate data distribution, and checked for critical comments in the final open feedback question that could have hinted towards issues with understandability. Our pilot test did not raise any issues.

3.3 Procedure

We implemented the questionnaire in the survey tool Qualtrics and recruited participants through Prolific. We balanced the participant pool by gender, age, and country of residence and required participants to speak English fluently. We rewarded participation with 3£ as the study took approximately 17 minutes.

3.4 Participants (Survey Part 1)

We recruited 100 participants (47 female, 50 male, and 3 non-binary), aged 18 to 66 (M = 31.9, SD = 10.1). Most participants were either full-time (50) or part-time employed (24). A third (34) were students, and half held a university degree (35 had bachelor's degrees, and 20 had master's

[1] https://developer.android.com/reference/android/Manifest.permission
[2] https://developer.android.com/reference/android/accessibilityservice/AccessibilityService
[3] https://developer.apple.com/documentation/bundleresources/information_property_list/protected_resources

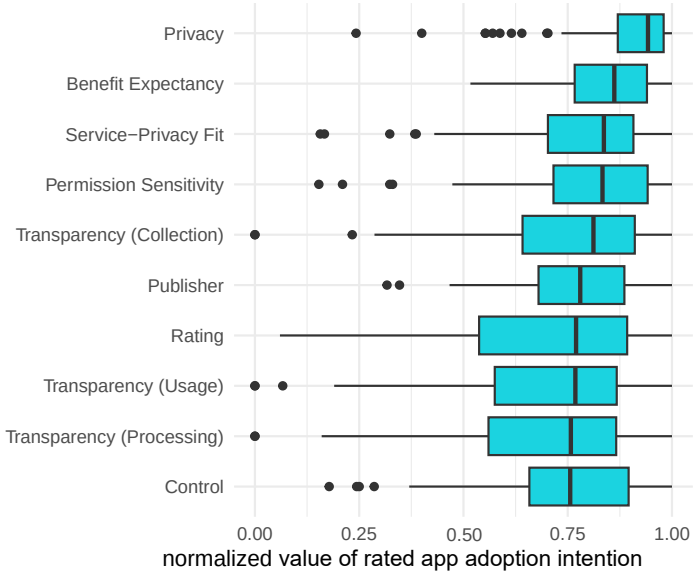


Fig. 1. Ratings of app adoption intention, for ten factors.

degrees). Most participants lived in Poland (13), South Africa (11) and Italy (10). To assess our sample's affinity with technology, we used the affinity for technology interaction scale (ATI) [23]. Its scale ranges from 1 (least affinity for technology) to 6 (highest possible affinity). Our sample had an average score of around 4 ($M = 4.13$, $SD = 0.82$). This indicates a tendency towards a higher technology-affine sample than the average population. According to the classification of Franke et al. [23], the ATI of an average population is to be expected at around 3.5, with high ATI samples around 4. Regarding the questions on perceived information privacy, our participants rated *Awareness* on average with 6.19 ($SD = .76$), *Control* with 5.83 ($SD = .87$), and *Collection* with 5.70 ($SD = 1.13$) (higher scores correspond to higher privacy).

4 Results

The participants took approximately 17 minutes to complete the study ($M = 16.83min, SD = 8.82min$). We ran the statistical evaluation in Python and R. Moreover, we applied non-parametric tests when normality was violated. We provide our data evaluation scripts alongside the anonymized data; see Section 7.

4.1 Factors to App Adoption (Survey Part 2)

In the second part of our survey, we assessed the relevance of a selection of factors to app adoption intention. We calculated the mean value over each factor's items, constituting a score value for each item. We inverted item values where necessary so that a higher score indicates higher app adoption intention for each factor. All scores were normalized to a value range from 0 to 1. The obtained scores are generally high, constituting a distribution that is shifted towards the upper end of the scale. Thus, our data is not normally distributed, so we regard the median instead of the mean in the following.

The strongest positive effect on app adoption intention was indicated for the factor *Privacy*, i.e., if users perceive an app as being privacy friendly ($Mdn = .94, SD = .14, min = .24, max = 1$).

Table 1. Descriptive statistics of the rated app adoption intention given that the respective feature is present in an app (left side). On the right, we show the p values of a pairwise Wilcoxon rank sum test (Bonferroni adjusted), for which we conducted post-hoc tests of a Friedman test.

					Post-hoc test									
Factor	**Mdn**	**SD**	**Min**	**Max**	Privacy	Benefit Expectancy	Service Privacy Fit	Permission Sensitivity	Transparency (Collection)	Publisher	Rating	Transparency (Usage)	Transparency (Processing)	
Privacy	.942	.137	.242	1.	–	–	–	–	–	–	–	–	–	
Benefit Expectancy	.862	.119	.517	1.	.057	–	–	–	–	–	–	–	–	
Service Privacy Fit	.837	.182	.157	1.	.	.764	–	–	–	–	–	–	–	
Permission Sensitivity	.833	.183	.153	1.	.001	1.	1.	–	–	–	–	–	–	
Transparency (Collection)	.812	.218	.	1.	.	.064	1.	1.	–	–	–	–	–	
Publisher	.780	.157	.317	1.	.	.035	1.	1.	1.	–	–	–	–	
Rating	.770	.241	.060	1.	.	.002	1.	.566	1.	1.	–	–	–	
Transparency (Usage)	.768	.245	.	1.	.	.001	.065	.136	1.	1.	1.	–	–	
Transparency (Processing)	.758	.239	.	1.	.	.	.467	.049	1.	1.	1.	1.	–	
Control	.756	.199	0.178	1.	.	.005	1.	1.	1.	1.	1.	1.	1.	

Thereafter, follow *Benefit Expectancy*, i.e.; users tend rather to install an app if they expect to have a benefit thereof ($Mdn = .86, SD = .12, min = .52, max = 1$). Thereafter follow the perceived *Service-Privacy Fit* (i.e., whether users perceive that the app's privacy invasions are appropriate regarding its provided service), *perceived permission sensitivity* and *Transparency about data collection* all with median scores above 0.8. With a median between 0.7 and 0.8 follow the type of *Publisher*, the app's *Rating*, and *Transparency about Data Usage*, *Transparency about Processing* and lastly, the presence of *Control features*.

The score on *Perceived Privacy* turned out to be significantly higher than all other factors except *Benefit Expectancy* (Friedman rank sum test with post-hoc pairwise Wilcoxon rank sum tests; $X^2(9, N = 100) = 128.21, p < .0001$). *Benefit Expectancy* also shows a significant difference with most factors. Besides, the only significant difference was detected between *Permission Sensitivity* and *Transparency about Processing*.

