Electronic Markets (2020) 30:607–625
https://doi.org/10.1007/s12525-019-00332-3

RESEARCH PAPER

The impact of transparency on mobile privacy decision making

Jan Hendrik Betzing[1] · Matthias Tietz[2] · Jan vom Brocke[2] · Jörg Becker[1]

Received: 24 May 2018 / Accepted: 8 January 2019 / Published online: 7 February 2019

Abstract

Smart devices provide unprecedented access to users' personal information, on which businesses capitalize to offer personalized services. Although users must grant permission before their personal information is shared, they often do so without knowing the consequences of their decision. Based on the EU General Data Protection Regulation, which mandates service providers to comprehensively inform users about the purpose and terms of personal data processing, this article examines how increased transparency regarding personal data processing practices in mobile permission requests impact users in making informed decisions. We conducted an online experiment with 307 participants to test the effect of transparency on users' decisions about and comprehension of the requested permission. The results indicate increased comprehension of data processing practices when privacy policies are transparently disclosed, whereas acceptance rates do not vary significantly. We condense our findings into principles that service providers can apply to design privacy-transparent mobile apps.

Keywords Mobile privacy decision making · Transparency · EU General Data Protection Regulation · Privacy notice · Consent · Experimental research

Introduction

Smart devices, which collect personal information such as users' location, calendar, and contacts, allow for new app-based business models that provide location-based (e.g., navigation, targeted advertising), social (e.g., friend finder, social networks), and personalized (e.g., mobile recommendations, mobile banking) services (Dhar and Varshney 2011; Tan et al. 2014). Such networked business models have substantial implications for data privacy because personal information is shared between and processed by a high number of actors (Wohlgemuth et al. 2014). Mobile operating systems feature safeguards against unauthorized access to personal information, and apps must request permission from users for these services prior to installation or at runtime (Aydin et al. 2017; Balebako et al. 2015). App providers can enrich runtime permission requests with custom explanations by adding a textual description to the mobile operating systems' inbuilt formal request dialogues (Tan et al. 2014). Alternatively, apps can present one or more dedicated screens that provide visual and textual explanations before triggering the actual request dialogue. However, so far app providers typically fail to comprehensively inform users about their data collection and sharing practices (Balebako et al. 2013). In turn, users often make decisions without realizing their consequences (Almuhimedi et al. 2015; Lin et al. 2012). In addition, users do not fully understand how data are processed and shared since data transmissions run in the background of apps (Wetherall et al. 2011). The case of Cambridge Analytica, which used a mobile app to collect private information from 50 million Facebook users

Responsible Editor: Mark de Reuver

✉ Jan Hendrik Betzing
jan.betzing@ercis.uni-muenster.de

Matthias Tietz
matthias.tietz@uni.li

Jan vom Brocke
jan.vom.brocke@uni.li

Jörg Becker
joerg.becker@ercis.uni-muenster.de

[1] European Research Center for Information Systems, University of Münster, Leonardo-Campus 3, 48149 Münster, Germany

[2] Institute of Information Systems, University of Liechtenstein, Fürst-Franz-Josef-Strasse, 9490 Vaduz, Liechtenstein

for voter-profiling, is one of many examples of privacy invasions that happen without users' knowledge (Rosenberg et al. 2018). Apart from illicit service providers that abuse data, even honest providers often fail to comprehensively explain their data practices. Users are given the opportunity to read privacy policies of service providers to make them aware of the personal data collection and sharing practices that are in place. However, studies confirm that privacy policies are ineffective due to their length and convoluted legal language (McDonald and Cranor 2008; Schaub et al. 2015; Tsai et al. 2011).

In response to ongoing transparency issues, policymakers and consumer advocates have increasingly emphasized the need to strengthen consumer rights regarding personal information (Gimpel et al. 2018). Based on the European Union (EU) General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which we consider as an exemplary legal framework, we investigate, how an increase in transparency on data processing compared to service providers' current communication practices affects users' privacy decision making in mobile contexts. The EU GDPR replaces the 1995 Data Protection Directive (95/46/EC) and harmonizes the privacy laws across the EU member states.

The regulation mandates, among other things, that service providers must comprehensively inform users about the purpose and terms of personal data processing before users' data are collected (European Union 2016). Users can then decide whether to opt-in giving *informed* and *active consent* (Carolan 2016). One could expect that increased transparency would lead users to make such consent decisions with careful consideration (Schaub et al. 2015). However, in light of reports in the media that many popular apps contain privacy threats such as disclosing location information to third parties (Aydin et al. 2017), users might react by not consenting to any data use at all. Without consent, business models that rely on personal data are at risk. Against this background, the central research question is:

> **RQ**: *How does increased transparency regarding personal data processing practices in mobile permission requests impact users in making informed decisions?*

The goal of our study is not to verify that users are concerned about privacy, but to determine whether increased transparency actually leads users to make *informed decisions*. We also investigate whether businesses that do transparently inform users have to fear that the number of users who consent to the collection of business-critical personal information will decline. We used a parallel-group experimental design with three conditions to test the effect of transparency on users' decisions about and comprehension of the requested permission. The results indicate that the participants' comprehension of data processing practices increases when increased transparency is established while acceptance rates do not significantly vary. We condense the findings of the study and interpretation of the regulation into design principles that aid app service providers in designing privacy-transparent apps that help their users to give informed consent. Following Gimpel et al. (2018) and Tsai et al. (2011), we maintain that increased transparency and protection of privacy can be an asset for service providers, rather than a liability.

The remainder of this paper is structured as follows: Section "Research background" provides more information on transparency regarding mobile privacy decision making and the EU GDPR. Section "Method" presents the research design. Section "Results" provides the results of our study. Section "Discussion" discusses the findings and derives design principles for app service providers, whereas Section "Conclusion" concludes the article.

Research background

Personal data are defined as "any information relating to an identified or identifiable natural person [...]; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person" (Art. 4, No. 1, European Union 2016). The terms "personal data" and "personal information" are used as synonyms in the literature and throughout this article. Data processing comprises any operation regarding personal data, including collection, analysis, storage, use, sharing, and deletion (Art. 4, No. 2, European Union 2016). Privacy is understood as "an individual's ability to control the terms by which their personal information is acquired and used" (Chellapa and Sin 2005, p.186).

Transparency of personal data processing practices

Personal data, most of which are collected in online-based environments, have become a corporate asset with growing monetary value (Wohlgemuth et al. 2014), and service providers extract value from personal data such as customer preferences, social networks, and geographic locations (Schwartz 2004). For example, Alphabet and Facebook have become multi-billion dollar companies, and are the leaders of the digital advertising market because they are profiling service users' data to allow businesses to more effectively target customers suited for their product portfolio (Kosinski et al. 2015).

Although service users can read privacy policies, most users do not comprehend service providers' personal

data processing practices (Schaub et al. 2015). Abundant research has shown that service users are unable to fully understand the convoluted legal language of privacy policies (McDonald and Cranor 2008; Schaub et al. 2015), and consequently, many people do not even bother reading them (Tsai et al. 2011). This leads to a lack of transparency that manifests in information asymmetry between user's and service provider's knowledge of processing practices (Acquisti et al. 2015; Jensen and Potts 2004).

In response to the economic significance of personal data and its potential impacts on service users, policymakers and consumer advocates around the world are requesting more transparency regarding service providers' data processing practices (Executive Office of the President 2015). They further concluded that regulations have to intensely focus on enabling individuals to actively make decisions about future usage and disclosures of any collected personal data (Podesta et al. 2014). In Europe, the recent EU GDPR is the central regulation that mandates service providers to more transparently inform users about personal data processing (European Union 2016) than they did so far (Robinson et al. 2009). Transparency aims to enable individuals to make more informed and privacy-conscious decisions regarding the disclosure of personal information (Tsai et al. 2011).

EU general data protection regulation

The EU GDPR, which came into effect on 25th May 2018, is meant to reduce information asymmetry by strengthening data protection for EU citizens (European Union 2016). It mandates that any processing of personal data must follow the principles of lawfulness, fairness, and transparency (Art. 5, No. 1a).

Lawfulness (Art. 6) requires an active consent, defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art. 4, No. 11).

This definition of consent requires that users have a choice, actively opt in ("freely given"), consent to data processing for a "specific" purpose, have received information regarding data processing ("informed"), and be presented the consent form in a clear, understandable way that distinguishes this consent from other contractual terms ("unambiguous") (Art. 7, No. 1 and 2).

