Privacy-Aware Decision Making: The Effect of Privacy Nudges on Privacy Awareness and the Monetary Assessment of Personal Information

Vera Schmitt[1], James Nicholson[2], Sebastian Möller[3]
Quality and Usability Lab, Technische Universität Berlin, Berlin, Germany[1,3]
Department of Computer and Information Sciences, Northumbria University, Newcastle, United Kingdom[2]

***Abstract*—Nowadays, smartphones are equipped with various sensors collecting a huge amount of sensitive personal information about their users. However, for smartphone users, it remains hidden, and sensitive information is accessed by used applications and data requesters. Moreover, governmental institutions have no means to verify if applications requesting sensitive information are compliant with the General Data Protection Directive (GDPR), as it is infeasible to check the technical details and data requested by applications that are on the market. Thus, this research aims to shed light on the compliance analysis of applications with the GDPR. Therefore, a multidimensional analysis is applied to analyzing the permission requests of applications and empirically test if the information provided about potentially dangerous permissions influences the privacy awareness and their willingness to pay or sell personal data of users. The use case of Google Maps has been chosen to examine privacy awareness and the monetary assessment of data in a concrete scenario. The information about the multidimensional analysis of the permission requests of Google Maps and the privacy consent form is used to design privacy nudges to inform users about potentially harmful permission requests that are not in line with the GDPR. The privacy nudges are evaluated in two crowdsourcing experiments with overall 426 participants, showing that information about harmful data collection practices increases privacy awareness and also the willingness to pay for the protection of personal data.**

***Keywords*—Privacy protection; privacy policy analysis; GDPR; willingness to pay, privacy awareness**

I. Introduction

Smartphone applications (apps) are nowadays considered an indispensable part of our lives due to the wide range of services and utilities they provide, such as digital contact tracing, public transport, navigation, education, and many others. Many business strategies depend on continuous data collection to earn revenue by leveraging personal data. Firms such as Google and Facebook require users to continuously provide personal information as a precondition for accessing their services. This enables them to profit through detailed targeting and advertising [1], [2], [3]. Additionally, a growing number of firms and institutions are engaging in the exchange of users' personal data, often navigating ambiguous legal areas while handling the earnings from these transactions [4]. However, the continuous data sharing from many applications on smartphones, which monitor, collect, and transmit data about the daily lifestyle of their owners, can reveal sensitive information, such as camera feeds, messages, moving patterns, voice commands, physiological data, and much more [5]. However, it is not a trivial task for the users to verify whether applications might induce a potential privacy threat. Due to the mobile nature and use of wireless communication protocols, applications are able to access, use, and transmit sensitive information to remote servers without user interactions [6]. Often it remains unclear to users what data is being transferred and how to turn continuous data sharing off. The complexity and length of privacy consent forms and the lack of technical knowledge are obstacles hindering the user from making privacy-conscious decisions [7]. Cases of mishandling and misuse of personal information have heightened government awareness about the necessity of creating regulatory structures to protect personal data on the internet. The General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) exemplify this, setting standard data privacy regulations and enhancing individuals' authority over their personal information [8]. While the industry has attributed economic value to personal data, utilizing it across various businesses from social media and advertising to the enhancement of personalized products, the assessment of the monetary worth of the data from the viewpoint of the user remains a largely unexplored area of study [8], [9], [10], [3], [11]. To assess the monetary value of specific goods from the users' perspective, the metrics employed are the Willingness to Pay (WTP) for a particular item and the Willingness to Accept (WTA) compensation in exchange for that same item [11].

Therefore, a detailed analysis is presented in the following to shed light on regulatory compliance issues, inappropriate design and development strategies, and severe privacy issues applications might have. The analysis follows a similar structure as proposed in [6], [12] to evaluate potential GDPR compliance issues of a sensitive domain such as location tracking applications. Moreover, different privacy nudges are designed based on the results of a multistage analysis to examine effective means of informing users about potentially harmful privacy practices. Additionally, we examine whether users have higher WTP and WTA ratings to protect their personal information on a monthly basis when presented with information about what data is collected continuously.

Thus, this analysis aims to answer the following research questions:
RQ1: Do privacy nudges about potentially harmful privacy practices increase the awareness of users?
RQ2: Do information about potentially harmful permission requests change users' privacy awareness and willingness to

pay for the protection of personal data?

Our analysis comprises two main phases. The *Phase I* consists of three steps: (1) we analyze the apps' permission requests within their Android manifests to provide an overview of the most prominent permission requests and their potential privacy and security implications; (2) we inspect statements made by app providers in their privacy policies with respect to the fulfillment of legal requirements enforced by the data protection legislation; and (3) we explores the apps' run-time permission accesses to investigate if apps access any sensitive resources without users being aware of it. In *Phase II* the results from *Phase I* are used to design privacy nudges to be incorporated in crowdsourcing studies. The privacy nudges are examined if they increase privacy awareness and facilitate privacy-aware decision-making. In sum, the contributions of this work are the following: (1) detailed compliance analysis of privacy policies of surveillance and behavior analysis of location tracking apps' permission access patterns at run-time; (2) Design of privacy nudges based on the findings to inform users about potentially harmful permission requests; (3) and evaluation of whether information about potentially harmful permission requests not in line with the GDPR influence users' privacy awareness and monetary assessment of their personal data. This paper is organized as follows: first, an overview of related work is given in Section II. In Section III the privacy nudges are described which are designed based on the results from the GDPR compliance analysis. In Section IV the methodological background for privacy awareness, privacy nudges, WTP and WTA, and the experimental workflow are described and Section V empirically examines if information about potentially harmful permission requests changes the privacy awareness and monetary assessment of personal data. Finally, Section VI discusses the multidimensional analysis of applications GDPR compliance, privacy nudges, and their influence on privacy awareness and monetary assessment and concludes this paper and indicates future research directions.