4.2 Factors in Detail (Survey Part 3)

4.2.1 Data Access. In four blocks, we asked our participants to rate each data access' (1) permission sensitivity and (2) perceived risk. We did that separately for permissions that depict read data access (*read* scope) and permissions that have write data access, i.e., perform some action (*write* scope). The rating was done on a continuous slider, yielding values between 1 and 100. The two measures *sensitivity* and *potential risk* show a significant moderate to strong correlation to each other ($r(98) \in [.49; .79]; p < .0001$), except for *reading wallet information*, whose correlation is only weak ($r(98) = .35, p < .0001$), cf., classification of Schober et al. [62]. Therefore, we will report on both measures together. Detailed independent values can be found in Table 2.

Read Data Access. The highest is rated data access to *wallet* and *account information*, followed by the contentful data accesses *text messages*, *microphone data*, *files and media*, *camera*, *location*, and *contacts*; see Figure 2. They all show a median-rated permission sensitivity of at least 82.5 and a potential risk above 82.0. After a gap of 12.5 points on the sensitivity scale and 7 points on the potential risk scale, users rank *screen content*, *keyboard typing data* and *data from smart home*

Table 2. Statistics of participants' sensitivity ratings and potential risk for various read and write scope data accesses. Pearson's correlation statistics show how the two assessed factors *sensitivity* and *potential risk* correlate (*** p<.001).

	Sensitivity		Potential Risk		Pearson Correlation		
Item	**Mdn**	**SD**	**Mdn**	**SD**	**r(98)**		**CI**
Read Data Access							
wallet information	99.5	17.5	100	20.1	.35	***	[.17;.51]
account information	94	21.8	94	26.3	.53	***	[.37;.66]
text messages and calls	91	27.2	90.5	28.4	.61	***	[.47;.72]
microphone data	89	30.4	87	30.2	.65	***	[.52;.75]
camera data	87	26.7	82	28.9	.66	***	[.54;.76]
location	84.5	26.3	86.5	28.6	.59	***	[.45;.71]
contacts	82.5	28.7	85	28.2	.64	***	[.50;.74]
screen contents	70	27.7	75	28.7	.62	***	[.48;.73]
data from smart home devices	65.5	30.3	67.5	30.2	.58	***	[.43;.69]
keyboard typing data	63	31.5	67.5	33.	.64	***	[.50;.74]
notifications	59	30.5	51	29.9	.49	***	[.32;.62]
calendars and reminders	58	30.3	53.5	30.4	.66	***	[.53;.76]
body sensors and health data	52.5	31.8	50.5	31.2	.70	***	[.58;.79]
interactions and touch behavior	51	28.3	54	27.5	.63	***	[.50;.74]
phone state	51	30.5	55	29.	.63	***	[.49;.73]
physical activity data	50.5	27.8	49	27.	.62	***	[.48;.73]
motion data	48	26.6	44.5	26.7	.59	***	[.45;.71]
usage statistics	47.5	26.6	46	30.	.73	***	[.62;.81]
music library	22	25.3	22.5	24.4	.59	***	[.44;.70]
Write Data Access							
send text messages	92	20.3	89	21.9	.73	***	[.63;.81]
edit contacts	89	22.8	81.5	24.	.69	***	[.57;.78]
install apps and packages	89	24.3	88	24.6	.66	***	[.54;.76]
add, edit, and delete files and media	87	24.4	88	25.8	.71	***	[.59;.79]
change my phone's state	67.5	31.8	63	31.	.72	***	[.61;.80]
access the internet	67	31.6	68	30.9	.79	***	[.71;.86]
edit calendar entries and reminders	65	27.9	65	30.	.75	***	[.66;.83]
send me notifications	49.5	30.6	44	30.3	.72	***	[.61;.81]
edit my music library	40.5	31.3	33	31.1	.74	***	[.63;.81]

devices with at least 63 points regarding sensitivity and 67.5 potential risks. For potential risk, we see another gap between the remaining data accesses. None reach a higher median than 55, while that is not the case for sensitivity (the next-highest data access at 59). The last and by far lowest ranked data access is *music library* with a median sensitivity of 22 and a median potential risk of 22.5. The second-last data access ranks at least twice as high for both scales.

Write Data Access. Regarding write scope data access, for both scales, the four permissions *send text messages*, *install apps*, *add, edit and delete files*, and *edit contacts* were rated the highest, showing a gap between 87 and 67.5 points in sensitivity respectively 81.5 and 68 points in potential risk;

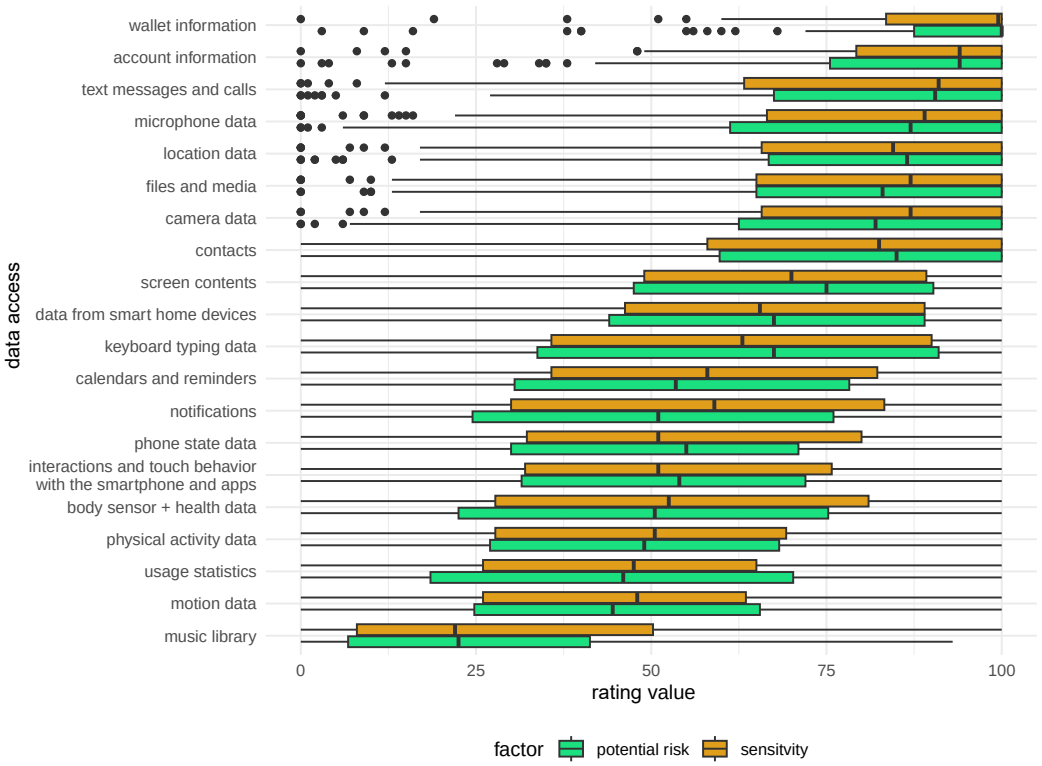


Fig. 2. Ratings of participants' perceived sensitivity and potential risk of different read-scope permissions.

see Figure 3. The following three data accesses *change my phone's state*, *access internet*, and *edit calendar entries and reminders* were rated between 67.5 and 65 in sensitivity, respectively 68 and 63 points in potential risk. With some distance, *send me notifications* and *edit my music library* are at the end of the spectrum with a sensitivity of 49.5 and 40.5 points and a potential risk of 44 and 33.