For a user to be "informed", the service provider must reduce information asymmetry prior to collecting personal data from the data subject (Art. 13). Most importantly, users must be informed about the "identity and contact details of the [service provider]" (Art. 13, No. 1a), "the purpose of the processing" (Art. 13, No. 1c), and "the recipients [...] of the personal data" (Art. 13, No. 1e). Further, for processing to be fair and transparent, users must be informed of "the period for which the personal data will be stored" (Art. 13, No. 2a), the right to access the information (Art. 15; Art. 13, No. 2b), the rights to rectify and erase data (Art. 16; Art. 17; Art. 13, No. 2b), the right to withdraw consent at any time (Art. 13, No. 2c), and "the existence of automated decision making, including profiling" (Art. 13, No. 2f). Finally, all information should be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12, No. 1).

Users can make active consent decisions by accepting or declining permission requests, such as giving an app access to location services or contacts. For the decision to be informed, users must have previously received all of the information listed above. The EU GDPR is a legal norm, but does not provide explicit guidelines on how to establish transparency and display the necessary information. Developers can textually provide the mandated information within the permission request (Tan et al. 2014), so that the privacy decision is put into context and the users are given a choice. Additionally, users must be able to access a long-form privacy policy at any time.

We identified five dimensions affecting user's comprehension of the consequences of their actions: users should know what personal information will be used (collected data), when and how often it will be collected (time of collection), how the information will be processed (processing), with whom it will be shared (sharing), and how long it will be retained (erasure). Transparently providing the EU GDPR-mandated information in mobile permission requests should enable users to make informed consent decisions. We assess, whether this form of information provision increases the comprehension of these five dimensions and suggest our first hypothesis:

> **H1**: *More transparent provision of information regarding personal data processing practices in mobile permission requests increases users' comprehension of the consequences of the consent decision.*

With reduced information asymmetry and increased comprehension of data processing practices, users' perception of the risks associated with disclosing personal information might increase as well. Privacy calculus theory (Dinev et al. 2006) explains that users perform a risk-benefit analysis in which the willingness to provide personal information is positively related to the perceived value of information disclosure and negatively related to the perceived risks thereof (Xu et al. 2011). However, research showed that this rational view of maximizing benefits while at the same time minimizing risks, corresponding to expectancy theory

(Dinev et al. 2006), not always holds for real-world user behavior (Keith et al. 2013). The "privacy paradox" (Acquisti and Grossklags 2005; Adjerid et al. 2018) subsumes discrepancies between users' conservative behavioral intentions and their more liberal real-world behavior. In effect, some users ignore long-term privacy costs in favor of short-term functional and monetary benefits (Gimpel et al. 2018).

Consequently, we assume that with increased comprehension of personal data processing practices, many users will react with skepticism, raise privacy concerns, and deny permission requests (Keith et al. 2016). Although the privacy paradox might mitigate the effect as some users supposedly trade risks for short-term benefits, we expect to see an overall decrease in the number of users consenting. Therefore, the second hypothesis for this study reads as follows:

H2: *More transparent provision of information regarding personal data processing practices in mobile permission requests decreases the number of users who consent to the use of their data.*

Mobile privacy decision making

Previous research on mobile privacy decision making has highlighted issues regarding the provision of privacy-related information. In general, mobile users value control over their personal information (Pentina et al. 2016), but they are often unaware of the data collection and sharing practices of apps they use (Almuhimedi et al. 2015; Shklovski et al. 2014). When informed about their actual practices, many users are upset and respond by uninstalling the apps (Balebako et al. 2013; Harbach et al. 2014; Shklovski et al. 2014).

Although mobile permission-based access systems should protect users from unwittingly disclosing private information, privacy notices and permission requests provide insufficient explanations of the types of data collected, frequency of collection, entities with which data are shared, and reasons for doing so (Balebako et al. 2013; Lin et al. 2012). Studies have also confirmed that users have difficulty understanding the default mobile permissions (Felt et al. 2012; Kelley et al. 2012) and that their beliefs about apps' behaviors often do not align with their actual behavior (Lin et al. 2012). Some works have proposed highlighting threats to privacy using mobile security extensions like application and network analysis (Aydin et al. 2017), privacy nudges (Acquisti 2009; Balebako et al. 2013), and just-in-time disclosures of data sharing (Almuhimedi et al. 2015).

Others have sought to improve the design and timing of privacy notices. Harbach et al. (2014) augmented permission requests with examples of users' personal data to demonstrate the consequences of consent. Kelley et al. (2013) designed a privacy fact sheet. Schaub et al. (2015) presented a framework for designing privacy notices, taking into account the timing, channel, modality, and control of notices.

Balebako et al. (2015) compared the impact of timing on users' ability to recall privacy policies as a proxy for an informed consent. Their results indicated that permission requests shown at run time are more salient than is displaying permissions at the time of installation.

Previous research on human-computer interactions further reminds us of the ineffectiveness of warnings, prompts, and permission requests due to users' habits (Böhme and Grossklags 2011; Harbach et al. 2014; Tan et al. 2014). Some users get used to such requests and respond automatically, without making an informed decision. For example, Fisher et al. (2012) showed that 15% of respondents granted all location permission requests on Apple iOS. It is fair to assume that habituation effects will also affect permission requests that transparently explain data processing practices.

Following proven practices from mobile app design (Marrs 2016), privacy information can be presented through onboarding, which is "the process of familiarizing a customer with a firm's service offering" (Voorhees et al. 2017, p. 274). Mobile app designers frequently include short introductory tutorials that explain the app's key benefits. Commonly, this process will comprise a few swipe-through screens that combine images or videos with explanatory text. Studies show that a multi-modal presentation of instructional materials can improve the effects of learning, in line with cognitive load theory (Sombatteera and Kalyuga 2012). The GDPR's transparency principle also proposes using visualization where appropriate (Recital 58). In addition, mobile operating systems' permission request interfaces have word count limits, so developers can only briefly state the mandatory information (Keith et al. 2016), whereas an onboarding process can utilize the full screen of the mobile device. Therefore, we propose an onboarding process as an alternative design, where visual cues accompany a textual representation of the EU GDPR-mandated privacy information. After the user has received the information, he or she is asked to provide consent using the operating system's permission request dialogue. In addition to potentially counteracting habituation, onboarding has higher expressive power than solely text-based permission requests. The onboarding process might reduce the cognitive load required to understand the risks associated with disclosing personal information compared to the text-based request. Thus, the established transparency might negatively affect users' consent decisions in comparison to current nontransparent practices. With regard to an onboarding process, we propose a second set of hypotheses:

H3: *More transparent provision of information regarding personal data processing practices in an onboarding process increases users' comprehension of the consequences of a consent decision.*

H4: *More transparent provision of information regarding personal data processing practices in an onboarding process decreases the number of users who consent to the use of their data.*

Method

Design Similar to other studies on mobile privacy notices (Balebako et al. 2015; Harbach et al. 2014; Kelley et al. 2013; Tan et al. 2014), we conducted a web-based experiment and presented participants with app screens framed with a phone border to resemble a virtual smartphone. The experimental design caters to ecological validity as it features both the look and the feel of a real-world mobile app, and a realistic real-world use case. We designed the privacy note and app permission request in accordance with previous research. Following Schaub et al. (2015), the permission request should appear in direct context to the processing practices and block the current application's operations when it wants to access a restricted resource for the first time (Schaub et al. 2015). Our app resembles the flow and user interface (UI) of Apple iOS (version 10, which was current during the experiment) because this operating system uses just-in-time permissions for many years (Tan et al. 2014), while Google Android only recently adopted this behavior (Aydin et al. 2017).

Material and procedure The use case of our fictitious app—called shop.io—is a mobile shopping platform for high streets (Bartelheimer et al. 2018). Retailers register as partner shops, present their businesses, and engage in targeted location-based marketing, which is facilitated by Bluetooth beacons that retailers install in their shops. These small tokens broadcast a uniquely identifiable signal to which smart devices can react (Betzing 2018). A customer-facing mobile app, which is the subject of our study, allows the user to find local shops and obtain personalized offers. When the customer enters a partner shop, shop.io receives the shop beacon's signal and tracks the customer's visit. The system profiles the customer's shopping preferences based on tracked shop visits and uses collaborative filtering to recommend relevant shops and offers that match the user's interests (Bartelheimer et al. 2018). Location-based business models like shop.io depend on customers' decisions to allow the app to access location services, and to consent to the processing of location information; the use of beacons requires that the app continuously accesses location services in the background to identify beacon signals, even when the user is not actively interacting with the app (Betzing 2018). These concerns, in combination with users' desire for location privacy (Eastin et al. 2016; Keith et al. 2013; Kelley et al. 2013), lead us to test for the "location always" permission instead of other permission requests, such as access to calendars or contacts.