II. Related Work

After the GDPR was enforced in 2018, it can be expected that service providers and app developers have adapted to the GDPR by either improving their privacy statements or through the improvement of software design and consideration of GDPR principles in the development phase [13]. The empirical verification, if principles of the GDPR, such as *transparency*, *data minimization*, or *data protection* have been considered in the design of services and applications has not yet been enforced by the European Commission or any other official authority. Previous studies have shown that there is still a vast amount of data requested from users of mobile applications, where there is no comprehensive approach for users to verify if the app's privacy consent form is compliant with the GDPR requirements and also if the app itself does comply with the own privacy consent form and the GDPR alike [14], [15]. Therefore, the assessment of privacy risks associated with various applications suffers from a general shortage of empirical evidence [16], [13]. Some approaches have been proposed for assessing the privacy of apps by monitoring sensitive permissions, such as location information, contacts, of camera access [17], [18]. Other approaches such as FAIR [19] propose a privacy risk assessment of Android apps by monitoring the behavior with regards to monitoring the access to sensitive personal information. Further research has been done by developing an automatic framework, called *Trust4App* to assess the trustworthiness of mobile applications [20]. While these approaches focus on the risk assessment of mobile applications, there are only a few approaches that integrate the privacy policies in their assessment, such as [6]. Not much information can be found in the literature, which reveals a comprehensive analysis concerning the GDPR compliance of mobile applications [13]. Therefore, more research needs to be done to shed more light on transparently verifying GDPR compliance of online services and mobile applications, especially where sensitive data is shared continuously. Especially in context-sensitive digital ecosystems, there is a high risk of privacy violations [21]. Many business models are built on the ongoing acquisition of data to profit from the personal information of individuals. Major technology firms, like Google and Facebook, necessitate the constant sharing of personal data by users in return for their services, deriving revenue through targeted advertising and profiling techniques [1], [2]. The GDPR is designed to increase control over personal data shared online, yet it frequently results in intricate rules and settings that might not align well with the specific needs of individual users. However, users typically show limited capacity in evaluating the pros and cons of data exchange scenarios and might consent to enduring privacy risks for immediate benefits [22]. Moreover, a fundamental issue concerning privacy regulations and settings is whether users place importance on and value their privacy and are aware of potentially harmful data-sharing practices [8].

Previous studies highlight usability issues in mobile app permissions, impacting user comprehension and control, leading to inadequate privacy risk assessments and decision-making. Research indicates a general deficit in privacy literacy and awareness among mobile users, complicating their ability to navigate privacy concerns effectively. Despite some flexibility in iOS permission settings, both Android and iOS platforms fall short in offering clear explanations about permission functionalities, data access, and usage scope, thus obscuring the implications of permission settings for personal data security [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [15], [33]. Recent research has focused on enhancing privacy permission interfaces, aiming to better inform user decision-making. These interfaces have been refined to highlight apps' potentially invasive privacy practices and incorporate warning indicators, as well as clearly listing the data apps collect and do not collect [23], [26], [25]. Studies, such as the one by Kelley et al. [34], demonstrate that such interfaces can significantly raise users' awareness of privacy risks, leading to more informed choices. The emphasis has largely been on delivering explicit information regarding data usage, thereby fostering transparent user engagement. Additionally, there's a growing trend towards employing soft paternalistic strategies like privacy nudges to subtly guide users towards safer privacy practices without compromising their autonomy [25], [33], [35], [36]. Efforts in research have aimed at creating privacy nudges tailored to the permission requests of diverse apps, yielding mixed results. These variations are attributed to factors like the context of data sharing [35], the type of device used [30], and the app's functional domain [37]. Notably, the impact of privacy nudges seems negligible on users' awareness of video-call and messenger applications,

yet significant for weather or fitness apps [38]. Additionally, some nudges are designed to enhance user understanding by comparing the number of permissions an app requests against similar apps, thereby aiding users in grasping the implications of the permissions sought [36], [39], [37], [38], [23]. However, the relation between enhanced privacy awareness through privacy nudges and the relation to monetary assessment of personal information has not been systematically covered by the previous literature.

Therefore, this analysis aims to shed light on privacy assessment concerning personal data sharing and GDPR compliance of apps with access to very sensitive data. Previous research has shown that privacy nudges have the potential to support privacy-aware decision-making of users [40], [7], [36], [41], [42], [37]. Thus, the GDPR compliance analysis is used to design privacy nudges to support the decision-making process of users. Different types of privacy nudges are then empirically examined in two user experiments concerning privacy awareness and their influence on the monetary assessment of privacy.

III. Analysis Design and Methodology

Assessing the privacy risks associated with different smartphone apps is challenging for users. Due to their dependence on wireless communication, these apps can independently access, use, and send sensitive information to remote servers [6]. The details of how data is transferred are usually not clear to the user, including the methods to stop ongoing data sharing. Furthermore, the complexity and excessive length of privacy policies, coupled with a lack of technical knowledge, hinder users from making knowledgeable choices about their privacy [7]. Therefore, privacy nudges or framing techniques are frequently employed to alert users to privacy dangers. For the following analysis, different privacy nudges have been designed to examine their influence on privacy awareness and the monetary assessment of personal data. Hereby, the procedure of analyzing permission requests, the permission manifest, and the privacy policy of applications is followed which has been introduced by [3], [43], [6], [25].

In the analysis that follows, two kinds of privacy nudges are utilized to demonstrate the effect of informational and visual nudges on both privacy on privacy awareness and monetary assessment. This research on privacy awareness includes an in-depth examination designed to emphasize the difficulties associated with adhering to regulations like the GDPR, limitations in design and development approaches, and critical privacy concerns that could affect surveillance applications. Often, users remain unaware of the specific data being shared and the methods to stop continuous data transmission. The complexity and lengthiness of privacy consent forms, along with a lack of technical knowledge, create obstacles that hinder individuals from making educated choices about their privacy [7]. Past research has demonstrated that users often express surprise and discomfort upon learning the extent of information collected by smartphone applications [35], [11]. Therefore, the purpose of privacy nudges and framing effects is to aid users in making decisions that are aware of privacy concerns and to highlight the potential risks associated with sharing sensitive personal information.