Differences Between Read and Write Scope Data Access. We compared the participants' ratings between the according read and write scope data accesses for all that can be paired to a respective read and write variant, see Figure 4. Write scope data access was rated more sensitive and imposing higher potential risk, except for *notifications*; there, users did rate oppositely. Differences are significant for both ratings of phone state ($p < .01$), notifications ($p < .05$), music ($p < .01$), the sensitivity of text messages and calls ($p < .05$) and contacts ($p < .05$), and the potential risk of calendar and reminders ($p < .05$) (paired Wilcoxon Signed rank tests).

4.2.2 Publisher. Regarding the app publisher (see Figure 5a), users rate apps published by universities as most likely to be adopted ($Mdn = 76, SD = 26.9$) and non-profit organizations as second ($Mdn = 61.5, SD = 28.0$). Thereafter, governmental organizations ($Mdn = 52, SD = 30.1$) and the lowest app adoption intention were rated to companies ($Mdn = 35.5, SD = 28.1$). The best-rated option *university* and the last option *company* each differ from all other options significantly (Friedman rank sum test with post-hoc pairwise Wilcoxon rank sum tests; $X^2(3) = 79.02, p < .0001$).

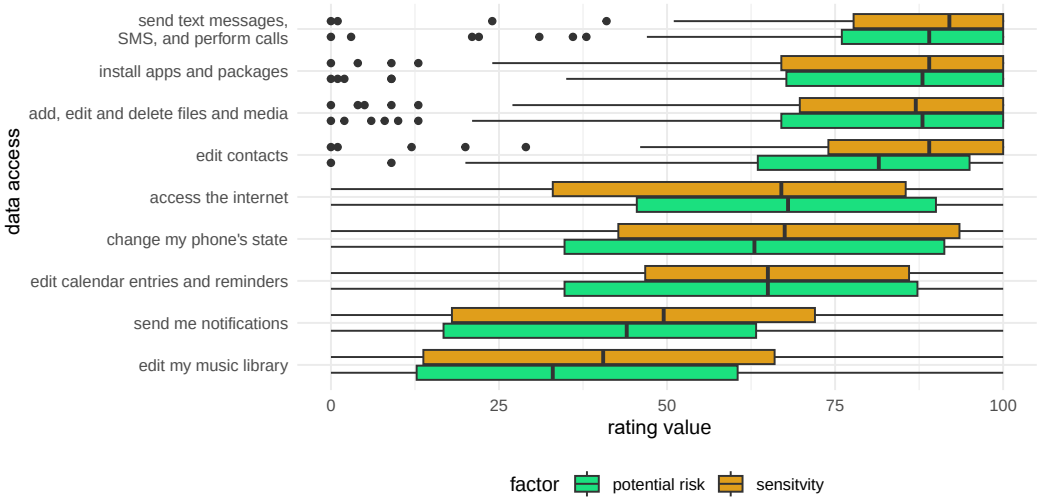
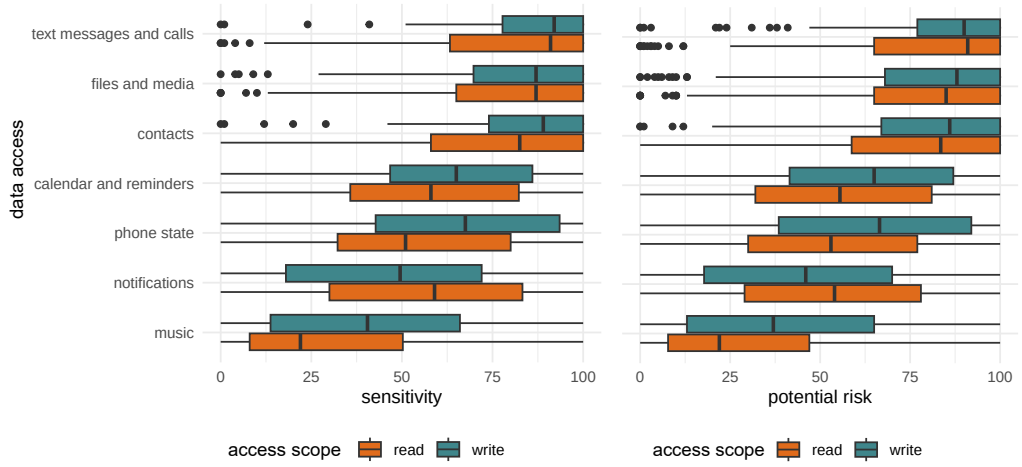


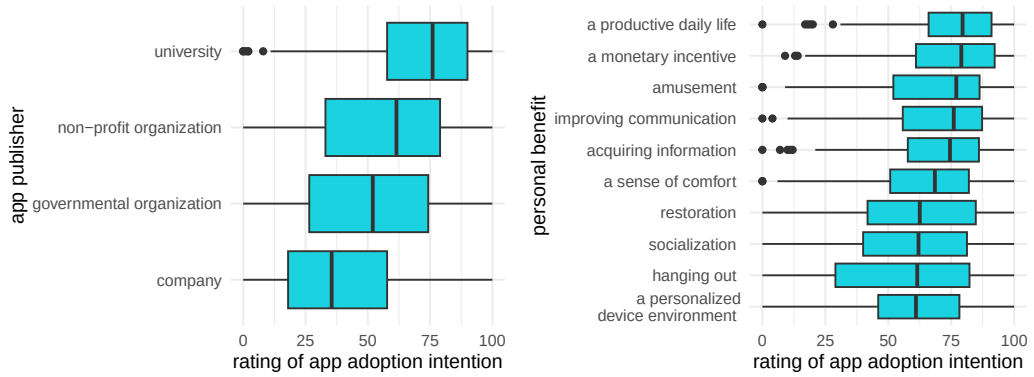
Fig. 3. Ratings of participants' perceived sensitivity and potential risk of different write-scope data accesses.



(a) Sensitivity (b) Potential Risk

Fig. 4. Pairwise comparisons of read and write scope permissions show that users rate write permissions more sensitive and impose higher potential risk than their read equivalent, except for notification access.