Participants were introduced to the experiment with a detailed description of the setting in which they were hypothetically located. They received a fictive promotional leaflet for shop.io (see Fig. 1) that lists the key benefits of the app and closely resembles real-world app advertisements. Tech-savvy users could infer the app's functionality and behavior from this leaflet. Some statements were directly related to questions regarding comprehension asked in the experiment. Participants then saw the virtual phone's home screen with the app icon and imagined that they were opening shop.io for the first time.

Our experiment was a hypothetical thought experiment, so participants were asked to select the answer they would choose in real life. After deciding, participants answered ten comprehension questions related to the five dimensions (i.e., collected data, time of collection, data processing, data sharing, and data erasure). The questions are shown in Appendix A.1. Then, participants provided personal and demographic information and were presented with a simple debriefing that explained the purpose of the study.

Conditions To test the hypotheses, we used a parallel group experimental design with three conditions: a baseline

Fig. 1 Leaflet that promotes the fictional shop.io app

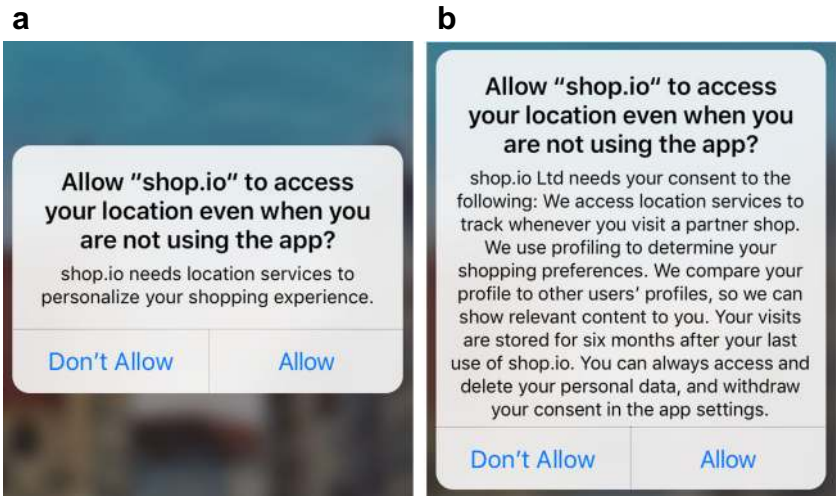
condition and two treatment conditions. The baseline condition resembles current app practices; developer-specified explanations for permission requests are vague and do not provide details about the app's data processing practices (Tan et al. 2014). Figure 2a shows a request for the "location always" permission. The headline and buttons are predefined by iOS, and developers can only define the body of the permission request.

To test for hypotheses *H1* and *H2*, the first treatment condition (henceforth, *EU notice*) uses the same UI but replaces the marketing-driven text with a short-form privacy notice (see Fig. 2b). This treatment features increased transparency and is compliant with the EU GDPR. The text, which we developed in consultation with a legal expert, closely resembles the wording of the regulation and fulfills, to the best of our knowledge, the prerequisites for an informed consent decision (cf. Section 2): the identity of the service provider (shop.io Ltd) and a request for consent; the purpose of collection (to determine shopping preferences and show relevant content); which personal information is collected (visits to partner shops) and when it is collected (every time a shop is visited); a statement that shop.io profiles and compares various users' personal data to other users' data; how long the information is stored; and the users' rights regarding access to and deletion of personal information and the option to withdraw consent at any time.

To test for hypotheses *H3* and *H4*, the second treatment condition uses an onboarding process (henceforth, *onboarding*) which presents the same EU GDPR-mandated information as the EU notice but in a multi-modal fashion. We consulted existing practitioner guidelines regarding mobile privacy notices published by the US National Telecommunications and Information Administration and the OECD. The former suggests a standardized structure for short-form notices (NTIA 2013), but the proposed data categories have been identified as difficult to understand (Balebako et al. 2015). The OECD recommends a process of preparing a long-form privacy policy, developing a simplified notice, testing its usability, and deploying the notice (OECD 2006). However, as Schaub et al. (2015) remarked, the OECD (2006) fails to address what the policy should look like. Therefore, our onboarding process is inspired by real-world examples (Marrs 2016). Figure 3 shows the four onboarding screens and the subsequent permission request. Each screen is consistently structured and focuses on one aspect of data processing. The screens feature a headline, visualization, mandatory information regarding the data processing, and statements that limit the extent of processing. For example, the first screen states that visits to partner shops are tracked but that no other location information is collected. In this treatment, most EU GDPR-mandated information is provided before the permission request is shown. In effect, the explanation only states that it is a consent form, the name of the service provider, and the purpose of data collection.

Participants were randomly assigned to one of the three conditions. The baseline and the EU notice conditions instantly showed the respective location permission requests, whereas participants in the onboarding condition had to go through the onboarding screens before seeing the location permission request.

Measures The decision variable was binary; participants were asked to either accept or deny the permission request. The comprehension score variable was composed of five comprehension dimensions, each of which had two true/false questions. As suggested by Dolnicar and Grün (2014), participants could choose to respond don't know to prevent contaminating the data with guesses. The comprehension score was continuously coded between −10 points and +10 points (+1 per correct and −1 per incorrect answer).



Baseline condition *EU Notice condition*

Fig. 2 Location permission requests

Fig. 3 Five-step onboarding process

Following the location permission request, participants' privacy preferences were tested and typed according to the Westin privacy index, which categorizes individuals as either a privacy pragmatist, a privacy fundamentalist, or a privacy unconcerned individual (Taylor 2003). We replicated Westin's approach by asking the same three standardized questions (Kumaraguru and Cranor 2005, p.13,15) on a four-point Likert scale and also use the same classification key (p.13). We also controlled for habituation (Böhme and Grossklags 2011; Fisher et al. 2012; Harbach et al. 2014). To identify users with privacy habits, we both determined the .25 quantile of the decision time as a reference time for quick decision makers and asked two questions using five-point Likert scales (see Appendix A.2).

Participants The minimum feasible sample size—252 participants, 84 per condition—was estimated using G*power analysis (Faul et al. 2007). This number of participants enables us to make a fairly accurate and reliable statistical judgment (power = 0.95) based on a medium effect size as well

Table 1 Descriptive statistics of the sample

	N	Gender		Age	
		Female	Male	Mean	SD
Baseline	105	71	34	35.59	11.61
EU Notice	104	68	36	32.51	10.13
Onboarding	98	69	29	32.89	11.26
Σ	307	208 (67.75%)	99 (32.25%)	$\bar{x} = 32$	$\sigma_x = 11.06$

as to detect any effect between the three study groups that may result from providing them with different degrees of transparency regarding personal data processing (Cohen 1988).

We recruited 382 EU residents who were at least eighteen years of age via the online recruitment platform *prolific.ac* on the 21st and 22nd of March 2018. This platform is appropriate for random-sample populations (Berinsky et al. 2012), and the behavior of the respondents on online recruiting platforms closely resembles that of participants in traditional laboratory experiments (Mason and Suri 2012). Further, prolific.ac allowed us to lock participants to use desktop PCs only to keep this situational variable constant. We pre-tested the study with 45 additional participants from prolific, discussed the experiment in depth with fellow researchers to ensure its clarity and comprehensiveness, and set up a questionnaire to accurately measure the comprehension level.

Unfamiliarity effects were prevented a priori by preselecting participants that primarily use an Apple iOS device. We also surveyed for smartphone experience and found that 87.3% of the respondents had more than four years of experience. To ensure high data quality, respondents who either failed an attention check question (from Oppenheimer et al. 2009) or failed a simple comprehension check question were removed. This process left us with a sample of 307 participants. The mean age of the participants was 33.69 years (median 32 years, SD 11.06 years), and 67.75% were women (see Table 1). Each session lasted an average of 6 min, and respondents were paid £1 for participation. Participants were evenly distributed among conditions. Slight variations are the result of filtering. In total, 105 participants were assigned to the baseline condition, 104 were assigned to the EU notice condition, and 98 were assigned to the onboarding condition.