The examination of legal compliance is organized based on the proposed framework introduced in [6], [43], [44], specifically designed to evaluate the GDPR conformity of widely used and renowned applications. The analysis of technical and legal compliance is divided into three primary phases. In *Phase I*, the analysis focuses on the permissions requested in the applications' Android manifests, providing an overview of the most critical permission requests and their potential impacts on privacy and security. *Phase II* assesses the claims made by app developers in their privacy policies about adherence to data protection regulations. Finally, *Phase III* investigates the runtime permissions used by the apps to ascertain if they access sensitive information without the users' knowledge. Drawing on the insights from the three stages of the analysis, the outcomes have been leveraged to create visual and informational nudges for some well-recognized applications. The privacy nudges were developed using the insights from the analysis across all three phases. These nudges integrate design principles from existing studies [45], [37] by incorporating clear, short, and relevant information summarized from the analysis of permission requests and privacy policies of chosen applications. The purpose of the nudges is to decrease *information asymmetry* and *cognitive load*, helping users to swiftly evaluate which information an application can access and whether this complies with legal requirements in the EU.

A. Analyzing Permission Requests and Privacy Policy

1) Permission requests analysis: The device's resources can be accessed by apps through permissions in Android. Consent from users is sometimes required depending on the source type. Android defines three types of permissions [12]: *install-time*, *run-time*, and *special*. *Install-time* permissions are automatically granted to an app when the user installs it. Android defines two sub-types of install-time permissions, including *normal* and *signature* permissions. *Normal* permissions allow access to resources that are considered low-risk, and they are granted during the installation of any apps requesting them. Only when the app that aims to access specific permissions is signed by the same certificate as the app that defines the permission, so-called *signature* level permissions are granted at install-time [12]. In fact, the system grants permission to one app at install time only if the app is requesting signature permission that another app has defined and if they are both signed by the same developer.

The *run-time* permissions, also known as dangerous permissions, grant access to resources that are considered to be high-risk [12]. In such cases, users are asked to explicitly grant permission to these requests. *Special* permissions correspond to particular app operations. Only the platform and the Original Equipment Manufacturer (OEM) can define special permissions. Every app has an `AndroidManifest.xml` file that contains information about that particular app (e.g., its name, author, icon, and description) and permissions that grant access to data such as location, SMS messages, or camera on the device.

2) Privacy policy analysis: For the privacy policy analysis, we explore the compliance of Google Maps with fundamental legal requirements. For this, we rely on the EU GDPR benchmarking conducted in [46] that resulted in the identification of 12 privacy policy principles.

(a) Baseline nudge control group

(b) Information nudge (experimental group

(c) Visual nudge experimental group

Fig. 1. Example of privacy nudges designed containing the plain nudge for the control group in Fig. 1(a), the information nudge in Fig. 1(b), and the visual nudge containing a classification of privacy nudges in the traffic light metaphor. The privacy nudges are designed based on the permission request analysis.

The privacy policy of an app is a statement or a legal document that gives information about the ways an app provider collects, uses, discloses, and manages users' data. By law, data collectors (including app providers) are required to be transparent about their data collection, sharing, and processing practices and specify how they comply with legal principles [46]. Based on keyword- and semantic-based search techniques, a data protection expert went through each privacy policy to analyze the compliance of these apps concerning the following principles which are summarized and used similarly in [12] and [6].

a) Data collection: The legal foundation is defined in Art. 5 (1) GDPR, which states the general principles of processing personal data. Also, Art. 6 in the GDPR indicates when processing is lawful, which includes when consent is given by a user of a service or application. Moreover, both articles address the question of when consent is necessary for the performance of a contract or compliance with legal obligations when the vital interests of the user or another natural person need to be protected, and when a task is carried out for the public or legitimate interest pursued by the controller or by a third party. Nevertheless, this applies only if such interests do not conflict with fundamental rights and also the freedom of a user. Hereby, e.g. advertising is not classified as a necessary interest and thus, needs to be analyzed based on other legal foundations [47], [12], [6].

b) Children protection: Personal data which is related to children needs to be treated with special attention. As defined in Rec. 38 in the GDPR children "may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data". Service providers need to provide information in a very clear and comprehensive language so that also children are able to understand it easily (Rec. 58 GDPR). Moreover, the processing of children's data is strictly regulated and data can only be processed on a lawful basis if the child is at least 16 years old (Art. 8 GDPR). In case the child is younger, processing of children's data is only lawful when a parent or also legal guardian has given consent [12], [6].

c) Third-Party sharing: Third-party tracking is one of the most common approaches to collecting personal information through various apps. Hereby, it is legally regulated by Art. 13 in the GDPR, where it is defined that the recipients or categories of recipients of personal information must be declared to the users [12], [6].

d) Third-Country sharing: The legal requirements for third-country sharing are described in *Chapter 5* in the GDPR. Hereby, personal data can only be transferred to other countries when a similar level of protection is enforced. This means that the protection of personal data travels also across borders when personal data is transferred to servers outside of the EU. Furthermore, the privacy policy must state its procedures when personal data is shared with other countries outside of the EU [12], [6].

e) Data protection: Technical and organizational measures to ensure the appropriate security of personal information must be ensured by the data controller as stated in Art. 32 in the GDPR. Especially in the smartphone ecosystem, this has major implications, as they are usually linked to huge amounts of data transfer. Moreover, the components of data protection are closely interrelated with privacy-by-design principles [48], [12], [6].