4.2.3 Personal Benefits. The ratings of personal benefits regarding app adoption intention indicate that participants' app adoption intention does not differ that much by which personal benefit an app provides; see Figure 5b. The medians of all ten rated benefits range between 79.5 and 61 and thus show less spread than the other factors that we assessed. The top five benefits are goal-oriented, rather productive benefits (*productive daily life* ($Mdn = 79.5, SD = 22.1$), *monetary incentive* ($Mdn = 79, SD = 23.3$), *amusement* ($Mdn = 77, SD = 25.4$), *improving communication* ($Mdn = 76.5, SD = 22.7$) and *acquiring information* ($Mdn = 74.5, SD = 24.4$)). Less concrete and



(a) App Publisher (b) Personal Benefit

Fig. 5. While participants indicated clear differences in their willingness to adopt an app between different publishers, the differences between various personal benefits are rather low.

more leisure-focused benefits show up at the end of the rating: *Sense of comfort* ($Mdn = 68.5, SD = 24.1$), *restoration* ($Mdn = 62.5, SD = 27.7$), *socialization* ($Mdn = 62, SD = 27.0$), *hanging out* ($Mdn = 61.5, SD = 30.7$), and *personalized device environment* ($Mdn = 61.0, SD = 25.3$).

4.3 Demographic Effects

We additionally explored whether the demographic characteristics of our participants influence app adoption intentions. We took age and education level as independent variables and correlated them with participants' stated app adoption intentions for the ten app factors (see Section 3.1.2), sensitivity and risk of individual data accesses, and overall sensitivity and risk perception of read and write data access. We conducted Pearson's product-moment correlation tests for correlations involving age (numeric, interval-scale variable). We conducted a Kruskal-Wallis test for those involving education (ordinal variable of 6 education levels).

We did not find any significant correlation between age and education with the reported app adoption intentions of the ten app factors. We only find a marginally significant negative correlation between *age* and *rating*, indicating that a good rating of an app in the app store could be more important for younger than for older people ($r(98) = -0.196, p = .051$). Also, for aggregated app adoption intentions of (1) read and (2) write data access, we only found some marginally significant tendencies that require further studies to draw conclusions. Participants of higher age could perceive write data access as more sensitive and risky than younger participants ($r(98) = 0.168, p = .094$). All results are reported in detail in the Appendix, tests regarding the app adoption intention of the ten factors in Table 3, results regarding correlations between age and education with specific read and write data access in Table 4 respectively Table 5.

Making pairwise correlation tests of age and education with specific read and write data accesses, we, however, found some correlations. Higher age correlates with a higher perceived sensitivity of *read contacts* data access ($r(98) = 0.201, p = .045$), a higher education level correlates with higher perceived sensitivity of *read interactions and touch behavior* ($r(98) = 0.105, X^2(5, N = 100) = 11.885, p = .036$). Regarding writing data access, a higher age correlates significantly with higher perceived sensitivity of *sending me notifications* ($r_{age}(98) = 0.295, p_{age} = .003$), and higher education with higher perceived risk ($r(98) = 0.249, X^2(5, N = 100) = 11.272, p = .046$). *Accessing the internet* was perceived as more sensitive ($r(98) = 0.273, p = .006$) and risky ($r(98) = 0.256, p = .010$) by older

people. Lastly, we found that education decreases the perceived risk of write data access to *files and media* ($r(98) = -0.080, X^2(5, N = 100) = 11.975, p = .035$) and *contacts* ($r(98) = -0.057, X^2(5, N = 100) = 11.253, p = .047$).

5 Discussion

In this section, we recap the research questions and their motivation and discuss how our study's results contribute to them. We derive recommendations for app designers and researchers, and finally critically discuss the limitations of our study and what future work remains in its domain. In contrast to insights from prior work, we provide a quantification of the effects of specific app factors on app adoption and unravel users' perceived permission sensitivity and risk in individual data accesses.

5.1 RQ1: The Ratio of Privacy and Benefits Mainly Decides App Adoption Behavior

Our review of related work has shown that, while literature has pointed out many aspects that are relevant to app adoption decisions, their relative importance in comparison to each other has not been studied yet. We approach this gap with our first research question: *Which app characteristics hinder or facilitate the adoption of a mobile sensing app?*

Our ranking of the importance of factors for app adoption (see Section 4.1) shows that the ratio of privacy and benefit matters most for potential users. The top 4 rated factors to app adoption all relate to privacy and benefits. In general, that aligns with past work where related constructs are studied, such as the privacy calculus (e.g., [21, 37]), although the very high rating of privacy exceeded our expectations. Our study supports the findings of Harris et al. [29], who state that privacy-related aspects are more relevant than app reputation. It is notable that the vague, abstract concept of *privacy* ranked way higher than the more concrete factor of *permission sensitivity*. Also, with the low scoring of transparency and control, users express a comparatively low desire for privacy-enhancing features. We assume that current privacy-enhancing technologies are simply not present enough in systems to users - thus, users are still rather overwhelmed by the issue and do hardly see ways to mitigate it. This may, in effect, explain the high presence of user frustration and perceived helplessness and resulting resignation, that is reported, e.g., by Schomakers et al. [63]. Prior work such as Hsieh and Li [32] pointed out the relevance of the promotion of privacy-enhancing measures, which our findings underline. However, prior work on the promotion of privacy-enhancing features is rare. While related constructs such as familiarity and reputation (e.g., in Harris et al. [29]) have been studied, to the best of our knowledge, no dedicated study on promotional strategies for privacy-enhancing features exists yet. We motivate that more effort should be spent on this, as in line with our findings also Bemmann et al. [9] have found that the presence of privacy-enhancing features and the promise of being in control all time, made the difference for user perception.

5.2 RQ2: Users Are Most Concerned About Leakage of Contentful Data and Actions on Their Behalves

In the literature, we found a lack of evidence on how specific data access and provided benefits are regarded by users towards app adoption. We let users rate a set of data accesses and benefits to get insights on our second research question: *Which data accesses stop people most from adopting a mobile sensing app?*

To gain a deeper understanding of the two aspects *privacy* and *benefits*, we let users rank their characteristics more specifically in Section 4.2, to go beyond the insights of existing literature.

In contrast to the ratings of general factors to app adoption (see Section 4.1), the ratings of specific data accesses covered the full spectrum of our scale for each data access. While the lowest,

respectively, highest ranked factor to app adoption in Section 4.1 has a median of 75.6% resp. 94.2%, the ranking of individual data accesses in Section 4.2 range from a median of 22 to 99.5 on the same scale. This shows a variance in the perception of datatypes and permissions. Although permission sensitivity was rated as highly relevant to app adoption decisions ($Mdn = 0.833, SD = 0.183$, see Section 4.1), this does thus not hold for all permissions likewise. Designers of privacy-enhancing technologies should thus differentiate by the perceived severity of permissions when designing their interfaces.

Identity- and Financial Theft. *Wallet information* and *account information* rank highest on our scale of perceived sensitivity and potential risk. These are not of an informational nature that reveals something about their user, but rather can give third parties access to one's resources and may enable identity theft. This is in line with *send text messages* being rated as the most concerning writing data access, which also depicts some sort of identity theft. We conclude that users are generally most afraid of outcomes that affect their financial status and online identity.