Results

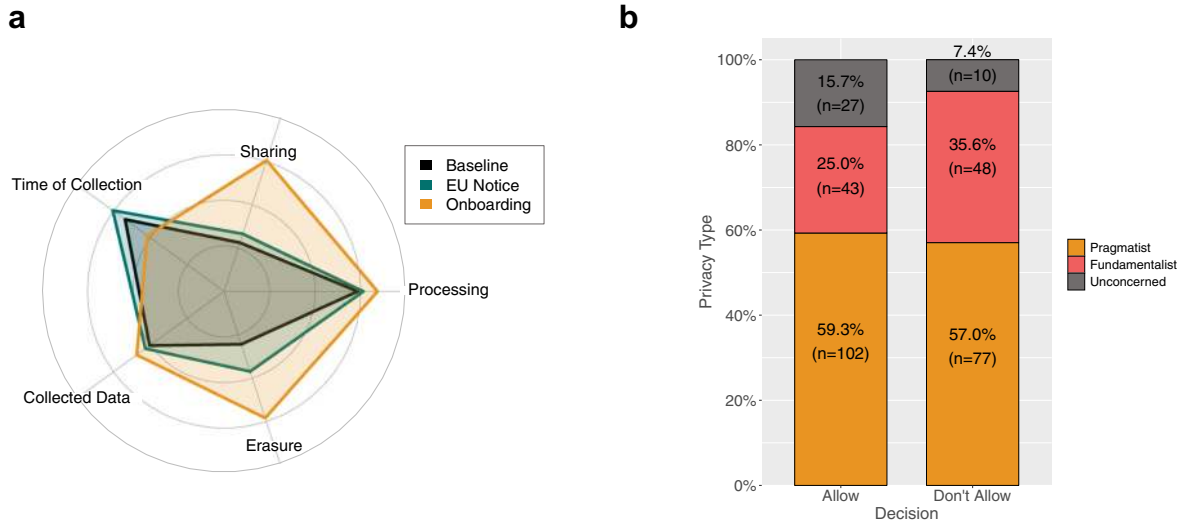
Descriptive results

In support of hypotheses *H1* and *H3*, which propose that users' comprehension increases when privacy-related information is presented more transparently, participants in the treatment conditions achieved higher comprehension scores than did those in the baseline (Table 2). Thus, it is reasonable to claim that they made more informed consent decisions (Fig. 4a). Appendix A.4 gives the distribution of comprehension performance across conditions.

The comprehension scores of participants in the baseline condition were the lowest of almost all dimensions, followed by participants in the EU notice condition (see Appendix A.4, Table 5). The scores of those in the onboarding condition were much higher than the scores of those in the other two conditions in almost all dimensions. With a maximum of 10 points and a minimum of −10 points, the baseline group achieved an average of −.02 points (EU notice 1.38 points; onboarding 3.76 points) over all dimension areas with homogeneous distribution as the standard deviation is almost identical across conditions (SD baseline 2.68; SD EU notice 3.54; SD onboarding 3.07). Furthermore, we descriptively analyzed how much time participants needed to make their decisions across conditions (see Appendix A.3).

Table 2 Descriptive statistics of the results

	N	Comprehension		Decision		Privacy type			Habituation
		Mean	SD	Don't Allow	Allow	Unconcerned	Pragmatist	Fundament	
Baseline	105	−.02	2.68	45 (42.9%)	60 (57.1%)	10 (9.5%)	61 (58.1%)	34 (32.4%)	6 (5.7%)
EU Notice	104	1.38	3.54	44 (42.3%)	60 (57.7%)	16 (15.4%)	60 (57.7%)	28 (26.9%)	9 (8.7%)
Onboarding	98	3.76	3.07	46 (46.9%)	52 (53.1%)	11 (11.2%)	58 (59.5%)	29 (29.6%)	9 (9.2%)
Σ	307	$\bar{x} = 1.66$	$\sigma_x = 3.47$	135 (44%)	172 (56%)	37 (12%)	179 (58.3%)	91 (29.6%)	24 (7.8%)



Distribution of different dimensions of comprehension by treatment groups

Distribution of permission request decisions by privacy types

Fig. 4 Dimensional segmentation of comprehension results and distribution of privacy types

The distribution of the permission request decision is similar for all conditions. In the baseline condition, 57.1% of the participants allowed access to location services (EU notice 57.7%; onboarding 53.1%), which might indicate that increased transparency does not affect respondents' decisions.

Table 2 also provides descriptive statistics concerning the the shares of habituated users, as well as distribution of the three types of privacy preferences. In total, 7.8% of the participants made privacy-related decisions out of habit, as did 5.7% of those in the baseline condition, 8.7% of those in the EU notice condition, and 9.2% of those in the onboarding condition. Although we expected the onboarding process to counteract habituation, there is no evidence that it does. With regard to the three types of privacy preference, more than half of the participants were privacy pragmatists and around a third were privacy fundamentalists, with fewer reporting to be unconcerned about privacy. The resulting distribution of privacy types (Table 2) can be interpreted as a reliable replication of Westin's 2003 study (presented in Taylor 2003), in which 26% of adults were classified as privacy fundamentalists, about 10% were unconcerned, and 64% were pragmatists. In our study, a large majority (73%) of unconcerned participants allowed access to their data for location services, while the other two groups' decisions were more balanced (Fig. 4b).

Inferential results

Table 3 presents the regression results. We conducted a linear regression to test the effect of increased transparency, in the form of an EU GDPR-compliant notice and the additional onboarding process, on participants' comprehension as well as a logistic regression to test the effect of the treatments on users' decisions. The strong positive relationship indicated by Fig. 4a was confirmed with the following linear regression model:

$$\begin{aligned}\text{Comprehension Score}_i \;=\; & \beta_0 + \beta_1 \times \text{EU Notice}_i + \beta_2 \\ & \times \text{Onboarding}_i + \beta_3 \times \text{Pragmatist}_i \\ & + \beta_4 \times \text{Unconcerned}_i \;+ \beta_5 \\ & \times \text{Fundamentalist}_i + \gamma' \times \text{Controls}_i + \varepsilon \quad (1)\end{aligned}$$

where i indexes the individuals, β_0 is the intercept, β_1 and β_2 are the effects of the respective treatment (i.e., EU notice and onboarding), β_3, β_4, and β_5 are the coefficients for the privacy type which are dummy variables, γ' is the coefficient for the controls$_i$, which were *Habit*, *Age*, and *Gender*, and ε represents the error term.

We used the baseline condition as the reference condition. Model [1] (Table 3) contains only the treatment variable (condition), while Model [2] also includes the covariates indicating the privacy preferences of each individual and the control variables. In Model [1], the comprehension scores of participants in the EU notice condition increased significantly to 1.40 ($p < .01$). This effect was amplified when the control variables were added (Model [2]: 1.47, $p < .01$). The effect was even greater for the onboarding condition (Model [1]: 3.77, $p < .001$; Model [2]: 3.8, $p < .001$). Therefore, the study provides evidence that the users' comprehension of the consequences of the consent decision

Table 3 Regression results (odds ratios for model [3] and [4])

Model #	[1]	[2]	[3]	[4]
Dependent variable	Comprehension Score (continuous)		Decision (binary)	
EU Notice	1.40** (.43)	1.47** (.43)	1.02 (.28)	.93 (.29)
Onboarding	3.77***(.44)	3.80*** (.44)	.85 (.28)	.79 (.29)
Pragmatist	–	.42 (.40)	–	1.17 (.26)
Unconcerned	–	.59 (.61)	–	3.16** (.43)
Fundamentalist	–	–.45 (.39)	–	.31 (.26)
Habit	–	–.09 (.63)	–	2.15 (.48)
Age	–	.03 (.02)	–	.99 (.01)
Gender	–	–.55 (.38)	–	.98 (.25)
Intercept	–.02 (.30)	–.75 (.72)	1.08 (.48)	1.61 (.45)
N	307	307	307	307
AIC			426.60	429.76
BIC			437.78	452.13
Adj. R2	.19	.20		
F-statistic	37.81***(df = 2; 304)	11.99***(df = 7; 299)		

* p < .05, ** p < .01, ***p < .001; standard errors are in parentheses

increases when there is increased transparency regarding data processing.