f) Data retention: The principle of data minimization and storage limitation is described in Art. 13 (2), and 14 (2) in the GDPR. Hereby, the data controller has the obligation to inform users how long personal data is retained. Especially for "the right to be forgotten" (Art. 17) this is crucial as personal data can only be stored for a limited time [12], [6].

g) User's control: Further user rights are defined in *Chapter 3* of the GDPR, which contains the right to information and access to personal data; the right to rectification;

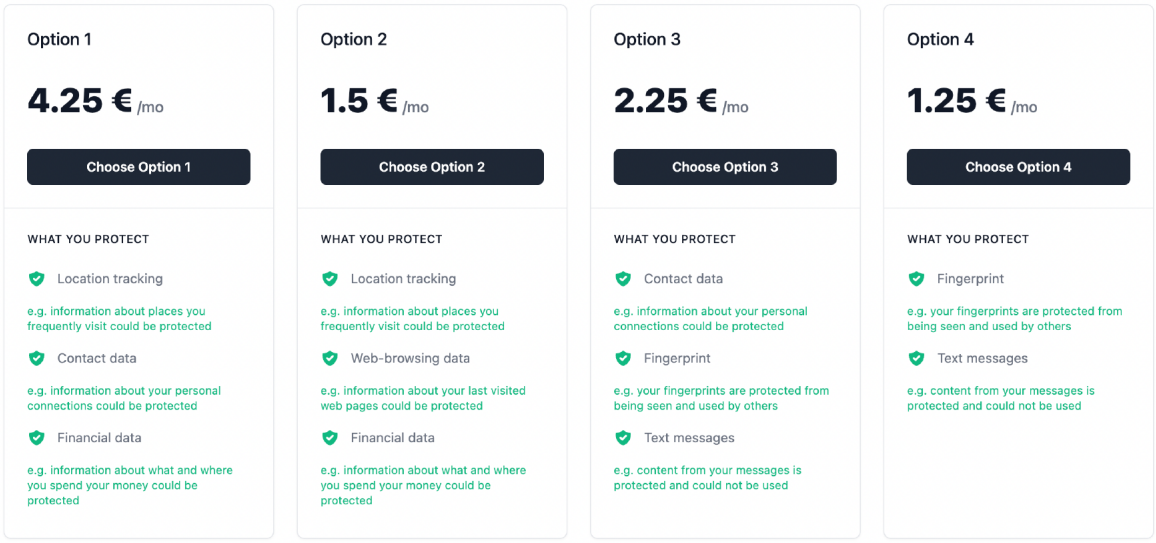

Fig. 2. Privacy nudges for the WTP scenario, where participants are asked to indicate the price preferences they are willing to pay for protecting their personal information.

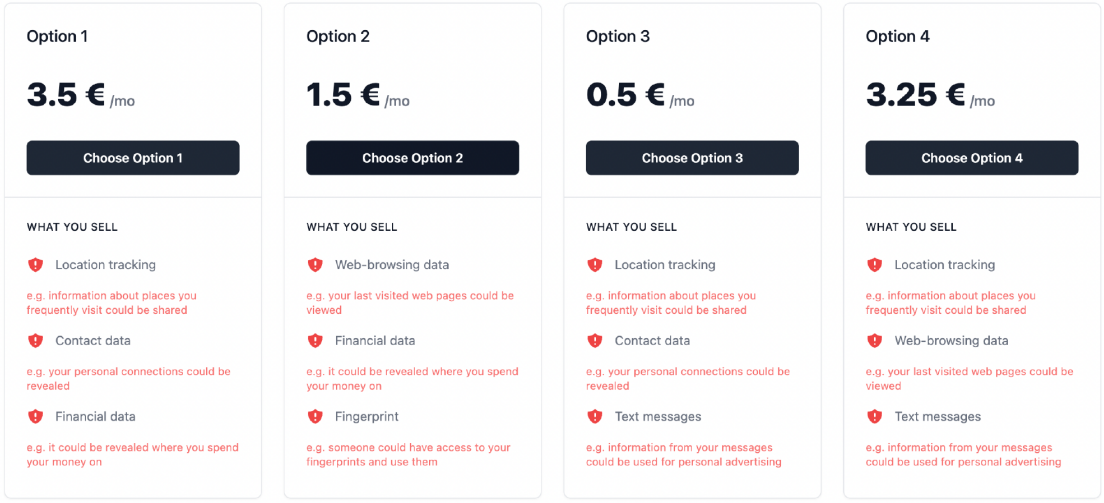

Fig. 3. Privacy nudges for the WTA scenario, where participants are asked to indicate the price preferences they are willing to accept and exchange for their personal information.

the right to erasure; the right to restriction of processing; the right to data portability; and the right to object and automated individual decision-making. IN Art. 13 (2), and 14 (2) it is defined that service or app providers are required to provide these rights to users to ensure fair and transparent data processing [12], [6].

h) Privacy policy changes: In Art. 12 of the GDPR app or service providers have the obligation to inform users about privacy policy changes in a transparent and comprehensive way. This should further ensure lawful, fair, and transparent processing of personal information [12], [6].

i) Privacy breach notification: In Art. 34 of the GDPR it is defined that in case a data breach occurs that might result in a risk to the rights and freedoms of users, the data controller or service provider must inform the users asap. Also, the information that needs to be provided in the data breach notification is regulated by this article. Thus, a data breach notification must name the data protection officer and mention the likely consequences of the data breach. Furthermore, measures must be mentioned how to mitigate the effects of the data breach. Moreover, the supervisory authority must be informed not later than 72 hours after the detection of the data breach [12], [6].

j) App-Focused: Often, the privacy policy is not exclusively formulated for only one application, but shared among multiple services that are provided by the same data controller or app developer [49]. This principle is incorporated in the principle of lawfulness, fairness, and transparency [12], [6].

k) Purpose specification: Data collection must be specified by service providers or data controllers according to Art.

