An (Un)Necessary Evil - Users' (Un)Certainty about Smartphone App Permissions and Implications for Privacy Engineering

Kerstin Bongard-Blanchy
Department of Behavioural and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg
kerstin.bongard-blanchy@uni.lu

Jean-Louis Sterckx
Department of Behavioural and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg
jean-louis.sterckx@live.be

Arianna Rossi
Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg
Esch-sur-Alzette, Luxembourg
arianna.rossi@uni.lu

Verena Distler
Department of Behavioural and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg
verena.distler@uni.lu

Salvador Rivas
Luxembourg Center for Educational Testing (LUCET)
University of Luxembourg
Esch-sur-Alzette, Luxembourg
salvador.rivas@uni.lu

Vincent Koenig
Department of Behavioural and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

***Abstract*—App permission requests are a control mechanism meant to help users oversee and safeguard access to data and resources on their smartphones. To decide whether to accept or deny such requests and make this consent valid, users need to understand the underlying reasons and judge the relevance of disclosing data in line with their own use of an app. This study investigates people's certainty about app permission requests via an online survey with 400 representative participants of the UK population. The results demonstrate that users are uncertain about the necessity of granting app permissions for about half of the tested permission requests. This implies substantial privacy risks, which are discussed in the paper, resulting in a call for user protecting interventions by privacy engineers.**

***Index Terms*—human computer interaction, user interface, design, security evaluation**

1. Introduction

"GoogleMaps would like to access your location." As users of mobile phones, we come across such requests regularly. The newly installed social media app would like to access our contacts, and the texting app asks for access to our photos triggered by our wish to share a screenshot with a friend. Apps rely on user's personal data and smartphone resources to fulfil their purpose because, indeed, of what use would a navigation app be without access to the user's location? Install-time permissions are granted automatically by the system when the app is installed, while run-time permissions may access personal data (e.g., contacts) including user-generated content (e.g., photos), protected resources (e.g., Wifi connections), and device functionalities and sensors (e.g., camera) [1], [2]. App permissions constitute an access-control mechanism that regulates the app's access to such system resources [3]: users need to explicitly grant permission before an app can start accessing restricted data or performing restricted actions. These decisions determine users' privacy on their mobile devices and the entailed risks. Privacy engineers need to balance the amount and type of data they gather with the regulatory obligations these require. More data bring about a higher risk and demand more robust security measures for the app companies.

As per developer guidelines, information about the type of data and why they are collected must be communicated transparently to allow people to understand what the app will access and thus exercise an informed decision [1], [2]. However, deciding how to answer an app permission request is a non-trivial task that interrupts the user's primary task. Moreover, users typically have an imperfect understanding of the consequences of choosing one option over the other: declining the permission could potentially lead to a loss of app functionality, whereas accepting it could lead to an excessive disclosure of personal data with severe implications on data confidentiality, especially when apps gather sensitive information (e.g., health apps).

This survey investigates whether users consider app permission requests understandable enough to make an informed decision when they grant access to their smartphones' data and resources. We contribute to the discussion about the transparency and understandability of privacy notices and discuss how the current practices infringe upon legal obligations in the EU and other places. We provide suggestions on actions that can be taken by privacy engineers to communicate more transparently and protect user privacy more effectively.

DOI 10.1109/EuroS&PW55150.2022.00023

2. Related work

Some argue that, if decision-making regarding app permissions was completely rational, users would grant the fewest permissions needed for their regular use of the app to protect their privacy [4]. However, due to the constant evolution of information technologies and the complex, nuanced trade-offs associated with decisions about one's personal data, users are left with incomplete information about both the set of possible privacy-relevant outcomes (e.g., sharing of location data to advertisers) and the respective consequences (e.g., receiving location-based personalized ads) [5], [6]. As users face these layers of complexity, bounded rationality and systematic psychological deviations from rationality (i.e., cognitive biases) influence the decision-making process [7]. According to the dual-system thinking theory [8], "warning fatigue" is also likely to influence user behaviour when reacting to permission requests. Users become habituated to frequent warnings and notifications, leading them to simply "click away" permission requests to continue with their primary task, rather than reading, trying to understand the request [9] and taking decisions accordingly.

Research has also shown that it is difficult for users to understand app permissions. In a series of semi-structured interviews, Kelley et al. [10] noticed that users did not understand Android permissions when they installed an application. Many participants ignored the permissions and used word of mouth and ranking as elements to decide whether to install the app instead. Felt et al. [11] found that most study participants did not pay attention to Android permissions, and only 3% understood the implications of the permission requests correctly. The other participants imagined the permission's scope to be narrower or broader than it was. The authors concluded that most individuals could not derive the inherited privacy risks from the permission descriptions, leading them to overestimate or underestimate such risks. While factual understanding takes is vital for users' decision-making, another less researched yet decisive aspect is their perceived understanding, i.e., the uncertainty they experience about the meaning and consequences of their permission choices. The uncertainty laypeople feel towards personal data disclosure requests, together with privacy risk, ambiguity of language and framing, are likely to influence their privacy decisions [12], [13].