Misuse of Contentful Datatypes. Besides the identity-related datatypes, we see datatypes that are contentful, i.e., user-centric information that may contain private topics, which rank high. Namely, these are *text messages and calls*, *microphone data*, *files and media*, *camera data* and *screen contents*. Within these also occur *location data* and *contacts*, which, however, are rather an observed property of the user respectively actively entered collection of information. The information value contained therein is diverse and can range from worthless ambient noise to personal private conversations.

5.2.1 Productive Benefits over Leisure stuff. In the ranking of the effect that several benefits that an app provides have on the app adoption intention, we see that productive and user-oriented benefits make a stronger impact on app adoption than fun and leisure-oriented apps. *A productive daily life* as app purpose even surpasses *a monetary incentive*. The rather abstract purpose *amusement* is the only non-productivity benefit that was rated to the upper half of the spectrum by our participants.

5.3 Users Do Hard Implying Privacy Risks of Abstract Data Types

From the literature, we know that users do hard estimating which high-level information about them can be inferred from low-level data, such as raw sensor values [28, 42]. Our study shows that this also applies to less abstract data types: Interestingly, users rated potential risk and sensitivity of *screen contents* only on rank 9, and thus lower as, e.g., *text messages* or *files and media*. This shows that, although it might be logical for most users that screen content can also contain textual content, it is perceived as less sensitive at first sight, as the informational content is less abstract. We advocate future research to investigate potential solutions to this issue. Ambient interface concepts that, without the user actively looking for them, convey a sense of hidden information in abstract and rich data, which helps users be informed about privacy risks induced through feature extraction and inference.

5.4 Transparency and Control: Users Act Short-Sighted

Interestingly, *Control* ranks rather low, while *Transparency* ranks rather high. At first sight, that contradicts existing research: For example, Bemmann et al. [9] found that adding *Control* significantly increased app adoption rates, while *Transparency* did the opposite. This contradiction of results between our hypothetical study and in-the-wild experiments as the one of Bemmann et al. [9] again shows that people do hard estimating privacy preferences and stating concrete desires. *Transparency* is the first step that they desire, and people assume they will feel better protected by it. However, in practice, as soon as *Transparency* is given, people become aware of logged data and processing practices, which induces the opposite. They feel more invaded and less safe than

before. Only the addition of *Control*, which allows them to control these things, actually mitigates their concerns in practice. While this effect is notable in experiments, people do not indicate that in hypothetical settings such as surveys and vignette studies, likely because they do hard judging privacy far-sighted. This aligns with past findings that the gap between stated intentions and actual behavior is especially prominent in the privacy domain (e.g., Keith et al. [37]), and an omnipresent lack of awareness when it comes to smartphone security practices [3]. For researchers and app developers, this implies that solutions need to be found to convey the omnipresent availability of control features to app users. Without annoying the user and occluding interfaces, users need to be made aware of these features' omnipresence. Current privacy-enhancing features hardly meet this trade-off, being either hidden in deep menus or annoying their users by requiring disproportionate interface space and mental user capacity.

5.5 Recommendations to App Designers

Consider twice whether a permission is needed. Maybe there's an easier, less invasive way to implement a feature? Prior work [32, 34] and our results have shown the importance of a good service-privacy fit. Especially for permissions that, at first sight, do not meet the application's purpose, app developers should act carefully. For permissions whose purpose is not obvious, reasoning should be provided.

Convey clearly and proactively how its data is used. If users see a good service-privacy fit, they are more likely to adopt an app [32, 34]. They, in general, accept data processing to a huge extent if it meets a desired purpose [59]. However, as many users (e.g., the privacy cynics, c.f. Schomakers et al. [63]) are not actively looking for privacy information, reasoning of an app's service-privacy fit and the thereof generated benefit needs to be conveyed proactively.

Consider a Permission's Specific Perceived Sensitivity and Risk. When considering privacy-enhancing features for their apps, developers have to decide how much they want to bother their users with privacy information and decisions. They have to weigh the effort that they enforce to their users (i.e., time that they make users spend with privacy information and decisions) and the provided privacy benefits (i.e., gain of privacy benefit that users perceive by dealing with their privacy). In the trade-off decision, the perceived sensitivity of the specific permission and data type should be considered. Thus, for permissions that we found to be perceived as less sensitive and risky, users can be confronted less with privacy-enhancing interfaces.

5.6 Calls for Research: Privacy Enhancing Technologies for Contentful Data Needed

Current privacy consent mechanisms are rather limited in their options. Usually, one can only completely grant or deny access to a datatype. Therefore, all datatypes are treated similarly without considering the inherent differences that they pose. For example, different granularities could be offered for location or microphone data, and the user's context may be considered. The span of inherent information is wide, and with nowadays all-or-nothing permission concepts such data cannot be used in a privacy-respectful way. Our study thereby motivates the design and evaluation of novel privacy-enhancing technologies, especially for contentful datatypes. We especially call operating system developers to improve on this. The smartphone permission system is not in the app developer's hands. Thus, studies and proposed concepts initially have rather low impact. Nevertheless, we argue that evaluating alternative concepts and investigating the underlying factors from the user perspective is important to motivate operating system developers to spend effort on that topic and guide them in promising directions. If the proposed concepts were implemented, app developers and users would benefit: Besides gaining increased privacy and mitigating risks, they would benefit from more adaptive and intelligent apps fueled by rich, detailed data.

5.7 Effects of Personal Characteristics

Individual characteristics of users, such as personality traits, also affect their app adoption intention. We look at these factors only peripherally, as a large body of related work yet did so (e.g., Xu et al. [70]). Our analysis of the effects of age and education nevertheless shows some interesting effects. Especially the high correlation of age with the perceived sensitivity and risk of allowing an app to access the internet shows that perceptions differ among different age groups. While younger people take internet access as usual, older people might not regard internet access for apps as usual. However, demographic analyses are not our study's main objective. Thus, it is not ideally designed, therefore, especially regarding the sample size and composition. Based on the tendencies that we found, our results motivate future research to take a close look at such aspects. The correlations that we report need to be regarded with care. Due to the high number of pairwise comparisons, the significant correlations that we found can be misleading and occur just by random chance. We nevertheless considered it interesting to report them to guide future research toward aspects to look into in more depth.

5.8 Limitations

The applied methodology was specifically designed to compare a wide and diverse set of factors. We, therefore, applied a within-subject design, where each participant rates each aspect individually, which allows us to assess that with relatively low participant efforts; however, it also comes with limitations. The results indicate the relative ratio between the factors but do not tell much about the absolute app adoption likelihood. While we find which factors are more important than others, we cannot conclude in which order of magnitude of app adoption likelihood a combination of factors situates. Therefore, a vignette study with a factorial design (e.g., Bemmann et al. [9] applied) would have been necessary to ask users for their app adoption intention of multiple hypothetical app compilations. However, this is not possible in line with our aim to assess a large number of factors, as the number of vignettes that users had to rate would become very large.