13 (1c), and 14 (1c) in the GDPR. The principle of purpose limitation is relevant to preventing the exploitation of personal data for other use cases. It is also closely related to the data collection principle but refers rather to a clear statement and explanation of data collection purposes [12], [6].

l) Contact information: Users have the right to be informed about the identity of service providers and data controllers, which includes the name of service providers, also legal representation, legal status, and postal address (Art. 13 (1a), and 14 (1a) in the GDPR). The principle of contact information is closely interrelated with the principle of lawfulness, fairness, and transparency. Providing such information is relevant to give users the option to also file a formal compliance [12], [6].

We conducted a user study to better understand how users behave when informed of these digressions by apps. Specifically, we selected the Google Maps app due to its popularity (> 500 Mio downloads) and has access to sensitive information.

IV. Empirical Examination of Permission Requests in Terms of Privacy Nudges

The analysis of permission requests can serve as an automatic tool to monitor whether applications available in the app store are compliant with GDPR at a technical level. While this kind of monitoring has not been established yet, it offers a promising strategy to assist developers in adhering to GDPR guidelines and inform users if the respective applications are privacy-preserving.

A. Nudge Design and Monetary Valuation

According to Almuhimedi et al. [36], users are mostly unaware of data collection practices, and when information is provided users are motivated to adjust their app settings [36]. According to Shih et al. [50], the purpose for data access was the main factor affecting the users' choices, e.g., if the purpose is vaguely formulated, participants became privacy-aware and were less willing to disclose information. The traffic light metaphor thus serves as a useful tool for users to efficiently oversee valid and invalid permission requests in compliance with GDPR [51]. To investigate the impact of information about permission requests and access to sensitive data on privacy awareness, the aforementioned procedure is applied to track permission requests from the popular Google Maps app. Google Maps was selected for its widespread usage, in contrast to more niche applications like specific security camera apps. The permission requests of the Google Maps app were monitored for one week, and the privacy policy was analyzed to classify these requests according to the traffic light metaphor as either valid (green), critical (orange) or invalid (red).

In Fig. 1, the privacy nudges are displayed for the example of Google Maps. Hereby, the nudge for the control group is displayed in Fig. 1 A providing only plain details on the types of information collected while using Google Maps. In a crowdsourced study, these nudges were evaluated by randomly allocating 100 participants to an experimental group and another 100 participants to a control group. The study is designed to investigate whether privacy nudges increase privacy awareness among the experimental group. Thus, questions measuring privacy awareness were included in the survey both before and after the presentation of the privacy nudges. Another approach has been chosen, where information about potential risks of sharing information or benefits when protecting personal data is directly incorporated in the monetary assessment of the experiment. Hereby, the privacy nudges are positively associated by using the *green* color of traffic light metaphor for the WTP scenario, where participants are requested to indicate how much they would pay for protecting the personal data collected by Google Maps as displayed in Fig. 2. For the WTA scenario, the privacy nudges use the *red* color to indicate the potential risk when sharing the information with Google Maps as displayed in Fig. 3. For the second privacy nudge design approach another crowdsourcing study was conducted, where 112 participants were randomly assigned to the control group and 114 to the experimental group. Additionally, the WTP and WTA questionnaire was customized for the privacy nudge scenarios. Participants were queried about their readiness to pay for data protection to avoid sharing the shown information with the data requester, and conversely, how much compensation they would require to allow their data, collected by the applications used in the experiment, to be shared. For measuring the WTP and WTA discrete choice surveys have been incorporated to measure the individual monetary value preferences following the study design of [8] and [9].

Moreover, privacy awareness is assessed through five dimensions derived from prior studies [52], including (1) the perceived sensitivity of personal information, (2) the awareness of being surveilled, (3) the feeling of intrusion, (4) the sense of control over one's personal information, and (5) the perception of secondary use of personal information. Responses to these questions are captured on a 7-point Likert Scale, where 1 signifies "strongly disagree" and 7 represents "strongly agree."

B. Experiment Workflow

A crowdsourcing experiment was prepared to test the influence of privacy nudges on privacy awareness and the monetary assessment of privacy. To empirically assess whether privacy nudges affect users' privacy awareness, we adopted a privacy awareness questionnaire from prior research [29], [53], [40], including also items about privacy concerns, and perceived control as subdimensions for privacy awareness. Moreover, the influence of privacy nudges is further examined on WTP and WTA for the protection of personal data collected by the Google Maps app. WTP and WTA are measured by using the Discrete Choice Experimental design method [9] particularly useful for assessing the impact on non-market goods, for which value cannot be determined using revealed preference methods that depend on observing actual behavioral choices. Here the participants can rate how much they would pay on a monthly basis for using the Google Maps app, but not sharing their personal information. Both experiments contain three survey parts and two experimental parts. First, the participants are asked to fill out a questionnaire about their privacy awareness. Afterward, the participants were randomly assigned to the experimental or control group. The use case of the Google Maps app is explained to the participants. They receive the respective privacy nudges depending on the control or experimental group. Afterward, the participants are required

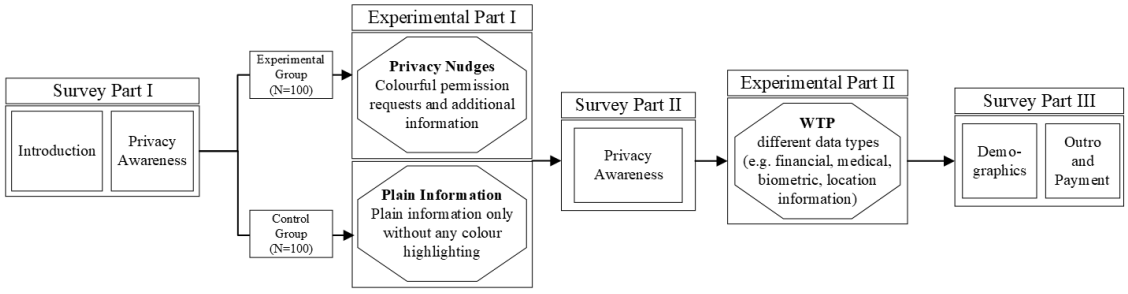

Fig. 4. Visual depiction of the workflow of the human evaluation experiment.