Various studies demonstrate that apps often ask for more permissions than needed [14], [15], and users seem, at least in part, aware of such practice [3]. Unfortunately, the current permission-based app model has a relatively narrow focus on what an app does (i.e., app X wants to access Y), but it tends to gloss over whether and how that action engenders risks or other consequences for the users [16].

3. Research questions

This survey seeks to investigate **(RQ1) to which extent users associate uncertainty with app permissions.** We hypothesize that uncertainty arises from a lack of understanding of the link between the app features and the app permissions (permission-feature link). If a user is unsure why an app needs a specific permission, they will be unsure whether they should accept or decline the access request. We, therefore, ask: **(RQ2) To which extent do people understand why applications ask for specific app permissions?** Here we focus on perceived understanding by exploring whether participants, who are familiar with the app, *think* they understand what the app permission does. We do *not* evaluate participants' factual understanding. Beyond the permission-feature link, uncertainty may furthermore arise when the user is unsure whether a feature is relevant for their app use (relevance-feature link). Suppose a user understands why an app needs the permission (e.g., TikTok needs access to the camera so that users can film the clips to post), they might still be uncertain about the relevance for their own app use (e.g., will I use TikTok to post clips versus only watch other users' clips?). We hence furthermore ask: **(RQ3) To which extent do people consider specific app permissions relevant for their own app use?**

4. Method

We conducted an online survey in December 2021, hosted on Limesurvey and distributed via the Prolific platform [17]. We recruited 400 adult participants using the sampling option that allows gathering a representative sample of the UK population in terms of age, gender and ethnicity, matching the numbers of the UK Office of National Statistics. The survey completion took about 5 minutes. Participants received a compensation of £7.55/hr. The study obtained ethical clearance from the institutional board.

As study material, we selected eight of the most downloaded mobile phone apps worldwide [18] with their associated app permissions (48 in total) and wordings as stipulated in the Google Play store [19] (cf. Table 1). After demographic questions (i.e., age, gender, education and mobile phone operating system), the participants were asked to select all the apps they use at least once a month from eight options. Next, participants saw all applicable permissions of their selected app(s) and answered the following question: *When using (app name) on your mobile phone, these are the permissions that the app can ask. Do you understand why (app name) needs the following permission?* The answer options were binary: *I understand why the app needs this permission* or *I am not sure why the app needs this permission.* The answers allowed calculating the percentage of participants that considered each request understandable. A negative answer was considered an indicator of user uncertainty (cf. Figure 1).

However, even if users believe they understand why the app asks for a specific permission, they might not be certain about its relevance for their own app use. Therefore, participants saw a second question block with all permissions they had rated as understandable in the first block. This time they answered the question: *Do you find the following permission relevant for how you use (app name)?* The three answer options were: *Yes, this permission is relevant* or *I'm not sure this permission is relevant* or *No, this permission is not relevant*. We computed the percentages of the occurrence for the three answers. If participants found the app permission relevant or irrelevant, we considered the participants' choice as certain. We combined the results of the two question blocks

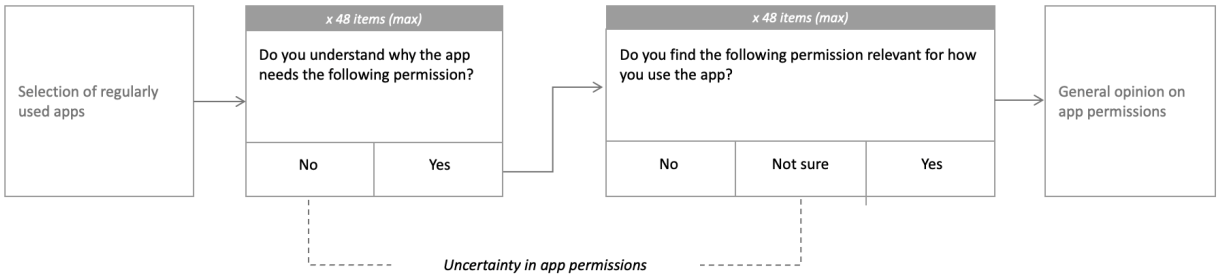

Figure 1. Survey architecture, combining understandability and relevance as a measure for (un)certainty.

by coding certainty as absent if participants answered a lack of understanding in question 1 or uncertainty about the permission's relevance in question 2 (c.f. Fig. 1). As a result, we obtained a certainty percentage per app per permission. At the end of the survey, participants could share their general opinion on app permissions via a text field (*What is your take on app permissions?*). We coded their comments inductively with MaxQDA along the categories *understanding, relevance, consent strategy, consent requirements, and general attitude*. 10% of the data were double coded by two researcher pairs, yielding an interrater agreement of Kappa Brennan & Prediger 0.77 and 0.79 respectively. Researcher 2 finalized the coding of the whole data set.