To test hypotheses *H2* and *H4*, we used the following logistic regression model that contains the same index, intercepts, and coefficients as the linear model, excluding the linear-specific error term:

$$\begin{aligned} Pr(\text{Choice}_i = 1) = \; & logit^{-1}(\beta_0 + \beta_1 \times \text{EU Notice}_i + \beta_2 \\ & \times \text{Onboarding}_i + \beta_3 \times \text{Pragmatist}_i \\ & + \beta_4 \times \text{Unconcerned}_i + \beta_5 \\ & \times \text{Fundamentalist}_i + \gamma' \times \text{Controls}_i) \end{aligned} \quad (2)$$

In line with Model [1] and Model [2], Model [3] features only the treatment variable, while Model [4] also incorporates the covariates for the privacy type and the control variables (Table 3). The results indicate that participants' consent decisions were not significantly negatively affected by a more transparent provision of information regarding data processing (EU notice: Model [3]: 1.02, p = .94, Model [4]: .93, p = .94; onboarding: Model [3]: .85, p = .56, Model [4]: .79, p = .43), so we reject hypotheses *H2* and *H4*. Therefore, increased transparency does not decrease the number of users who consent to data processing.

When we control for privacy preferences, the coefficients of the treatment conditions remain largely unchanged, indicating that the effect is robust, except the EU notice condition significantly caused privacy-unconcerned participants to consent to data processing (EU notice: 10, p = .056). Participants who were unconcerned about privacy were 2.41 times more likely than those with other privacy preferences to accept the permission request (p = .03). The results for the comprehension score largely reflect the findings from the main analysis, except for unconcerned participants in both conditions, who show an insignificant improvement in comprehension (EU notice: .99, p = .45; onboarding: 1.89, p = .20).

Qualitative results

All participants were asked to provide a rationale for their decisions by means of an open-ended question immediately after decision making. The responses were split into two data sets: 172 cases of acceptance and 135 cases of denial of the permission request. We conducted a qualitative content analysis that followed the content structuring approach presented by Mayring (2014). Two researchers independently analyzed the data set to exploratively create a category-based coding scheme that allows responses to be assigned to at least one non-mutually exclusive category. The coding scheme was iteratively revised until a consensus among both researchers was reached and every response could be assigned.

Table 6 in Appendix A.5 provides inter-rater agreements regarding both subsets and individual categories using percent agreement and Cohen's Kappa. The results indicate a very high agreement for both the acceptance (95.60% agreement; overall Cohen's Kappa .840) and rejection (96.48% agreement; overall Cohen's Kappa .853) subsets (Landis and Koch 1977). In instances of disagreement, the

researchers discussed the respective codes until a complete consensus was established.

Seven categories were derived from the responses related to acceptance of the permission request. Table 7 in Appendix A.5 provides the categories, their descriptions, and number of mentions. Evidence from the responses was added for clarity. All quotes are taken verbatim without correcting punctuation or spelling. Most respondents reported receiving personal benefits (111, 64.53%) or allowing the app to properly execute its service (89, 51.74%) as rationales for consenting to the request. In total, 56 respondents (32.56%) reported both personal benefits and functional reasons. Ten respondents (5.81%) acknowledged habituation and eight respondents (4.65%) stated that they did not care about the consequences of their decision. Although, shop.io is a fictional app, ten respondents (5.81%) explicitly stated that they trusted the app. Eight of the respondents within this category received the onboarding treatment. Lastly, five participants (2.95%) reported feelings of control as they explicitly or implicitly knew that they could revoke the location permission and their consent later on.

Table 8 in Appendix A.5 lists eight categories of rationales for why participants denied the location permission request. Most frequently, respondents disliked the feeling of intrusiveness evoked by tracking (45, 33.34%), giving the app permanent access to location data (43, 31.85%), or providing personal information in general (42, 31.11%). Across groups, about a third of participants reported that they would grant shop.io access to location data if the information is only collected when the app is opened (i.e., when the user is actively interacting with the app). Twenty-one (15.56%) participants had bad experiences in the past, recalling battery drain and high use of mobile data due to background location services. Some users (19, 14.07%) decided out of habit and stated that they completely disabled location features or denied all requests. Seventeen respondents (12.60%) did not understand why shop.io required location services and denied the request. Further, ten participants (7.41%) feared a data breach, intrusion by hackers or unauthorized sharing of personal information. Lastly, seven participants (5.19%) denied the request because they were not interested in the app and the functions enabled by location services.

Discussion

Interpretation of results

Transparency regarding personal data processing practices in mobile permission requests does influence users in making more informed decisions (H1, H3). Both an EU GDPR-compliant notice and an onboarding process are suitable designs that app providers can apply when developing privacy-transparent mobile apps. Since an EU GDPR-compliant notice suffices to give users all of the information required by law, an onboarding process that exclusively informs on data privacy might—at first—appear over-engineered. However, onboarding had the superior comprehension rates to both the baseline and the EU notice designs. From an ethical perspective, service providers should aim at maximizing comprehension. Although legally sufficient, over time the EU notice design (with its brief textual explanation) might come with social penalties if superior practices of disclosure such as onboarding will establish themselves on the market. We maintain that onboarding should be preferred generally to maximize comprehension, and particularly in cases of complicated services that require explanation. Nevertheless, in our case, the onboarding process also had a negative effect on some respondents. Among the seventeen users that did not understand the necessity of granting the permission request (Table 8), nine received the onboarding treatment, which explains in detail that location is sensed through Bluetooth beacons and not via GPS. Although technically correct, this statement caused confusion since users associate the location permission request primarily with GPS. However, Apple iOS uses the same permission and dialogue for both Bluetooth beacons and GPS. This limitation is specific to our case but reminds us that providing more information can sometimes increase the risk of misunderstandings.

We expected that more transparently informing users about data processing practices would reduce acceptance rates (H2, H4). However, users showed no significant differences in their consent decision in either of the two treatment conditions. One the one hand, this might suggest that users are prejudiced, react regardless of the treatment, and are not impacted by increased transparency. On the other hand, a lack of behavioural change at the aggregated level can mask changes at the individual level. Some users who would have previously declined might have become convinced by the given information, while other users might have become alienated.

The qualitative analysis of users' rationales for deciding on the permission request reveals that most participants follow the traditional privacy calculus and weigh permanent tracking against personalized services and monetary benefit (Xu et al. 2011). Regardless of their decision, the established transparency might reduce the users' cognitive load related to their privacy calculus. In contrast to related studies by Shklovski et al. (2014), no participant expressed helplessness or reported lack of transparency as a reason for denying the permission request.

We also find evidence for the privacy paradox (Acquisti and Grossklags 2005; Adjerid et al. 2018). In total, 43

participants were classified as privacy fundamentalists (16 baseline, 16 EU notice, 11 onboarding), but provided their location information to receive personal benefits. Further, with regard to the effect of transparency and perceived control on user behavior, related work names the "Peltzman effect," in which users offset their increased feelings of control and trust by engaging in riskier disclosures (Brandimarte et al. 2013). The EU notice and onboarding treatments do explicitly present the users' rights to access and delete collected data, which can increase users' perceived control relative to the baseline condition. However, given that no statistically significant differences in users' decisions were evident in our study, we cannot confirm the existence of the Peltzman effect.

While this study focuses on the influence of increased transparency on making informed privacy decisions, it also stimulates the need for further research. Trust is a known influence on the willingness to provide personal information (Dinev et al. 2006). Given its expressive nature, an onboarding process could be used by service providers to market their reliability and seriousness regarding the protection of personal information. The qualitative analysis provides preliminary evidence that particularly the onboarding design can evoke feelings of trust (cf. Appendix A.5, Table 7). For example, one participant stated to agree "*because the app explains privacy so well that I'd enable location permission*." However, further studies are required to explore whether transparent information provision facilitates cognitive and affective trust (Johnson and Grayson 2005), if there is an interplay between trust and the different privacy types (Kumaraguru and Cranor 2005), and how trust mediates the consent decision in such a scenario.

In our case, less than two-thirds of participants consented to data processing (Table 2). In the real world, this would cause businesses models like shop.io, which rely on tracking personal information, to lose potential customers. The most frequently mentioned reasons for declining the permission request were related to privacy concerns and location tracking (cf. Appendix A.5, Table 8). In particular, 33 participants disliked that the app had constant access to location services, preferring to control tracking themselves. One participant stated: "*I don't mind if I am using the app, but its a bit creepy to constantly track my location*." In response, service providers should consider hybrid approaches to personal data collection, where a secondary means of collection eclipses a primary one. Collecting less personal information might lead to a reduced range of functions, but it would be more likely to retain privacy-conscious users. Instead of automatically tracking users, shop.io could track shop visits through "check-ins" or users could manually select their favorite shops, which would still enable the provider to personalize the service to some extent. Nevertheless, requesting access to a reduced set of personal information after the user denied the primary means of data collection might appear as bold or even "greedy" to some users and might have a negatively impact trust. In total, 7.8% of respondents were classified as habituated based on the quantitative analysis, while the qualitative analysis revealed that 11.4% of respondents acted out of habit. About 6% of respondents stated that they accept all requests or do not care about the consequences of their decisions (cf. Table 7). Another 6% of respondents stated to deny all location permission requests (cf. Table 8). In effect, even when transparently providing information to users, there will be a fraction of potential users who service providers cannot influence either way.

