Android Permission Manager, Visual Cues, and their Effect on Privacy Awareness and Privacy Literacy

Vera Schmitt
Quality and Usability Lab, Technische Universität Berlin
Berlin, Germany
vera.schmitt@tu-berlin.de

Maija Poikela
Fraunhofer Institute for Applied and Integrated Security, AISEC
Berlin, Germany
maija.poikela@aisec.fraunhofer.de

Sebastian Möller
Quality and Usability Lab, Technische Universität Berlin, and DFKI
Berlin, Germany
sebastian.moeller@tu-berlin.de

ABSTRACT

Android applications request specific permissions from users during the installations to perform required functionalities by accessing system resources and personal information. Usually, users must approve the permissions requested by applications (apps) during the installation process and before the apps can collect privacy- or security-relevant information. However, recent studies have shown that users are overwhelmed with the information provided in privacy policies and do not understand permission requests and which functionalities are necessary for certain applications. Hereby, the collection of personal information remains mostly hidden, as the task of verifying to which information different apps have access to can be very complicated. Therefore, it is necessary to develop frameworks and apps that enable the user to perform informed decisions about apps' run-time permission access to facilitate the control over sensitive information collected by various apps on smartphones. In this work, we conducted an online study with 70 participants who interacted with a mockup app that enables advanced control over permission requests. The selected permissions are based on the apps' run-time permission access patterns and explanations, and commonly known visual cues are used to facilitate the user's understanding and privacy-conscious decision making. Furthermore, the effects of perceived control over information sharing and privacy awareness are examined in combination with the permission manager mockup app to investigate if increased control over information sharing increases general privacy awareness.

Our results show an interplay between increased control and privacy awareness when explanations and common visual cues are presented to the user. However, the direction of the interplay between increased control and privacy awareness was surprising. Privacy awareness dropped for the experimental group, which received advanced explanations and visual nudges for privacy-conscious decision making. Interestingly privacy awareness significantly increased for the control group, which only received a plain privacy nudge. Therefore, we suggest that increased control over information sharing does not necessarily lead to improved privacy-decision making, and privacy by default might be a more effective design choice.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; **Privacy protections**; *Social aspects of security and privacy*;

KEYWORDS

Permission request analysis, permission manager, privacy awareness, privacy literacy, privacy nudges

ACM Reference Format:
Vera Schmitt, Maija Poikela, and Sebastian Möller. 2022. Android Permission Manager, Visual Cues, and their Effect on Privacy Awareness and Privacy Literacy. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3538969.3543790

1 INTRODUCTION

When we are browsing online, we often make ubiquitous choices and uninformed decisions due to an overload of information about terms and conditions and privacy consent forms when using any digital service [9]. Regulations such as the General Data Protection Directive (GDPR) or the California Consumer Privacy Act (CCPA) force online companies to request consent to the terms and conditions when using their services. However, "I have read and agree to the terms and conditions" is the biggest lie on the internet, according to Obar and Oeldorf-Hirsch [32]. Privacy policies and consent forms are generally complicated to read and very long. The average internet user is confronted with an information overload of the extent they cannot overcome [2, 5, 32]. Thus, any online activity comes with an increasing number of security and privacy decisions, which often remain unclear to the user.

These privacy and security decisions range from agreeing to cookies or terms and conditions of various platforms, sharing personal information online, to downloading smartphone apps, where the access to personal information on the used devices is often unintentionally granted Hatamian et al. [17]. Especially smartphone apps have the power to very closely monitor private spaces, access, and map social relationships Hatamian et al. [17]. Such practices are still commonplace, even though regulations such as the GDPR are intended to improve the protection of users' behavioral data and other personal information online. App developers have been required to consider the legal framework within their app development lifecycle and to ensure that the app complies with the legal privacy principles defined in the GDPR Momen et al. [31]. However, bridging the gap between legal regulations and technical

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3543790

implementation is not often straightforward, and various applications, either intentionally or unintentionally, do not comply with the legal requirements, as shown by recent findings of Hatamian [15], Hatamian et al. [17], Momen et al. [31]. Privacy issues often remain undetected, and users are left alone deciding what services or apps to use and what security and privacy vulnerabilities might be involved. Thus, users have access to mostly incomplete and asymmetric information with no possibility of determining how much data might be collected and how it might be used and shared with third parties [2]. Privacy decisions are usually not the user's primary task, and users have limited mental resources to evaluate possible consequences of their data sharing behavior and accept privacy policies they never read before. Furthermore, users are more willing to keep track of the benefits online services provide than evaluate the privacy risks that might result from using these services [9, 27]. In recent years much research has been done on more privacy-friendly choice architecture giving rise to the concept of "nudging" [3, 30].