5. Results

5.1. Understandability of app permissions

When investigating the extent to which people understand why apps ask for specific permissions (RQ2), we see a strong divide between seemingly obvious app permission requests and ambiguous ones. Table 1 displays the percentage of participants who rated the permission request as understandable. The least understandable permission (below 20%) requests appeared to be calendar for TikTok, contacts for Youtube, camera for Spotify, and contacts for GoogleMaps. Most users failed to see why the apps require access to such data or resources. The permissions that almost all participants who are familiar with the app found understandable were location for GoogleMaps, camera and microphone for TikTok, contacts and camera and microphone for WhatsApp, camera for Instagram, storage for Spotify, and contacts for Messenger. These permissions concern access to data and resources that constitute the app's core functionality.

In our open-ended question, we asked participants more generally about their opinion on app permissions. 51 of the 400 (13%) participants stated their general understanding of those app permission requests (e.g., *"I do understand that some permissions are required or the app couldn't work" P036*). Regarding strategies, 13 (3%) participants explicitly indicated not paying much attention to app permission requests. 22 (6%) always accept (*"I am too trusting with apps perhaps and since I need to use them to make my life more convenient I am rather naïve in assuming everything is secure and necessary" P382*), while 5 (1%) reject the permission requests by default (*"I don't understand why apps need to have access to these features on my phone, i usually say no when they ask unless it's unavoidable" P202*)". 16 (4%) of the 400 participants minimize their acceptance rate (*"I am relatively tight on them, and unless I have an understanding of the reasons why permission is required, I won't accept" P170*). Many (63, i.e., 16%) attested difficulties in understanding the underlying reason for the requests (*"I'm often not sure why they are needed or what I am allowing the app to do" P017).*

5.2. Relevance of app permissions

Regarding the extent to which people consider specific app permissions relevant for their app use (RQ3), we observed a strong linear relationship between participants' perceived understanding of an app permission and the perceived relevance for their app use (r=.86). Participants evaluated very few permissions as irrelevant, possibly suggesting that irrelevant requests had already been assessed as not understandable. Table 2 displays the percentage of participants who rated the permission requests as not relevant (-), uncertain (0) or relevant (+) for their app use. The least relevant permissions (Table 2) were camera for Spotify, calendar for TikTok, contacts for Youtube, and calendar for Messenger. They were considered relevant for app use by less than half of the participants who understood why the app asked for the permission in the first place. In the qualitative answers, participants voiced doubts when it came to such permission requests (*"I believe that not all the permissions that I give or am asked to give are necessary for my full enjoyment of the app" P025*.

The permissions that obtained the highest relevance percentages were location for GoogleMaps, camera and storage and microphone for Instagram, camera and microphone and contacts for Messenger, storage for Spotify, microphone and camera for TikTok, camera and contacts and microphone for WhatsApp. Those permissions were considered indispensable for the app use (*"I think that they are mostly relevant because a lot of apps, such as Instagram and Whatsapp, are used to share photos or send voice notes so require access from the camera and microphone. But I am unsure why a lot of these apps ask for location" P001).* 27 (7%) of the 400 participants explicitly stated that they deliberately reflect on the relevance of the requested data or resource before granting an app access (*"I generally grant permission only if it's clear why the app needs the permission, and how I will benefit by granting it" P349).*

	GoogleMaps	Instagram	Messenger	Spotify	TikTok	Twitter	WhatsApp	YouTube
Calendar			32%		**9%**			
Call logs							43%	
Camera	27%	90%	73%	**13%**	95%	65%	85%	45%
Contacts	**17%**	60%	80%	25%	56%	55%	91%	**12%**
Location	98%	73%	52%			63%	47%	41%
Microphone	38%	73%	72%	32%	92%	44%	83%	50%
Phone		44%	60%			44%	72%	29%
Sms			40%				48%	
Storage	50%	65%	56%	83%	65%	55%	71%	51%

TABLE 1. PERCENTAGE OF PARTICIPANTS WHO RATED THE PERMISSION REQUEST AS UNDERSTANDABLE. THE APP PERMISSION REQUESTS WITH THE LOWEST UNDERSTANDABILITY PERCENTAGES ARE MARKED IN BOLD.