Although we tried to recruit participants with diverse backgrounds through a panel service, our sample with $N = 100$ can, of course, not be coined representative. While we included participants from various countries, age groups, and professions, way more participants would have to be recruited to get representative results.

6 Conclusion

In this paper, we shed light on app characteristics that hinder and facilitate smartphone users' app adoption intention. In a survey ($N = 100$), we confirmed that the main decision criterion is the trade-off between privacy concerns and expected benefits. Building on this, we extended prior knowledge with insights on specific data types and benefits. Users were most concerned about their account- and wallet information being used by apps, alongside contentful datatypes such as text messages or microphone data. While these concerns throttle the app adoption intention, the expectation of benefits brought by an app mitigates the concerns. Especially benefits around productive app purposes rather than increasing the app adoption intention. Our results help app designers understand which features might lead to non-adoption of their apps, and point out necessary further research, especially concerning privacy-enhancing technologies for contentful datatypes.

7 Open Science

We encourage readers to reproduce and extend our results. Therefore, we made the data collected in our study and our analysis scripts available on the Open Science Framework https://osf.io/6wpju/.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.1126/science.aaa1465

[2] Divine Q Agozie and Tugberk Kaya. 2021. Discerning the effect of privacy information transparency on privacy fatigue in e-government. *Government Information Quarterly* 38, 4 (2021), 101601. https://doi.org/10.1016/j.giq.2021.101601

[3] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[4] Ibrahim Alnawas and Faisal Aburub. 2016. The effect of benefits generated from interacting with branded mobile apps on consumer satisfaction and purchase intentions. *Journal of Retailing and Consumer Services* 31 (2016), 313–322. https://doi.org/10.1016/j.jretconser.2016.04.004

[5] Catherine L Anderson and Ritu Agarwal. 2011. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research* 22, 3 (2011), 469–490. https://doi.org/10.1287/isre.1100.0335

[6] Sandeep Arora, Frenkel Ter Hofstede, and Vijay Mahajan. 2017. The implications of offering free versions for the performance of paid mobile apps. *Journal of Marketing* 81, 6 (2017), 62–78. https://doi.org/10.1509/jm.15.0205

[7] Naveen Farag Awad and Mayuram S Krishnan. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly* 30, 1 (3 2006), 13–28. https://doi.org/10.2307/25148715

[8] Susanne Barth, Menno DT de Jong, Marianne Junger, Pieter H Hartel, and Janina C Roppelt. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics* 41 (2019), 55–69. https://doi.org/10.1016/j.tele.2019.03.003

[9] Florian Bemmann, Maximiliane Windl, Jonas Erbe, Sven Mayer, and Heinrich Hussmann. 2022. The influence of transparency and control on the willingness of data sharing in adaptive mobile apps. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI (2022), 1–26. https://doi.org/10.1145/3546724

[10] JL Boyles, A Smith, and M Madden. 2015. Apps and privacy: More than half of app users have uninstalled or decided to not install an app due to concerns about their personal information. http://pewrsr.ch/1m8FevL

[11] Alex Braunstein, Laura Granka, and Jessica Staddon. 2011. Indirect content privacy surveys: measuring privacy without asking about it. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 15, 14 pages. https://doi.org/10.1145/2078827.2078847

[12] Sunny Consolvo, Jaeyeon Jung, Ben Greenstein, Pauline Powledge, Gabriel Maganis, and Daniel Avrahami. 2010. The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (Copenhagen, Denmark) *(UbiComp '10)*. Association for Computing Machinery, New York, NY, USA, 321–330. https://doi.org/10.1145/1864349.1864398

[13] Mark de Reuver and Harry Bouwman. 2015. Dealing with self-report bias in mobile Internet acceptance and usage studies. *Information & Management* 52 (2015), 287–294. https://doi.org/10.1016/j.im.2014.12.002

[14] Kenan Degirmenci. 2020. Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management* 50 (2020), 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

[15] Robert F DeVellis and Carolyn T Thorpe. 2021. *Scale development: Theory and applications*. SAGE Publishing, Thousand Oaks, CA, USA. https://uk.sagepub.com/en-gb/eur/scale-development/book269114

[16] Tamara Dinev, Heng Xu, Jeff H Smith, and Paul Hart. 2013. 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

[17] Leyla Dogruel, Sven Joeckel, and Nicholas D Bowman. 2015. Choosing the right app: An exploratory perspective on heuristic decision processes for smartphone app selection. *Mobile Media & Communication* 3, 1 (2015), 125–144. https://doi.org/10.1177/2050157914557509

[18] Sophia Xiaoxia Duan and Hepu Deng. 2022. Exploring privacy paradox in contact tracing apps adoption. *Internet Research* 32, 5 (2022), 1725–1750. https://doi.org/10.1108/INTR-03-2021-0160

[19] Jiaming Fang, Zhirong Zhao, Chao Wen, and Ruping Wang. 2017. Design and performance attributes driving mobile travel application engagement. *International Journal of Information Management* 37, 4 (2017), 269–283. https://doi.org/10.1016/j.ijinfomgt.2017.03.003