Implications for App service providers

Although the EU GDPR only protects the data of EU citizens, it is the most far-reaching regulation concerning transparency and data privacy to date (Carolan 2016), and thus, should be kept in mind by any privacy-conscious service provider. In its first months of being effective, the regulation most prominently impacted users by omnipresent notifications for updated privacy policies and requests for consent (Hern and Waterson 2018). Researchers also measured a reduction of third-parties that service providers share their service users' personal data with. For example, the number of third-party cookies (e.g., by ad networks) on European news websites declined by 22% (Libert et al. 2018). On the contrary, some service providers lock out EU customers or have shut down their service entirely instead of making their offerings compliant (Hern and Waterson 2018). While making existing business models and services compliant with the EU GDPR is a challenge, it is possible to design new services for transparency. The literature suggests the related concept of *privacy by design*, which describes practices to embed privacy into information systems design and development (Schaar 2010), such as requiring only a minimum amount of personal information for service delivery and utilizing appropriate technical means to protect data (Gimpel et al. 2018).

To identify the primary requirements for service providers concerning the design of privacy notices in particular and mobile privacy management in general, we consulted the EU GDPR. Against the backdrop of the study results and our interpretation of the regulation, we derived six design principles for privacy-transparent mobile apps (Table 4), which app service providers can apply in conjunction with the privacy by design approach (Schaar 2010).

Service providers must design for privacy by default (DP 1) so that no personal information is collected and processed before informed consent is given (Art. 25

Table 4 Design principles for privacy-transparent mobile apps

#	Name	Description
1	Privacy by Default	Design the app so it collects no personal information before obtaining consent from the user.
2	Short-form Notice	Provide users with short-form EU GDPR-mandated information in the form of a notice or an onboarding process to enable them to give an informed consent.
3	OS Dialogues	Make use of mobile operation systems' permission request dialogues to ask informed users for consent to a particular purpose.
4	Privacy Self-service	Provide the system with a privacy menu that allows users to inspect the personal information that is collected about them (right to access), correct inaccurate data (right to rectification), export collected data (right to data portability), delete their personal data (right to be forgotten), and withdraw given consent (right to object).
5	Long-form Policy	Provide users with a long-form privacy policy that follows the principles of lawfulness, fairness, and transparency.
6	Plan B	Design the app to ask for consent to less privacy-intrusive means of data collection if consent to the primary means is denied.

EU GDPR). As this study showed, transparency can be established by a short-form notice (DP 2) that includes all EU GDPR-mandated information (Art. 13). Regardless of whether app designers use a textual description or an onboarding process, the mobile operating system's permission dialogues should be used as a mechanism to request consent (DP 3). With a single input, the user gives both legal consent to data processing and technical access to the underlying data sources.

Given the goals of transparency and legal compliance, service providers must provide users with extensive control over their personal data. We suggest self-service privacy management (DP 4) within mobile apps that implements the rights users have through the EU GDPR. This system should disclose all information that the service provider has collected on the user (Art. 15), such as prior shop visits in the case of shop.io. The system should also allow users to request rectification of inaccurate data (Art. 16), decide which data to keep and which to delete (Art. 17), and export collected data (Art. 20). In addition, the legal expert we consulted stressed that withdrawing a consent must not be more complicated than giving the consent (Art. 7, No. 3). Consequently, app service providers must implement means for users to withdraw consent within the app (Art. 21). Further, as a part of privacy self-service, users must be able to inform themselves about all data processing practices in detail. Therefore, the short-form notice must be accompanied by a long-form privacy policy (DP 5) that is lawful, fair, and transparent (Art. 5). Lastly, as shown before, the study revealed that a binary choice is too restricting; some users might be comfortable with sharing only a subset of personal information or with deciding case by case. Consequently, when a binary choice is denied, service providers should revert to less intrusive methods of data collection (DP 6) with which some users might be more comfortable.

Limitations

Our study features certain limitations. First, our treatments were designed using the EU GDPR as underlying framework. Because the regulation is an abstract norm, it does not give concrete design requirements. While our study and design principles are one potential interpretation, there might be other ways to transparently provide information that will impact users differently. Moreover, users might want to receive further information such as technical details regarding the types of and protective measures applied to involved IT systems, which are categories of information that go beyond those mandated in the EU GDPR. Further, we only tested the impact of the "location always" permission, which is known to raise substantial privacy concerns.

We conducted a hypothetical web-based experiment that resembles real-world conditions by mimicking the look and feel and use case of an Apple iOS app. However, the experimental conditions may have biased the results. In particular, the level of acceptance might have been negatively affected by the random sample used in the experiment. A random sample is unlikely to be as interested in the app's features as a sample of tech-savvy users; those who download the app are more motivated to use it and are more likely to consent to data processing. Further, the level of comprehension might be positively biased because we asked users to read the text carefully. In the real world, users' primary desire is to use the app and privacy notices and permission requests are often seen as a distraction (Jensen and Potts 2004).

Conclusion

In this work, we demonstrated that increasing the transparency of data processing practices in the context of mobile privacy decision making does increase users' comprehension of their consent decisions but does not influence the decision outcome. We designed two treatments and identified six design principles that app service providers can use to design privacy-transparent mobile apps. Augmentation of standard permission request dialogues with privacy-related information and a dedicated onboarding process support users in making informed decisions.

Data-driven service can be a boon or a bane for users as the perceived benefits of personalization are often more visible than the perceived risks of sharing personal data. Mobile privacy decision making is particularly complicated because mobile devices provide far-reaching access to personal data but their interfaces complicate the communication of privacy-related terms of service. Increased transparency is an essential requirement for making informed consent decisions and might fundamentally influence users' behavior regarding (mobile) privacy decision making in the long run. This stream of research will be fruitful for future interdisciplinary research at the intersection of information systems, computer science, law, psychology, and service marketing. As the EU GDPR will continue to impact both users and service providers, we hope to see studies on the longitudinal impact of increased transparency on users' privacy-related behavior and service providers' business models soon.

Acknowledgements The research leading to these results has received funding from the RISE Programme of the European Union's Horizon 2020 Programme under REA grant agreement no. 645751 (RISE-BPM H2020-MSCA-RISE-2014). The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Appendix

A.1 Comprehension of the consequences of the consent decision

We asked ten questions to assess the participants' comprehension of the consequences of the consent decision using a binary choice with a *don't know* option. Each dimension of data privacy was surveyed with two questions. The questions were sorted so that questions of the same dimension were not visible at the same time to prevent users from answering by a process of elimination.

- Collected Data
  - The app monitors the products I have bought.
  - The app records whenever I visit a partner shop.
- Time of Collection
  - The app can access my location information at any time, even when I am not using it.
  - The app accesses my location information only when I am actively interacting with it.
- Processing
  - The app uses profiling to determine my shopping preferences.
  - My shop visits are processed with data on other users' visits to find shops that I might like.
- Sharing
  - Partner shops I visit can access my collected personal data.
  - shop.io sells user profiles to third parties.
- Erasure
  - shop.io retains my personal data until further notice.
  - shop.io will delete my personal data upon my request.

A.2 Identifying habituation

We asked two questions to determine if a participant decides on app permission requests as such by habit, using a five-point Likert scale (never, very rarely, occasionally, frequently, very frequently).

- How often do you **accept** app permission dialogs without reading them?
- How often do you **decline** app permission dialogs without reading them?