	GoogleMaps			Instagram			Messenger			Spotify			TikTok			Twitter			WhatsApp			YouTube		
	-	0	+	-	0	+	-	0	+	-	0	+	-	0	+	-	0	+	-	0	+	-	0	+
Calendar							17	37	**46**				43	29	**29**									
Call-logs																			8	24	68			
Camera	18	28	54	4	3	**93**	4	8	**89**	32	32	**36**	11	3	**87**	15	18	68	2	6	**92**	16	12	71
Contacts	23	25	52	18	27	55	5	15	**80**	29	21	50	20	18	61	20	29	51	2	7	**92**	22	34	**44**
Location	1	1	**98**	11	29	60	15	21	63							19	19	61	9	27	64	9	39	52
Microphone	16	22	62	7	12	**81**	7	11	**82**	11	25	64	11	1	**88**	18	12	69	5	8	**87**	15	20	65
Phone				14	19	67	6	25	69							15	20	65	4	21	75	10	22	68
Sms							11	20	69										7	24	69			
Storage	3	24	73	1	14	**84**	4	17	79	1	17	**82**	4	20	76	5	20	75	3	18	79	9	19	72

TABLE 2. PERCENTAGE OF PARTICIPANTS WHO RATED THE PERMISSION REQUEST AS NOT RELEVANT (-), UNCERTAIN (0) OR RELEVANT (+) FOR THEIR APP USE. THE APP PERMISSION REQUESTS WITH THE LOWEST AND HIGHEST PERCENTAGES ARE MARKED IN BOLD.

5.3. Uncertainty in app permission choices

When we combine the results for understandability and relevance, we obtain the certainty level for each permission per app (RQ1). In Table 3, high percentages indicate that most users understand why the app needs the requested data or resources and can judge the relevance for their app use. Among the evaluated app permissions, those for which participants had the lowest certainty were camera and contacts for GoogleMaps, calendar for Messenger, camera and contacts and microphone for Sportify, calendar for TikTok, contacts and location, and phone for YouTube.

Looking at the results from the individual participant's perspective, the average survey participant reported being uncertain about app permission requests 56% of the time, which translates into being uncertain of an average of 28 permissions for the total of 48 tested app permissions. In line with this result, the participants' comments reflect an ambiguous attitude towards app permission requests. While 54 (14%) of the 400 participants appreciate them as a privacy-protecting mechanism (*"Necessary so apps don't use you're [sic] information without knowledge" P233*), 65 (16%) participants voiced suspicion towards tech companies' data management practices. They suspect that a great part of the app permissions serves to exploit user data (*"I think some of the permissions I give are more beneficial to the app provider in giving them more data about my profile that helps them market their services to me" P025).*

Playing on users' uncertainty is a privacy dark pattern [20] which here too seems a winning strategy for companies who seek to gather user data beyond what is needed for their app. This was underlined by comments of 23 (6%) participants who believe their loss of privacy is the price they have to pay for using specific mobile apps (*"Some app permissions are not necessary yet they are there and you have no choice but to accept them in order to use the app." P187).* However, this can backfire for the company when users gain vigilance and move to the competitor that better protects their data(*"(...) if I think the permission that pops out is somehow relevant to what I was trying to do, then I usually just allow it. However, if it is not then I will not allow it to use the permission. In this particular case, if the app needs that permission to run then I usually just uninstall it and look for alternative applications." P269).*

To counteract excessive data gathering, 12 (4%) participants suggested that app permission requests should be limited to access data and resources that are strictly necessary for the app's functioning (*"Need to be limited to only what is needed and be clear about why they are needed" P265).* In this case, however, simply informing users without asking them to take any action would be a better strategy given that refusing would render certain functionalities of the app unusable (*"I think the permissions for the very obvious, essential access should be standard - ie maps needing location. If it wouldn't work without the permission then I don't think there is a need to ask." P150).*

Furthermore, 6 (2%) participants confirmed that it is easier to understand and judge the relevance of app permission requests if they appear in the use context instead of at the moment of app installation (*"Too many ask for all permissions at sign up even if I'll never use that facility ie camera on Tiktok when I only watch not post videos" P216).* Last but not least, numerous participants (35/9%) explicitly voiced the wish for better explanations (*"Perhaps instead of just asking for access to the microphone, apps should explain why." P028*) and regulation (*"they look like they aren't strictly regulated, for example "contacts" can mean a lot of things, I would like to know exactly what's being used." P209*) as a means