to fill out the privacy awareness questionnaire again, before starting with the monetary evaluation, if they would be willing to pay or accept money for their personal data related to the privacy nudges for the Google Maps app use case. In Fig. 4, a visual depiction of the experimental workflow is shown. Overall, 426 participants took part in the two experiments where the participants were randomly assigned to either the control or experimental group. For the first experiment containing the information and visual nudge the average age of the participants was 33.5, 81 participants were male, 118 female, and 1 reported to be of *other* gender. For the second experiment containing the privacy nudges incorporated in the monetary valuation the average age was 32.4, 104 were male, 106 were female, and six participants reported *other* gender.

V. Results

The two experiments with 426 participants have been conducted through the crowdsourcing platform Crowdee[1], to examine the influence of the privacy nudges for German participants who use the Google Maps app[2]. In the following, the results from the two experiments are described in more detail.

A. First Experiment

Fig. 5 illustrates the changes in awareness ratings for the experimental group, comparing their responses before and after being exposed to the privacy nudges. A slight increase in privacy awareness can be identified after the nudge has been presented (mean 4.86) in comparison to the privacy assessment before the nudge (mean 4.74). After the presentation of the nudge in the first experiment, a modest rise in privacy awareness is observed, with the mean score increasing to 4.86 from a pre-nudge mean privacy awareness of 4.74. Nonetheless, upon performing a Wilcoxon signed-rank test to compare the two related samples, the increase in privacy awareness was found to be statistically insignificant (W=2390.5, *p-value* = .76)[3]. In the comparison of the WTP and WTA between the control and experimental group, the experimental group showed a marginally higher WTP (mean .41) relative to the control

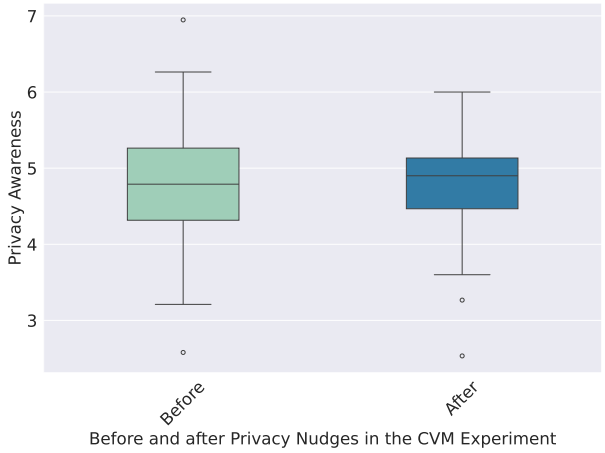

Fig. 5. Comparison of PA for the visual and information privacy nudges (W=2390.5, *p-value* = .76).

group (mean .38), although the difference is not statistically significant.

Remarkably, the control group exhibited a higher willingness to accept after exposure to the privacy nudges, with a mean of .91, compared to the experimental group, which had a mean of .84. Yet, when a Mann-Whitney U test was applied for the between-group comparison, the differences were found to be not statistically significant (U = 4573, *p-value*= .19). The findings from the first experiment including the information and visual privacy nudges indicate a minor trend towards heightened privacy awareness and a greater WTP for personal data protection. Nonetheless, these results do not allow for final conclusions due to the absence of significant differences, which could be attributed to random variations in the data. Additionally, since the privacy nudges were introduced prior to the monetary valuation of data types, participants noted difficulties in recalling the details presented in the privacy nudges.

B. Second Experiment

In the second experiment, the information is deliberately concise to avoid *information overload*, drawing upon the analysis of permission requests described earlier. In relation to the approach of the first study, the visual nudge employs the *traffic light metaphor* to underscore the risks associated with information sharing. In the WTA scenario, where participants

[1]https://www.crowdee.com/

[2]The participants received 6€ for on average participating 15 minutes in the experiment. General information about the study was given, but the experimental group and control group setup has not been mentioned beforehand.

[3]All *p-values* were corrected using the Benjamini-Hochberg procedure to mitigate the risk of *alpha* accumulation errors.

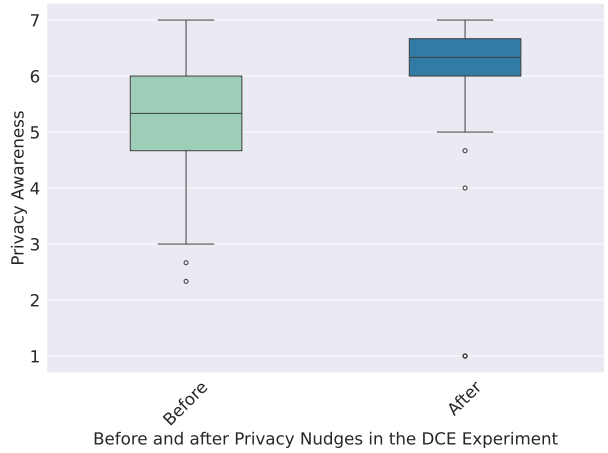

Fig. 6. Comparison of PA for the privacy nudges used DCE test paradigm (W=3095.5, *p-value*=< .01, Cohen´s D = .76).