[20] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article

3, 14 pages. https://doi.org/10.1145/2335356.2335360
[21] Daniel Fleischhauer, Benjamin Engelstätter, and Omid Tafreschi. 2022. The Privacy Paradox in Smartphone Users. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 62–70. https://doi.org/10.1145/3568444.3568467
[22] Claes Fornell and David F Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research* 18, 1 (1981), 39–50. https://doi.org/10.1177/002224378101800104
[23] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150
[24] Dale L Goodhue. 1995. Understanding user evaluations of information systems. *Management science* 41, 12 (1995), 1827–1844. https://doi.org/10.1287/mnsc.41.12.1827
[25] Jie Gu, Yunjie Calvin Xu, Heng Xu, Cheng Zhang, and Hong Ling. 2017. 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
[26] Oliver Günther and Sarah Spiekermann. 2005. RFID and the perception of control: the consumer's view. *Commun. ACM* 48, 9 (2005), 73–76. https://doi.org/10.1145/1081992.1082023
[27] Mattia Gustarini, Katarzyna Wac, and Anind K Dey. 2016. Anonymous smartphone data collection: factors influencing the users' acceptance in mobile crowd sensing. *Personal and Ubiquitous Computing* 20 (2016), 65–82. https://doi.org/10.1007/s00779-015-0898-0
[28] Gabriella M Harari. 2020. A process-oriented approach to respecting privacy in the context of mobile phone tracking. *Current opinion in psychology* 31 (2020), 141–147. https://doi.org/10.1016/j.copsyc.2019.09.007
[29] Mark A Harris, Robert Brookshire, and Amita Goyal Chin. 2016. Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management* 36, 3 (2016), 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004
[30] Jun-Jie Hew, Voon-Hsien Lee, Keng-Boon Ooi, and June Wei. 2015. What catalyses mobile apps usage intention: an empirical analysis. *Industrial Management & Data Systems* 115, 7 (2015), 1269–1291. https://doi.org/10.1108/IMDS-01-2015-0028
[31] Se-Joon Hong and Kar Yan Tam. 2006. Understanding the adoption of multipurpose information appliances: The case of mobile data services. *Information systems research* 17, 2 (2006), 162–179. https://doi.org/10.1287/isre.1060.0088
[32] Jung-Kuei Hsieh and Hsiang-Tzu Li. 2022. Exploring the fit between mobile application service and application privacy. *Journal of Services Marketing* 36, 2 (2022), 264–282. https://doi.org/10.1108/JSM-01-2021-0023
[33] Chin-Lung Hsu and Judy Chuan-Chuan Lin. 2016. Effect of perceived value and social influences on mobile app stickiness and in-app purchase intention. *Technological forecasting and social change* 108 (2016), 42–53. https://doi.org/10.1016/j.techfore.2016.04.012
[34] Joshua B Hurwitz. 2012. User choice, privacy sensitivity, and acceptance of personal information collection. In *European data protection: Coming of age*. Springer, Berlin, Germany, 295–312. https://doi.org/10.1007/978-94-007-5170-5_13
[35] Yoonhyuk Jung. 2014. What a smartphone is to me: understanding user values in using smartphones. *Information Systems Journal* 24, 4 (2014), 299–321. https://doi.org/10.1111/isj.12031
[36] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, and Daniel Veit. 2017. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems* 34, 2 (2017), 369–400. https://doi.org/10.1080/07421222.2017.1334467
[37] Mark J Keith, Samuel C Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies* 71, 12 (2013), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016
[38] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *Financial Cryptography and Data Security: FC 2012 Workshops, USEC and WECSR 2012, Kralendijk, Bonaire, March 2, 2012, Revised Selected Papers 16*. Springer, Berlin, Germany, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6
[39] Byoungsoo Kim and Ingoo Han. 2009. What drives the adoption of mobile data services? An approach from a value perspective. *Journal of Information Technology* 24 (2009), 35–45. https://doi.org/10.1057/jit.2008.28
[40] Hee-Woong Kim, Hock Chuan Chan, and Sumeet Gupta. 2007. Value-based adoption of mobile internet: an empirical investigation. *Decision support systems* 43, 1 (2007), 111–126. https://doi.org/10.1016/j.dss.2005.05.009
[41] Frauke Kreuter, Georg-Christoph Haas, Florian Keusch, Sebastian Bähr, and Mark Trappmann. 2020. Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review* 38, 5 (2020), 533–549. https://doi.org/10.1177/0894439318816389
[42] Jacob Kröger. 2019. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In *Internet of Things. Information Processing in an Increasingly Connected World: First IFIP International Cross-Domain*

Conference, IFIPIoT 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-19, 2018, Revised Selected Papers 1. Springer, Berlin, Germany, 147–159. https://doi.org/10.1007/978-3-030-15651-0_13

[43] Ivan Ka Wai Lai and Guicheng Shi. 2015. The impact of privacy concerns on the intention for continued use of an integrated mobile instant messaging and social network platform. *International Journal of Mobile Communications* 13, 6 (2015), 641–669. https://doi.org/10.1504/IJMC.2015.072086

[44] John Laugesen and Khaled Hassanein. 2017. Adoption of Personal Health Records by Chronic Disease Patients. *Comput. Hum. Behav.* 66 (jan 2017), 256–272. https://doi.org/10.1016/j.chb.2016.09.054

[45] Hansoo Lee, Joonyoung Park, and Uichin Lee. 2022. A systematic survey on android api usage for data-driven analytics with smartphones. *Comput. Surveys* 55, 5 (2022), 1–38. https://doi.org/10.1145/3530814

[46] Inseong Lee, Boreum Choi, Jinwoo Kim, and Se-Joon Hong. 2007. Culture-technology fit: Effects of cultural characteristics on the post-adoption beliefs of mobile Internet users. *International Journal of Electronic Commerce* 11, 4 (2007), 11–51. https://doi.org/10.2753/JEC1086-4415110401

[47] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 501–510. https://doi.org/10.1145/2370216.2370290

[48] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[49] Anshul Malik, S Suresh, and Swati Sharma. 2017. Factors influencing consumers' attitude towards adoption and continuous use of mobile applications: a conceptual model. *Procedia computer science* 122 (2017), 106–113. https://doi.org/10.1016/j.procs.2017.11.348

[50] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won't You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 437 (oct 2021), 35 pages. https://doi.org/10.1145/3479581

[51] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. 2016. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5421–5432. https://doi.org/10.1145/2858036.2858063

[52] Miriam J Metzger. 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 12, 2 (2007), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

[53] Mohammad Naseri, Nataniel P Borges Jr, Andreas Zeller, and Romain Rouvoy. 2019. Accessileaks: Investigating privacy leaks exposed by the android accessibility service. In *Proceedings on Privacy Enhancing Technologies*. Sciendo, Boston, MA, USA, 291–305. https://inria.hal.science/hal-01929049/

[54] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Redwood City. https://doi.org/10.1515/9780804772891

[55] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. 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

[56] Iryna Pentina, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior* 65 (2016), 409–419. https://doi.org/10.1016/j.chb.2016.09.005

[57] Sandra Petronio. 2002. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, Albany, NY, USA.

[58] Robert Pinter. 2015. *Willingness of online access panel members to participate in smartphone application-based research*. Vol. 141. Ubiquity Press, London, Chapter Mobile Research Methods: Opportunities and Challenges of Mobile Research Methodologies. https://doi.org/10.5334/bar.i

[59] Emilee Rader. 2022. Normative and Non-Social Beliefs about Sensor Data: Implications for Collective Privacy Management. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Usenix Association, Berkeley, CA, USA, 653–670. https://www.usenix.org/conference/soups2022/presentation/rader

[60] Ulf-Dietrich Reips and Frederik Funke. 2008. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior research methods* 40, 3 (2008), 699–704. https://doi.org/10.3758/BRM.40.3.699

[61] Melanie Revilla, Mick P. Couper, and Carlos Ochoa. 2019. Willingness of online panelists to perform additional tasks. (2019), 223–252 pages. https://doi.org/10.12758/mda.2018.01

[62] Patrick Schober, Christa Boer, and Lothar A Schwarte. 2018. Correlation coefficients: appropriate use and interpretation. *Anesthesia & analgesia* 126, 5 (2018), 1763–1768. https://doi.org/10.1213/ANE.0000000000002864