A.3 Submit times across conditions

We measured how much time participants took to make a decision (Fig. 5). The box plots represent the distribution of total time taken for the final decision across the three groups. For the onboarding condition, the data are further segmented; (a) only considers the time taken for the final location permission request, and (b) sums up the time measured for the entire onboarding condition including the four screens presented to the participants ex ante. Participants in the onboarding condition took considerably

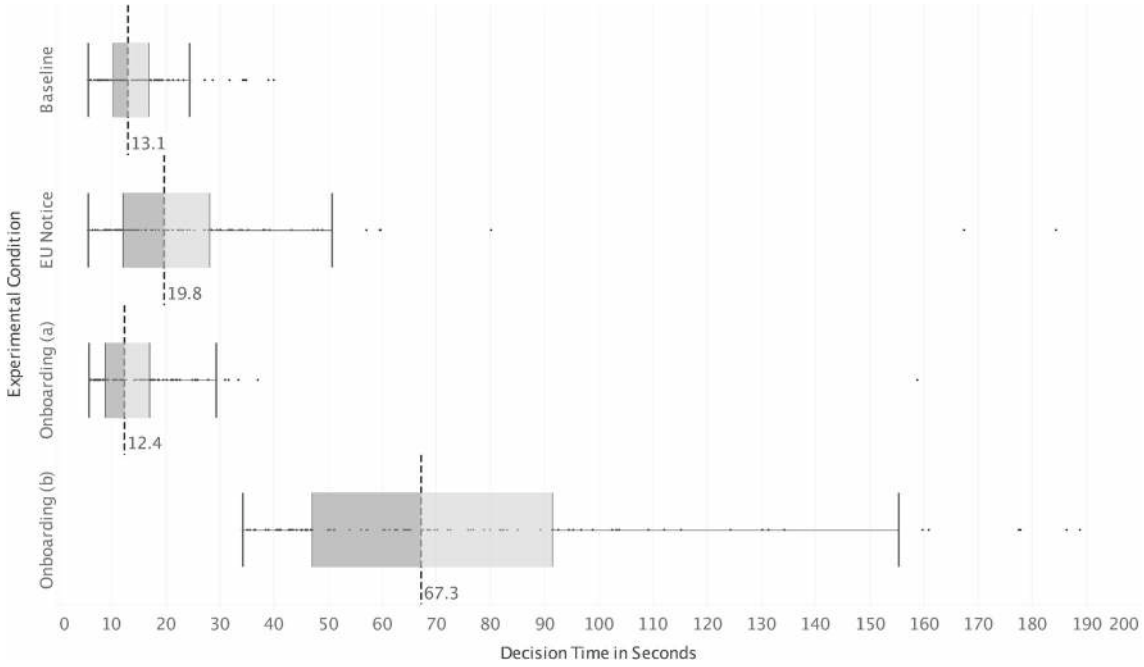


Fig. 5 Submit time for each experimental condition

more time for the entire process, which is plausible as they were confronted with substantially more text. However, it is worth mentioning that these participants took less time to make a decision regarding the actual permission request compared to the other two conditions, despite the fact that the provided text is twice the length of the marketing-driven text in the baseline condition.

A.4 Distribution of comprehension performance across conditions

Table 5 presents the distribution of the total scores achieved by the respective number of participants in each condition. This table ranges from −6 to 10 points as no participant scored below −6 points (i.e., each participant gave at least two correct answers). The baseline condition featured the most participants with very low overall scores. With increasing transparency, a clear shift occurred; more participants achieved considerably higher scores in the other two conditions, with a total of 15 participants who had answered at least 9 questions correctly in the onboarding condition. Participants across all groups who denied the permission request achieved a comprehension score that was about 13% higher than that of participants who gave permission (1.78 vs. 1.57).

A.5 Rationales for deciding on the location permission request

Immediately after making a decision regarding the location permission request and before seeing the comprehension questions, the participants were asked to provide a rationale for their decision by means of an open-ended question. The data was subject to qualitative content analysis (Mayring 2014) and was independently coded by two researchers. Table 6a and b provide the respective inter-rater agreements by content category using percent agreement and Cohen's Kappa.

Tables 7 and 8 provide the participants' reasons for accepting respective denying the location permission requests. The answers are clustered into content categories. For each category, the numbers of mentions by condition, category descriptions, and anchor examples from the survey are provided.

Table 5 Distribution of comprehension performance across conditions

	−6	−4	−2	0	2	4	6	8	10	∅
Baseline	3	11	21	37	19	10	4	0	0	−.02
EU Notice	4	8	15	20	21	20	11	4	1	1.38
Onboarding	1	0	5	13	20	21	23	14	1	3.76

Table 6 Inter-rater agreements

Category	Percent agreement	Cohen's Kappa
(a) Inter-rater agreement regarding responses for accepting the permission request		
Benefit	84.88	.691
Functional	88.95	.777
Habituation	98.84	.894
Trust	100	1
Ignorance	98.84	.851
Control	99.42	.854
Unrelated	98.26	.815
∅	95.60	.840
(b) Inter-rater agreement regarding responses for denying the permission request		
Tracking	94.81	.884
Permanent Access	98.52	.965
Privacy	92.59	.822
Use of Resources	100	1
Habituation	91.85	.623
Lack of Comprehension	97.04	.841
Fear of Abuse	98.52	.867
Disinterest	98.52	.826
∅	96.48	.853

Table 7 Participants' reasons for accepting the location permission request

Category	Frequency[a]	Description	Evidence
Benefit	111 (39, 38, 34)	The respondent gave the permission to receive personal benefits such as personalized service and promotions.	"I want the best deals"
Functional	89 (26, 29, 24)	The respondent named granting the permission a prerequisite for proper service execution.	"To allow them to track what shops I go into"
Habituation	10 (5, 3, 2)	The decision was made out of habit without reflecting its consequences.	"Knee-jerk reaction. I always allow apps access to my location"
Trust	10 (1, 1, 8)	The respondent explicitly stated to trust the app given the previously received information.	"The app gave me a peace of mind after informing me in detail how it will use my personal data - most importantly, my data wouldn't be shared. After that, I felt that I could trust the application."
Ignorance	8 (2, 3, 3)	The respondent explicitly stated to not care for the consequences of the decision.	"There are so much inevitable data miners in this day and age that even if there was something suspicious about it, it wouldn't mean much."
Control	5 (1, 2, 2)	The respondent explicitly stated a feeling of control regarding the option to withdraw consent and revoke the permission later.	"I can easily opt out if/when I delete the app [...]"
Unrelated	10 (3, 6, 1)	The answer did not contribute any meaningful explanation of the respondent's behavior.	"as i know its a survey and not real life"

[a]Total number of mentions (Baseline, EU Notice, Onboarding)

Quotes are taken verbatim

Table 8 Participants' reasons for denying the location permission request

Category	Frequency[a]	Description	Evidence
Tracking	45 (15, 17, 13)	The respondent stated a feeling of intrusiveness and disliked to be tracked by the service provider.	"It is scary to know that my location is tracked down even if the data might gets anonymized."
Permanent Access	43 (13, 20, 10)	The respondent named permanent background access to location data an inhibitor, but would grant access to location data for the time the app is actively opened and used.	"Because I'd rather just turn on location sharing when I leave home to go on a shopping trip, rather than always allowing location data to be shared as I feel that's a bit too much."
Privacy	42 (12, 9 ,21)	The respondent stated general privacy concerns that were not specific to the given shop.io scenario.	"I am very paranoid about location services."
Use of Resources	21 (9, 8, 4)	The respondent feared the app's/location service's use of power or data.	"It runs my battery down [...]"
Habituation	19 (7, 7, 5)	The respondent has completely disabled location features or usually denies location permission requests.	"I usually disable all the location function in order to protect my privacy."
Lack of Comprehension	17 (6, 2, 9)	The respondent did not understand, why the permission is needed.	"The app uses Bluetooth and doesn't need your location"
Fear of Abuse	10 (5, 1, 4)	The respondent explicitly stated a fear of abuse of the location data by third-parties.	"It makes me suspicious that it is collecting this information to sell."
Disinterest	7 (1, 2, 4)	The respondent was not interested in the functions enabled by location services.	"It doesn't seem like an app I would use, I don't really see a benefit for me."

[a]Total number of mentions (Baseline, EU Notice, Onboarding)

Quotes are taken verbatim

References

Acquisti, A. (2009). Nudging privacy: the behavioral economics of personal information. *IEEE Security and Privacy*, *7*(6), 82–85.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy*, *3*(1), 26–33.

Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–515.

Adjerid, A., Peer, E., Acquisti, A. (2018). Beyond the privacy paradox: objective versus relative risk in privacy decision making. *MIS Quarterly*, *42*(2), 465–488.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y. (2015). Your location has been shared 5,398 Times! In *Proceedings of the 33rd annual ACM conference on human factors in computing systems. CHI '15* (pp. 787–796). Seoul.