are asked to set a price for selling their information to a data requester, the color *red* is utilized, whereas *green* is applied in the WTP scenario to highlight the benefits of safeguarding specific types of information, making these advantages clearer to the participants (see Fig. 3 and Fig. 2). A comparison of privacy awareness (PA) assessments before and after the presentation of privacy nudges (see Fig. 6) reveals a significant increase in PA (W=3095.5, *p-value*< .01, Cohen's D = .76) for the experimental group post-nudges (mean = 6.1) compared to pre-nudges (mean = 5.2). In analyzing the impact of privacy nudges on the monetary valuation, specifically WTP and WTA, noticeable differences emerge. A Mann Whitney-U test comparing WTP shows significant differences (U= 52662, *p-value*=.01, Cohen's D = .44), with the WTP valuation significantly higher in the experimental group (mean = .40) than in the control group (mean = .36). Similarly, significant disparities are found in WTA between the experimental and control groups (U= 55055, *p-value*< .01, Cohen's D = .42), with the experimental group's WTA valuation also significantly higher (mean = .45) compared to the control group (mean = .42). The results from the modified privacy nudge design in the second study suggest a substantial impact (Cohen's D = .76) on privacy awareness (PA) and notably elevate the WTP and WTA evaluations relative to the control group. Therefore, when potential risks associated with selling personal data are clearly communicated and visually emphasized, participants tend to assign higher WTA values. Likewise, when information on the advantages of safeguarding specific data types is provided, participants demonstrate a significantly increased willingness to pay for the protection of their personal information.

Overall, the results from the user study show that when informed about valid, critical, and invalid permission requests according to the GDPR, users have a higher privacy awareness and are willing to pay to protect their personal information. We also highlight that future research can further explore the users' privacy awareness aspects concerning the integration of different types of privacy nudges into people's daily lives and activities. Users may not be fully aware of the negative consequences that such apps could potentially have on their privacy. We also note that the developers and providers of these apps should carefully address privacy threats discussed in this paper and make sure their app design and the development life cycle respect privacy by design.

VI. Discussion and Conclusion

In this paper, we first presented a multidimensional analysis to showcase potential GDPR compliance issues of Google Maps. In particular, we focused on the system permission requests of Google Maps for Android, their privacy policies, and adherence to existing regulations defined in the GDPR. Finally, we analyzed the run-time permission requests to identify potential privacy and security issues associated with this application. The analysis shows that this app accesses sensitive data from the users' devices while also embedding trackers to transfer this sensitive data to external servers. The findings show that further mechanisms are necessary to enforce data protection regulations, such as the GDPR. Secondly, we evaluated in an experiment if information about the requested permissions and the potential infringements of personal data protection outlined in the GDPR influence users' privacy awareness and WTP and WTA for protecting personal information. We found that, when users are presented with more information about potentially harmful permission requests, they show significantly higher privacy awareness, in comparison to the control group, not receiving detailed information about potentially harmful permission requests. Furthermore, when presented with visual and information nudges no significant differences have been observed for protecting personal information. When integrating the privacy nudges in the experimental setup when examining the monetary assessment of personal data in comparison to showing privacy nudges beforehand, significant differences can be observed between the privacy awareness before and after the privacy nudges are displayed. Moreover, the WTP and WTA ratings also significantly increased for the experimental group in the second experiment, indicating that privacy-aware decision-making is facilitated when the information is incorporated directly into the decision-making process, and not beforehand.

Overall, the findings of the permission request analysis of the first part, and the human evaluation of privacy nudges designed to empirically evaluate the permission request analysis show that procedures need to be developed to more closely monitor applications not only in the legal domain but also through technical analysis, e.g. analyzing permission requests and embedded trackers. Thus, an approach to automatize the analysis of technical dimensions is necessary, to enable the enforcement of data protection regulations also on a technical level and detect possible pitfalls and areas where adjustment or further clarification of the regulation is necessary.

References

[1] Y. Tang and L. Wang, "How chinese web users value their personal information: An empirical study on wechat users," *Psychology Research and Behavior Management*, vol. 14, p. 987, 2021.

[2] C. I. Jones and C. Tonetti, "Nonrivalry and the economics of data," *American Economic Review*, vol. 110, no. 9, pp. 2819–58, 2020.

[3] V. Schmitt, D. S. Conde, P. Sahitaj, and S. Möller, *What is Your Information Worth? A Systematic Analysis of the Endowment Effect of Different Data Types*. Springer Nature Switzerland, Nov. 2023, p. 223–242. [Online]. Available: http://dx.doi.org/10.1007/978-3-031-47748-5_13

[4] S. Spiekermann, A. Acquisti, R. Böhme, and K.-L. Hui, "The challenges of personal data markets and privacy," *Electronic markets*, vol. 25, no. 2, pp. 161–167, 2015.

[5] J. Bugeja, A. Jacobsson, and P. Davidsson, "Prash: A framework for privacy risk analysis of smart homes," *Sensors*, vol. 21, no. 19, p. 6399, 2021.

[6] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg, "A multilateral privacy impact analysis method for android apps," in *Annual Privacy Forum*. Springer, 2019, pp. 87–106.

[7] S. Human and F. Cech, "A human-centric perspective on digital consenting: The case of gafam," in *Human Centred Intelligent Systems*. Springer, 2021, pp. 139–159.

[8] A. G. Winegar and C. R. Sunstein, "How much is data privacy worth? a preliminary investigation," *Journal of Consumer Policy*, vol. 42, no. 3, pp. 425–440, 2019.

[9] J. Prince and S. Wallsten, "How much is privacy worth around the world and across platforms?" in *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 2020.

[10] V. Schmitt, M. Poikela, and S. Möller, "Willingness to pay for the protection of different data types," 2021.

[11] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of economic Literature*, vol. 54, no. 2, pp. 442–92, 2016.

[12] M. Hatamian, S. Wairimu, N. Momen, and L. Fritsch, "A privacy and security analysis of early-deployed covid-19 contact tracing android apps," *Empirical Software Engineering*, vol. 26, no. 3, pp. 1–51, 2021.