	GoogleMaps	Instagram	Messenger	Spotify	TikTok	Twitter	WhatsApp	YouTube
Calendar			**20%**		**6%**			
Call logs							33%	
Camera	**20%**	88%	68%	**9%**	92%	53%	80%	39%
Contacts	**13%**	44%	68%	**20%**	46%	39%	85%	**8%**
Location	97%	52%	41%			51%	34%	**25%**
Microphone	30%	64%	64%	**24%**	91%	39%	76%	40%
Phone		36%	45%			35%	57%	**23%**
Sms			32%				36%	
Storage	38%	56%	46%	69%	52%	44%	58%	41%

TABLE 3. PERCENTAGE OF PARTICIPANTS WHO ARE CERTAIN ABOUT THE APP PERMISSION REQUEST CALCULATED AS COMBINED RESULT FROM UNDERSTANDABILITY AND RELEVANCE RATING (IRRELEVANT OR RELEVANT). THE PERMISSIONS WITH THE LOWEST CERTAINTY PERCENTAGES ARE MARKED IN BOLD.

to take an informed decision when allowing apps to access their privacy-sensitive data and resources.

6. Discussion

App permission requests are meant to give users control over their data and other resources on their smartphones. However, the results of our study show that asking users to take granular decisions on each permission request for each app is not an effective strategy in this respect. It can be meaningful in those cases where people can judge the access request with high certainty because it is necessary for an app's core functionality (e.g., contacts for WhatsApp) or clearly relevant or irrelevant for specific users (e.g., camera for TikTok). Nevertheless, for many app permission requests, users are uncertain whether they should grant access or not. Thus we can assume that they do not know what they agree to and, most importantly, the privacy implications of their decisions. Even worse, in the case of the obviously necessary permission requests in our study (e.g., location for GoogleMaps), users might still have an incorrect understanding of what exactly the app will access and why, and what the inherited privacy risks are because no clear and comprehensive explanation on such aspects is provided.

Thus, app permission requests fall largely below the minimum requirement of transparency that is considered a threshold to justify and allow data processing in many legal regimes. For instance, in the EU, transparency is an overarching principle of the GDPR intended to allow individuals to "understand and, if necessary, challenge" how their personal data are processed [21, p.4]. To date, relevant details are entirely lacking, for instance, about how many times some data are accessed (which can demonstrably help users to adopt more privacy-preserving behaviours [22]) and to whom such information is disclosed and for which purposes. However, there is a fundamental tension on how to balance comprehensive information with a good user experience. The security context faces similar challenges. Recent research into how to best provide information on security mechanisms shows that a more detailed description of encryption leads to a more accurate understanding of the concept, without a negative effect on the user experience [23]. The authors also highlighted the challenge of defining and measuring non-experts' understanding of a technical and unfamiliar concept. This difficulty is likely to also play a role in the context of privacy permissions. Investigating the level of detail that privacy notices should provide to help people understand the privacy notice without disrupting their primary task is a pertinent direction for more research [24]. Similarly, the question of timing (i.e., when such notices should be presented to enable meaningful decision-making) [25] is a challenge that needs to be balanced with the legal requirement to inform users before the data collection occurs.

The results of our study show that even though people are uncertain about the privacy risks of providing app permissions, they still use the apps regularly. A lack of certainty does not necessarily motivate privacy-preserving behaviour, as convenience of use [26] and bandwagon effects (i.e., using an app because many others do) may be more influential. This is in line with previous work that highlighted the complexity of privacy trade-off decisions, finding that many factors beyond privacy concerns influence privacy decision-making (e.g., perceived usefulness of a technology, user autonomy, control, context-related factors) [27]. Moreover, always asking permission to access data and resources may lead to a bad user experience, while it does not necessarily translate into enhanced control over the app behaviour and one's own personal data. Similarly to cookie permission requests, access to strictly necessary data and resources should not be solicited [24]. Rather, the apps should be clear about what is necessary for their correct functioning, and what is not strictly necessary but useful for specific functionalities. This would allow users to only focus on truly risky practices where a decision is necessary [11] and counter warning fatigue which would help users fight the temptation to take blind decisions and provide apps access to anything they ask. In other words, present less but more meaningful requests. As the number of apps and sensors increases, an emerging solution is represented by smart privacy assistants that support Android users in the management of their permission settings through the use of personalized recommendations [28], [29]. Such automated, customized approaches are promising solutions to help users to efficiently manage their personal data in an increasingly digitized society, since privacy decisions are always contextual [30] and different users may have different needs and preferences that cannot be appropriately addressed through one-size-fits-all methods.