Aydin, A., Piorkowski, D., Tripp, O., Ferrara, P., Pistoia, M. (2017). Visual configuration of mobile privacy policies. In R. Huisman (Ed.), *Fundamental approaches to software engineering* (pp. 338–355). LNCS 10202.

Balebako, R., Jung, J., Lu, W., Cranor, L.F., Nguyen, C. (2013). "Little brothers watching you:" raising awareness of data leaks on Smartphones. In *Proceedings of the 9th symposium on usable privacy and security. SOUPS '13*. Newcastle.

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., Cranor, L. (2015). The impact of timing on the salience of Smartphone App Privacy Notices. In *Proceedings of the 5th annual ACM CCS workshop on security and privacy in Smartphones and mobile devices. SPSM '15* (pp. 63–74). Denver.

Bartelheimer, C., Betzing, J.H., Berendes, I., Beverungen, D. (2018). Designing multi-sided community platforms for local high street retail. In *26th European conference on information systems. ECIS '18*. Portsmouth.

Berinsky, A.J., Huber, G.A., Lenz, G.S. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis*, *20*(3), 351–368.

Betzing, J.H. (2018). Beacon-based customer tracking across the high street: perspectives for location-based smart services in retail. In *24th Americas conference on information systems. AMCIS '18*. New Orleans.

Böhme, R., & Grossklags, J. (2011). The security cost of cheap user interaction. In *Proceedings of the 2011 new security paradigms workshop. NSPW '11* (pp. 67–82). Marin County.

Brandimarte, L., Acquisti, A., Loewenstein, G. (2013). Misplaced confidences: privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347.

Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law and Security Review*, *32*(3), 462–473.

Chellapa, R., & Sin, R.G. (2005). Personalisation vs. privacy: an empirical examination of the online consumers' dilemma. *Information Technology and Management*, *6*(2–3), 181–202.

Cohen, C. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale: Lawrence Erlbaum Associates.

Dhar, S., & Varshney, U. (2011). Challenges and business models for mobile location-based services and advertising. *Communications of the ACM*, *54*(5), 121–129.

Dinev, T., Tamara, T., Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dolnicar, S., & Grün, B. (2014). Including don't know answer options in brand image surveys improves data quality. *International Journal of Market Research*, *56*(1), 33–50.

Eastin, M.S., Brinson, N.H., Doorey, A., Wilcox, G. (2016). Living in a big data world: predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220.

European Union (2016). Regulation 2016/679 of the European parliament and the Council of the European Union. http://eur-lex.europa.eu/eli/reg/2016/679/oj. (visited on 11/07/2018).

Executive Office of the President (2015). *Big data and differential pricing*. Tech. rep. Washington: Executive Office of the President.

Faul, F., Erdfelder, E., Lang, A.-G., Buchner, A. (2007). G*Power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D. (2012). Android permissions: user attention, comprehension, and behavior. In *Proceedings of the 8th symposium on usable privacy and security. SOUPS '12*. Washington, D.C.

Fisher, D., Dorner, L., Wagner, D. (2012). Short paper: location privacy: user behavior in the field. In *Proceedings of the second ACM workshop on security and privacy in smartphones and mobile devices. SPSM '12* (pp. 51–56). Raleigh.

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., Schmied, F. (2018). The upside of data privacy—delighting customers by implementing data privacy measures. *Electronic Markets*, *28*(4), 437–452.

Harbach, M., Hettig, M., Weber, S., Smith, M. (2014). Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems. CHI '14* (pp. 2647–2656).

Hern, A., & Waterson, J. (2018). Sites block users, shut down activities and flood inboxes as GDPR rules loom. In *The Guardian*. http://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect. (visited on 11/03/2018).

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on human factors in computing systems. CHI '04* (pp. 471–478). Vienna.

Johnson, D., & Grayson, K. (2005). Cognitive and affective trust in service relationships. *Journal of Business Research*, *58*(4), 500–507.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C. (2013). Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies*, *71*(12), 1163–1173.

Keith, M.J., Babb, J., Furner, C.P., Abdullat, A., Lowry, P.B. (2016). Limited information and quick decisions: consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction*, *8*(3), 88–130.

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D. (2012). A conundrum of permissions: installing applications on an Android Smartphone. In *International conference on financial cryptography and data security* (pp. 68–79).

Kelley, P.G., Cranor, L.F., Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems. CHI '13* (pp. 3393–3402). Paris.

Kosinski, M., Matz, S.C., Gosling, S.D., Popov, V., Stillwell, D. (2015). Facebook as a research tool for the social sciences: opportunities, challenges, ethical considerations, and practical guidelines. *American Psychologist*, *70*(6), 543–556.

Kumaraguru, P., & Cranor, L.F. (2005). *Privacy indexes: a survey of Westin's studies* (pp. 1–22). Tech. rep. Pittsburgh: Institute for Software Research International (ISRI).

Landis, J.R., & Koch, G.G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*, 159–174.

Libert, T., Graves, L., Kleis Nielsen, R. (2018). *Changes in third-party content on European News Websites after GDPR*. Tech. rep. Oxford: Reuters Institute for the Study of Journalism.

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J.I., Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile App privacy through Crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing. UbiComp '12* (pp. 501–510). Pittsburgh.

Marrs, M. (2016). App Onboarding 101: 7 tips for creating engaged, informed users. http://info.localytics.com/blog/app-onboarding-101. (visited on 11/07/2018).

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*(1), 1–23.

Mayring, P. (2014). *Qualitative content analysis. Theoretical foundation, basic procedures and software solution* (p. 143). Klagenfurt: Beltz.

McDonald, A.M., & Cranor, L.F. (2008). The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, *4*(3), 543–568.

NTIA (2013). Short form notice code of conduct to promote transparency in mobile app practices. https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf. (visited on 11/07/2018).

OECD (2006). *Making privacy notices simple*. Tech. rep. Paris: OECD Publishing.

Oppenheimer, D.M., Meyvis, T., Davidenko, N. (2009). Instructional manipulation checks: detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867–872.

Pentina, I., Zhang, L., Bata, H., Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419.

Podesta, J., Pritzker, P., Moniz, E.J., Holdren, J., Zients, J. (2014). *Big data: seizing opportunities, preserving values*. Tech. rep. Washington, D.C.: Executive Office of the President of USA.

Robinson, N., Graux, H., Botterman, M., Valeri, L. (2009). *Review of EU data protection directive: summary*. Tech. rep. Information Commissioner's Office.

Rosenberg, M., Confessore, N., Cadwalladr, C. (2018). How Trump consultants exploited the Facebook data of millions. In *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. (visited on 11/07/2018).

Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, *3*(2), 267–274.

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F. (2015). A design space for effective privacy notices. In *Proceedings of the 11th symposium on usable privacy and security. SOUPS '15*. Ottawa.

Schwartz, P.M. (2004). Property, privacy, and personal data. *Harvard Law Review*, *117*(7), 2056.

Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H. (2014). Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI*

conference on human factors in computing systems. CHI '14 (pp. 2347–2356). Toronto.

Sombatteera, S., & Kalyuga, S. (2012). When dual sensory mode with limited text presentation enhance learning. *Procedia - Social and Behavioral Sciences*, *69*, 2022–2026.

Tan, J., Nguyen, K., Theodorides, M., Negòn-Arroyo, H., Thompson, C., Egelman, S., Wagner, D. (2014). The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI conference on human factors in computing systems. CHI '14* (pp. 91–100). Toronto.

Taylor, H. (2003). Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. *The Harris Poll*, *17*(19), 44.

Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research*, *22*(2), 254–268.

Voorhees, C.M., Fombelle, P.W., Gregoire, Y., Bone, S., Gustafsson, A., Sousa, R., Walkowiak, T. (2017). Service encounters, experiences and the customer journey: defining the field and a call to expand our lens. *Journal of Business Research*, *79*, 269–280.

Wetherall, C., Greenstein, H., Hornyack, J., Schechter, W. (2011). Privacy revelations for web and mobile apps. In *Proceedings of the 13th USENIX conference on hot topics in operating systems. HotOS '11*. Napa.

Wohlgemuth, S., Sackmann, S., Sonehara, N., Tjoa, A.M. (2014). Security and privacy in business networking. *Electronic Markets*, *24*(2), 81–88.

Xu, H., Luo, X., Carroll, J.M., Rosson, M.B. (2011). The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52.