[63] Eva-Maria Schomakers, Chantal Lidynia, and Martina Ziefle. 2019. A typology of online privacy personalities: Exploring and segmenting users' diverse privacy attitudes and behaviors. *Journal of Grid Computing* 17, 4 (2019), 727–747.

https://doi.org/10.1007/s10723-019-09500-3
[64] George Chung-Chi Shen. 2015. Users' adoption of mobile applications: Product type and message framing's moderating effect. *Journal of Business Research* 68, 11 (2015), 2317–2321. https://doi.org/10.1016/j.jbusres.2015.06.018
[65] John W Thibaut. 2017. *The social psychology of groups.* Routledge, Milton Park, UK.
[66] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research* 22, 2 (2011), 254–268. https://doi.org/10.1287/isre.1090.0260
[67] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly* 27, 3 (2003), 425–478. https://doi.org/10.2307/30036540
[68] Chenyan Xu, Daniel Peak, and Victor Prybutok. 2015. A customer value, satisfaction, and loyalty perspective of mobile application recommendations. *Decision Support Systems* 79 (2015), 171–183. https://doi.org/10.1016/j.dss.2015.08.008
[69] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information systems research* 23, 4 (2012), 1342–1363. https://doi.org/10.1287/isre.1120.0416
[70] Runhua Xu, Remo Manuel Frey, Elgar Fleisch, and Alexander Ilic. 2016. Understanding the impact of personality traits on mobile app adoption–Insights from a large-scale field study. *Computers in Human Behavior* 62 (2016), 244–256. https://doi.org/10.1016/j.chb.2016.04.011
[71] Shuiqing Yang, Yaobin Lu, Yuangao Chen, and Sumeet Gupta. 2015. Understanding Consumers' Mobile Channel Continuance: An Empirical Investigation of Two Fitness Mechanisms. *Behav. Inf. Technol.* 34, 12 (dec 2015), 1135–1146. https://doi.org/10.1080/0144929X.2014.988176
[72] Chong Zhang and Min Chu. 2018. A Research of Adoption Process of Mobile APP Based on Massive Log Data. In *Proceedings of the 2018 9th International Conference on E-Business, Management and Economics* (Waterloo, ON, Canada) *(ICEME '18)*. Association for Computing Machinery, New York, NY, USA, 60–64. https://doi.org/10.1145/3271972.3271975

A Appendix

A.1 Demographic Effects

Table 3. Results of Pearson's product-moment correlation (PCC) between the independent demographic variables age and education level and the ten factors of app adoption intention that we have assessed. We used Pearson's product-moment correlation for age and a non-parametric Kruskal-Wallis test for education.

	age		**education**	
	PCC	**p**	**H**	**p**
Privacy	0.110	.276	0.039	.527
Benefit Expectancy	0.079	.436	0.223	.289
Service Privacy Fit	0.031	.763	0.133	.296
Permission Sensitivity	−0.043	.672	−0.112	.742
Transparency (Collection)	−0.066	.512	0.102	.457
Publisher	0.034	.739	.106	.550
Rating	−0.196	.051	0.049	.972
Transparency (Usage)	−0.143	.155	0.114	.332
Transparency (Processing)	−0.060	.556	0.143	.160
Control	−0.035	.728	0.099	.315

Received February 2024; revised May 2024; accepted June 2024

Table 4. Results of Pearson's product-moment correlation between the independent demographic variable age and participants' perceived sensitivity and risk for read and write permissions with Pearson's correlation coefficient and p-value of the significance test (df=98 for all tests).

	read				**write**			
	sensitivity		**risk**		**sensitivity**		**risk**	
	PCC	**p**	**PCC**	**p**	**PCC**	**p**	**PCC**	**p**
Overall	0.138, p=.171				0.168, p=.094			
location	−0.014	.893	−0.027	.792				
phone state	0.067	.510	0.155	.124	0.039	.703	0.030	.770
notifications	−0.095	.347	0.005	.963	0.295	.003	0.231	.021
physical activity data	0.089	.380	0.180	.072				
body sensor + health data	0.255	.011	0.161	.111				
camera data	0.001	.990	0.060	.556				
microphone data	0.128	.203	0.038	.709				
screen contents	0.027	.790	0.054	.594				
account information	0.067	.509	0.181	.073				
files and media	−0.003	.974	0.180	.073	0.150	.135	0.027	.792
usage statistics	0.184	.068	0.130	.200				
calendars and reminders	0.084	.406	0.061	.547	0.065	.522	0.119	.240
contacts	0.201	.045	0.169	.093	0.136	.176	0.068	.502
data from smart home devices	0.152	.131	0.161	.110				
music library	−0.097	.337	−0.151	.133	−0.071	.480	−0.089	.377
motion data	0.110	.275	0.196	.050				
wallet information	−0.039	.697	0.130	.196				
interactions and touch behavior	0.029	.776	0.064	.592				
keyboard typing	0.156	.122	0.108	.283				
text messages	0.174	.084	0.084	.406	0.115	.256	0.176	.080
install apps and packages					0.116	.250	0.080	.427
internet access					0.273	.006	0.256	.010

Table 5. Results of Pearson's product-moment correlation between the independent demographic variable education and participants' perceived sensitivity and risk for read and write permissions with Pearson's correlation coefficient and p-value of the significance test of the Kruskal-Wallis test, (df=5 for all tests).

	read				**write**			
	sensitivity		**risk**		**sensitivity**		**risk**	
	PCC	**p**	**PCC**	**p**	**PCC**	**p**	**PCC**	**p**
Overall	0.057, p=.576				0.048, p=.635			
location	−0.054	.186	−0.027	.792				
phone state	−0.012	.067	0.155	.123	0.039	.703	0.051	.307
notifications	0.035	.731	0.005	.963	0.195	.096	0.249	.046
physical activity data	0.164	.163	0.180	.072				
body sensor + health data	0.048	.076	0.161	.111				
camera data	−0.142	.162	0.060	.556				
microphone data	−0.051	.098	0.378	.709				
screen contents	0.012	.802	0.054	.594				
account information	0.053	.577	0.180	.073				
files and media	−0.095	.187	0.181	.073	0.150	.135	−0.080	.035
usage statistics	0.060	.345	0.130	.199				
calendars and reminders	−0.015	.215	0.061	.547	0.065	.522	0.273	.186
contacts	0.102	.502	0.169	.093	0.137	.176	−0.057	.047
data from smart home devices	0.037	.109	0.161	.120				
music library	0.078	.155	−0.151	.133	−0.071	.480	0.044	.885
motion data	0.006	.525	0.196	.050				
wallet information	0.091	.492	0.130	.196				
interactions and touch behavior	0.105	.036	0.064	.529				
keyboard typing	−0.072	.075	0.108	.283				
text messages	0.001	.326	0.084	.406	0.115	.256	−0.023	.244
install apps and packages					0.116	.250	−0.70	.684
access the internet					0.273	.006	0.175	.176