Another issue is that the reasons behind permission requests seem questionable when the access is not necessary for any app functionality, as studies have shown [31]–[33]. For instance, a recent survey [34] reveals that 80% of the 2020's top 10000 downloaded apps in terms of combined downloads across Android's Google Play and Apple's App

Store collect data for purposes that are unrelated to their functionality and are mostly used for product personalization and marketing. The majority of them, especially those developed by firms with larger market shares, tracks users and shares their data even of sensitive nature across networks and companies, including data brokers. The app tendency of requesting excessive privileges is growing [35], although it seems that regulations can help counter it: the GDPR's introduction of obligations for data minimization and purpose limitation (Art. 5, that restricts the data collection to what is "adequate, relevant and limited to what is necessary" and tied to "specified, explicit and legitimate purposes") and data protection by design and by default (Art. 25, that requires to process only personal data that are necessary for specific purposes) seem to have decreased excessive requests [3], even though more studies are necessary to confirm such a tendency.

Sometimes apps show overly data-hungry behaviour because their developers ignore what constitutes privacy-friendly practices in mobile data access [36], [37]. For instance, developers reuse existing code from available libraries that have been created with the advertisers' best interest in mind [38]. Several online blogs also provide wrong information, for example that the GDPR always requires user consent to process personal data [39], whereas consent is only one of the legal bases that can be used to motivate data processing. It could be argued that such disinformation can cause developers to ask for more permissions than needed, which engenders unnecessary legal and financial risks for the companies that develop and commercialize the apps, and that gather and often pass on their users' personal information. Data minimization is meant to lower such risks, as the more data, the more organizational and technical measures to protect them should be adopted. When data are of sensitive nature, like photos and locations could be considered, additional more stringent safeguards should apply. Failing to comply with data protection obligations can result in financial penalties, loss of reputation and loss of customers' trust.

The proverbial elephant in the room cannot be ignored either: the business model that supports many free apps is based on profiling and passing on the information they gather on the devices to dozens and even hundreds of advertisers [40]. Thus transparency about how user data are shared with other recipients may not be provided on purpose and would prove cumbersome to provide on the limited space of app permission requests. At that point, such transparency would not cause any actual benefit for the users when they cannot limit the disclosure of their personal information to third parties. This is where the decisions applied by app market gatekeepers, i.e., the app stores, can prove crucial. Bian et al. [34] demonstrated that the introduction of the Privacy Nutrition Label on Apple's App Store caused tangible decreases in app downloads (minus 15%) and in revenues from user subscriptions and in-app purchases (minus 14%), when compared to the same apps on the Google Store. Data-hungry apps significantly suffered more from increased transparency on data use. Such results imply that transparency can engender better privacy-aware decisions as long as it is provided in a concise, standardized form at meaningful points in time. It can also result in tangible financial losses for businesses. Requiring app developers to fill in the Privacy Nutrition Label can push them to be more truthful about their data practices and perhaps even review them, provided that there are mechanisms in place to check the veracity of such claims as many apps simply harvest data and access resources without disclosing it [40]–[42]. Watchdogs and researchers can use such disclosures to exercise better oversight on the practices of the app market. On the development and product design side efforts should be nevertheless undertaken to limit access to privacy-sensitive features by default. What is more, further development in privacy-enhancing technologies is urgently needed as such would allow companies to utilize user data in a meaningful, but privacy-preserving manner.

7. Limitations

App permission requests differ between operating systems. This study is based on app permissions described in the Google Play store [19] where they are explicitly listed. The Apple app store [43] does not show the permissions the app requests. They can only be viewed in the device's settings once the app is installed and in use. We initially intended to present a clear explanation for each app permission and its implications to the participants to allow them to judge the relevance for the different applications. Unfortunately, we could not find reliable resources that explain what happens when, e.g., an application accesses storage. We hence had to limit this study to the user's perceived understanding of app permissions.

It should also be noted that in a normal use situation, the app permission requests appear when the user attempts specific actions. The lack of such contextualization is a limitation of the present study design. Our findings nevertheless lay a general foundation upon which more contextualized studies can build.

Regarding the survey sample, we cannot be sure if the sample we recruited was as digitally literate and privacy-sensitive as the wider population. While Prolific allows the recruitment of a representative UK sample based on traditional demographic indicators (age, gender, ethnicity), other descriptors such as digital skills or privacy sensitivity are not available.