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

[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*, 2010, pp. 73–84.

[15] M. Hatamian, J. Serna, and K. Rannenberg, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets," *Computers & Security*, vol. 83, pp. 332–353, 2019.

[16] L. Fritsch and H. Abie, "Towards a research road map for the management of privacy risks in information systems," *SICHERHEIT 2008-Sicherheit, Schutz und Zuverlassigkeit. Beitrage der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft fur Informatik eV (GI)*, 2008.

[17] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 235–245.

[18] W. Enck, D. Octeau, P. D. McDaniel, and S. Chaudhuri, "A study of android application security." in *USENIX security symposium*, vol. 2, no. 2, 2011.

[19] 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, pp. 3–18.

[20] S. M. Habib, N. Alexopoulos, M. M. Islam, J. Heider, S. Marsh, and M. Müehlhäeuser, "Trust4app: automating trustworthiness assessment of mobile applications," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 124–135.

[21] M. Hatamian, A. Kitkowska, J. Korunovska, and S. Kirrane, "It's shocking!: Analysing the impact and reactions to the a3: Android apps behaviour analyser," in *Data and Applications Security and Privacy XXXII*. Cham: Springer International Publishing, 2018, pp. 198–215.

[22] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE security & privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[23] L. Kraus, I. Wechsung, and S. Möller, "Using statistical information to communicate android permission risks to users," in *2014 Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 2014, pp. 48–55.

[24] M. Hatamian, "Engineering privacy in smartphone apps: A technical guideline catalog for app developers," *IEEE Access*, vol. 8, pp. 35 429–35 445, 2020.

[25] M. Hatamian, S. Wairimu, N. Momen, and L. Fritsch, "A privacy and security analysis of early-deployed covid-19 contact tracing android apps," *Empirical Software Engineering*, vol. 26, no. 3, pp. 1–51, 2021.

[26] R. Li, W. Diao, Z. Li, S. Yang, S. Li, and S. Guo, "Android custom permissions demystified: A comprehensive security evaluation," *IEEE Transactions on Software Engineering*, 2021.

[27] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[28] P. K. Masur, D. Teutsch, and S. Trepte, "Development and validation of the online privacy literacy scale (oplis)," *Diagnostica*, vol. 63, no. 4, pp. 256–268, 2017.

[29] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *IFIP Summer School on the Future of Identity in the Information Society*. Springer, 2008, pp. 226–236.

[30] F. Alrayes and A. Abdelmoty, "Towards location privacy awareness on geo-social networks," in *2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST)*. IEEE, 2016, pp. 105–114.

[31] K. Bergram, V. Bezençon, P. Maingot, T. Gjerlufsen, and A. Holzer, "Digital nudges for privacy awareness: From consent to informed consent?" in *ECIS*, 2020.

[32] J. King, "How come i'm allowing strangers to go through my phone? smartphones and privacy expectations." *Smartphones and Privacy Expectations.(March 15, 2012)*, 2012.

[33] B. Zhang and H. Xu, "Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes," in *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, 2016, pp. 1676–1690.

[34] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2013, pp. 3393–3402.

[35] 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*, 2015, pp. 787–796.

[36] H. Almuhimedi, "Helping smartphone users manage their privacy through nudges," 2017.

[37] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper *et al.*, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–41, 2017.

[38] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[39] T. Kroll and S. Stieglitz, "Digital nudging and privacy: improving decisions about self-disclosure in social networks," *Behaviour & Information Technology*, vol. 40, no. 1, pp. 1–19, 2021.

[40] N. E. Díaz Ferreyra, T. Kroll, E. Aïmeur, S. Stieglitz, and M. Heisel, "Preventative nudges: Introducing risk cues for supporting online self-disclosure decisions," *Information*, vol. 11, no. 8, p. 399, 2020.

[41] J. Chantal, S. Hercberg, W. H. Organization *et al.*, "Development of a new front-of-pack nutrition label in france: the five-colour nutri-score," *Public Health Panorama*, vol. 3, no. 04, pp. 712–725, 2017.

[42] B. Stojkovski, G. Lenzini, and V. Koenig, "" i personally relate it to the traffic light" a user study on security & privacy indicators in a secure email system committed to privacy by default," in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, 2021, pp. 1235–1246.

[43] V. Schmitt, M. Poikela, and S. Möller, "Android permission manager, visual cues, and their effect on privacy awareness and privacy literacy," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3538969.3543790

[44] V. Schmitt, J. Nicholson, and S. Möller, "Is your surveillance camera app watching you? a privacy analysis," in *Science and Information Conference*. Springer, 2023, pp. 1375–1393.

[45] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *The Future of Identity in the Information Society: 4th IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School, Brno, Czech Republic, September 1-7, 2008, Revised Selected Papers 4*. Springer, 2009, pp. 226–236.

[46] M. Hatamian, "Engineering privacy in smartphone apps: A technical guideline catalog for app developers," *IEEE Access*, vol. 8, pp. 35 429–35 445, 2020.

[47] "Privacy and data protection in mobile applications. a study on the app development ecosystem and the technical implementation of GDPR," *ENISA*, 2017.

[48] A. Cavoukian *et al.*, "Privacy by design: The 7 foundational principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, 2009.

[49] A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, "Availability and quality of mobile health app privacy policies," in *American Medical Informatics Association*, 2015, pp. 288–33.

[50] F. Shih, I. Liccardi, and D. Weitzner, "Privacy tipping points in smartphones privacy preferences," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 807–816.

[51] V. Schmitt, M. Poikela, and S. Möller, "Android permission manager, visual cues, and their effect on privacy awareness and privacy literacy," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3538969.3543790

[52] J. Correia and D. Compeau, "Information privacy awareness (ipa): a review of the use, definition and measurement of ipa," 2017.

[53] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and informatics*, vol. 41, pp. 55–69, 2019.