8. Future work

Systematic psychological deviations from rational choice are known to emerge when individuals operate under uncertainty [6], [44]. Uncertainty arises in privacy decision making through various means [12]. In the context of app permissions, we identified two types of uncertainty, 1) related to the link between an app's features and its permissions and 2) the link between a feature and its clearly identifiable relevance to the user. Systematic psychological deviations from rational choice are known to emerge when individuals operate under uncertainty [6], [44]. In a future study, we intend to examine how users' disclosure behaviour is affected by the uncertainty associated with an app permission and by framing messages, known to be associated with predictable shifts in choice preference. The findings will contribute to our understanding of how uncertainty affects data disclosure. Furthermore, the study will investigate whether framing messages affect disclosure behaviour when applied to app permissions. Lastly,

if we find an interaction effect between message framing and uncertainty, we hypothesize that users disclose more personal data when framing messages are presented in highly uncertain circumstances. The use of framing messages in app permissions could therefore be regarded as a privacy-intrusive practice, needing careful evaluation from watchdogs.

9. Conclusions

The current survey examined the extent of uncertainty users report experiencing with app permissions of popular mobile applications. We found that participants do not fully understand over half of the requests, hindering a reflected decision about granting or refusing applications access to their personal data and privacy-sensitive resources. We conclude that privacy by consent is not working as intended. Other ways to protect user privacy are urgently needed. In a first step, privacy engineers should limit the use of privacy-sensitive features in mobile applications to what is necessary for the application's core functions. Furthermore, they need guidance to explain better why an app requests access to a specific resource so that users can judge the relevance for their app use and make truly informed decisions. Ultimately privacy-enhancing technologies are another promising path towards better user privacy protection.

Acknowledgment

This work has been partially supported by the Luxembourg National Research Fund (FNR) – IS/14717072 "Deceptive Patterns Online (Decepticon)"

References

[1] Android. (2021) Permissions on android. [Online]. Available: https://developer.android.com/guide/topics/permissions/overview

[2] Apple. (2021) Accessing user data and resources. [Online]. Available: https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/accessing-user-data/

[3] N. Momen, M. Hatamian, and L. Fritsch, "Did app privacy improve after the GDPR?" *IEEE Security & Privacy*, vol. 17, no. 6, p. 10–20, Nov 2019.

[4] Q. Ismail, T. Ahmed, A. Kapadia, and M. K. Reiter, "Crowdsourced Exploration of Security Configurations," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Seoul Republic of Korea: ACM, Apr. 2015, pp. 467–476. [Online]. Available: https://dl.acm.org/doi/10.1145/2702123.2702370

[5] G. A. Akerlof, "The market for "lemons": Quality uncertainty and the market mechanism," *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, 1970. [Online]. Available: http://www.jstor.org/stable/1879431

[6] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Comput. Surv.*, vol. 50, no. 3, aug 2017. [Online]. Available: https://doi.org/10.1145/3054926

[7] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *Security & Privacy, IEEE*, vol. 3, pp. 26 – 33, 02 2005.

[8] D. Kahneman, *Thinking, fast and slow*. Macmillan, 2011.

[9] A. Sasse, "Scaring and Bullying People into Security Won't Work," *IEEE Security & Privacy*, vol. 13, no. 3, pp. 80–83, May 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7118083/

[10] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone," in *Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, vol. 7398, pp. 68–79, series Title: Lecture Notes in Computer Science. [Online]. Available: http://link.springer.com/10.1007/978-3-642-34638-5_6

[11] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the eighth symposium on usable privacy and security*, 2012, p. 1–14.

[12] A. Acquisti, H. Heinz, and J. Grossklags, "Uncertainty, ambiguity and privacy," in *4th Annual Workshop on Economics and Information Security (WEIS 2005)*, 04 2005.

[13] C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, and R. Abu-Salma, "Cookie banners, what's the purpose? analyzing cookie banner text through a legal lens," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, ser. WPES '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 187–194. [Online]. Available: https://doi-org.proxy.bnl.lu/10.1145/3463676.3485611

[14] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji, "A methodology for empirical analysis of permission-based security models and its application to android," in *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*. ACM Press, 2010, p. 73. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1866307.1866317

[15] M. Hatamian, J. Serna, K. Rannenberg, and B. Igler, "Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps," in *International Conference on Trust and Privacy in Digital Business*. Springer, 2017, p. 3–18.

[16] G. Bal and K. Rannenberg, "User control mechanisms for privacy protection should go hand in hand with privacy-consequence information: The case of smartphone apps," in *Proceedings of W3C Workshop on Privacy and User-Centric Controls*, 2014, p. 1–5.

[17] Prolific. (2021) Welcome to prolific. [Online]. Available: https://www.prolific.com/

[18] Apptopia. (2021) Worldwide and us download leaders 2021. [Online]. Available: https://blog.apptopia.com/worldwide-and-us-download-leaders-2021

[19] Google. (2021) Google play apps. [Online]. Available: https://play.google.com/store/apps

[20] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side: Privacy dark strategies and privacy dark patterns." *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 4, pp. 237–254, 2016.

[21] A. . D. P. W. Party, "Guidelines on transparency under regulation 2016/679, 17/en wp260 rev.01," Apr 2018, published: Online at. [Online]. Available: https://ec.europa.eu/newsroom/article29/redirection/document/51025

[22] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, "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*. ACM, Apr 2015, p. 787–796. [Online]. Available: https://dl.acm.org/doi/10.1145/2702123.2702210

[23] V. Distler, T. Gutfleisch, C. Lallemand, G. Lenzini, and V. Koenig, "Complex, but in a good way? how to represent encryption to non-experts through text and visuals – evidence from expert co-creation and a vignette experiment," *Computers in Human Behavior Reports*, vol. 5, p. 100161, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2451958821001093

[24] C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, and R. Abu-Salma, "Cookie banners, what's the purpose?: Analyzing cookie banner text through a legal lens," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. ACM, Nov 2021, p. 187–194. [Online]. Available: https://dl.acm.org/doi/10.1145/3463676.3485611

[25] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, p. 1–17.

[26] S. Barth and M. D. de Jong, "The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review," *Telematics and Informatics*, vol. 34, no. 7, p. 1038–1058, Nov 2017.

[27] V. Distler, C. Lallemand, and V. Koenig, "How acceptable is this? how user experience factors can broaden our understanding of the acceptance of privacy trade-offs," *Computers in Human Behavior*, vol. 106, p. 106227, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563219304467

[28] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, "Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, 2016, pp. 27–41. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu

[29] D. Smullen, Y. Feng, S. Aerin Zhang, and N. Sadeh, "The Best of Both Worlds: Mitigating Trade-offs Between Accuracy and User Burden in Capturing Mobile App Privacy Preferences," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 195–215, Jan. 2020. [Online]. Available: https://www.sciendo.com/article/10.2478/popets-2020-0011

[30] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review*, vol. 79, no. 1, p. 119–158, 2004.

[31] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "Pscout: analyzing the android permission specification," in *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*. ACM Press, 2012, p. 217. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2382196.2382222

[32] N. Momen, T. Pulls, L. Fritsch, and S. Lindskog, "How much privilege does an app need? Investigating resource usage of android apps (short paper)," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, Aug 2017, p. 268–2685.

[33] N. Momen and L. Fritsch, *App-generated digital identities extracted through android permission-based data access-a survey of app privacy*, ser. Gesellschaft für Informatik. Gesellschaft für Informatik eV, 2020, p. 15–28.

[34] B. Bian, X. Ma, and H. Tang, "The supply and demand for data privacy: Evidence from mobile apps," *Available at SSRN*, 2021.

[35] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos, "Permission evolution in the android ecosystem," in *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12*. ACM Press, 2012, p. 31. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2420950.2420956

[36] K. Marky, A. Gutmann, P. Rack, and M. Volkamer, "Privacy friendly apps-making developers aware of privacy violations." in *1st International Workshop on Innovations in Mobile Privacy and Security, IMPS 2016, co-located with the International Symposium on Engineering Secure Software and Systems (ESSoS 2016)*, 2016, p. 46–48.

[37] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security APIs," *IEEE Security & Privacy*, vol. 14, no. 5, p. 40–46, 2016.

[38] T. Book, A. Pridgen, and D. S. Wallach, "Longitudinal analysis of android ad library permissions," *arXiv preprint arXiv:1303.0857*, 2013.

[39] foetusofexcellence on Reddit. (2018) Non-compliance of GDPR law with android permissions system : Android. [Online]. Available: https://www.reddit.com/r/Android/comments/8708vq/noncompliance_of_gdpr_law_with_android/

[40] A. Claesson and T. E. Bjørstad, "Out of control – a review of data sharing by popular mobile apps," Jan 2020. [Online]. Available: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf

[41] M. Hatamian, "Engineering privacy in smartphone apps: A technical guideline catalog for app developers," *IEEE Access*, vol. 8, p. 35429–35445, 2020.

[42] K. Kollnig, R. Binns, M. Van Kleek, U. Lyngs, J. Zhao, C. Tinsman, and N. Shadbolt, "Before and after GDPR: tracking in mobile apps," *Internet Policy Review*, vol. 10, no. 4, Dec 2021, arXiv: 2112.11117. [Online]. Available: http://arxiv.org/abs/2112.11117

[43] Apple. (2021) The apps you love.from a place you can trust. [Online]. Available: https://www.apple.com/app-store/

[44] H. A. Simon, "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics*, vol. 69, no. 1, pp. 99–118, 02 1955. [Online]. Available: https://doi.org/10.2307/1884852