Privacy nudges intend to influence people's behavior predictably without prohibiting any options or altering economic incentives [42]. Hereby, nudges have appeared in the privacy literature as effective means to assist user behavior and guide to better privacy choices [2, 4, 6, 25, 39]. Digital nudges can also guide users through mobile app permissions to make privacy risks more salient and support users' choices towards more privacy-friendly permission settings that better align with their privacy concerns and expectations [6]. The information must be presented to the users in a comprehensive and digestible manner to improve the choice architecture for online privacy decisions. Online privacy awareness can be increased by presenting relevant information that can be extracted either from the privacy policy of online services and apps, permission manifest of apps or monitoring the apps' behavior. As a result of this, users need to view, read and recall relevant facts and information presented by privacy nudges with the potential to move users towards informed consent [9]. Thus, this research investigates potential privacy infringements of mobile applications by analyzing their privacy policy with respect to the privacy principles stated in the GDPR. Furthermore, a technical analysis is performed, examining the requested permissions with existing frameworks, such as the Mobile Security Framework (MobSF) [1]. The apps' behavior in terms of requested permissions, is evaluated based on the alignment with the GDPR requirements. The findings from the first analysis are the foundation to design a more privacy-friendly choice architecture by developing a permission manager informing users about potential privacy threats. Additionally, the choice architecture and nudge design are evaluated in a user study, examining if users' privacy awareness increases and if the nudges lead to more privacy-conscious decisions. Moreover, the relation of privacy literacy and privacy awareness will be examined in the context of accepting permissions requested from apps in the installation process.

A detailed analysis is presented to shed light on regulatory compliance issues of well-known and widely used applications, developing a design architecture by including various types of nudges to guide privacy-friendly decision making and informed choice in the app installation process. Thus, this analysis aims at answering the following questions:

RQ1: How do information nudges and known metaphors influence privacy awareness and user acceptance of app permissions?

RQ2: Does privacy literacy positively correlates with privacy awareness and lead to fewer accepted permissions?

Our analysis comprises three main parts. First, the apps' permission requests within their Android manifests are analyzed to provide an overview of the most prominent permission requests and their potential privacy and security implications. Second, privacy nudges are designed based on the findings of the first step. Third, a user study is conducted to examine the effectiveness of the designed nudges in terms of increased privacy awareness and improved privacy choices. In sum, the contributions of this work are the following:

(1) An in-depth privacy analysis of various applications ranging from a detailed compliance analysis with the GDPR of privacy policies to a behavioral analysis and permission access patterns.
(2) Designing privacy nudges based on the compliance analysis with the GDPR, including information nudges and known metaphors to guide the decision-making process of users.
(3) Validation of the effectiveness of privacy nudges in a user study.

This paper is organized as follows: first, an overview of related work is given in Section 2. In Section 3, the nudge design and the experimental setup will be described, and in Section 4, the results of the user study are presented. Furthermore, Section 5 discusses the results of the user study, and finally, in Section 6, we conclude this paper and indicate future research directions.

2 RELATED WORK

2.1 Mobile Privacy Permissions

From a user‘s perspective, privacy is a state of limited access to personal information [38, 46]. Limited access to personal information can be achieved in an offline world more easily and controllably than in an online world. In the past years, apps have became an indispensable part of our daily life and cover a wide range of services and utilities, such as navigation services, educational use, and social media [18, 26, 46]. Most of the apps are equipped with multiple sensors that allow data controllers to collect sensitive personal data continuously. Most of the time, the access to personal information remains hidden to app users, and the procedure to inquire what kind of information has been accessed is not straightforward. Thus, the risk evaluation of applications is left to the users who need to judge independently which permission requests seem to be reasonable in the scope of the provided service [18].

Previous research has shown that various usability problems hinder the users' understanding of the control over app permissions and the possible consequences of accepting or denying certain permissions [15, 19, 24, 26]. Mobile users often lack sufficient privacy literacy [13, 28] and awareness [7, 9, 34] to evaluate privacy risks and make privacy-aware decisions properly. Within an interview study, King [22] found that users do not fully understand what information can be accessed by apps on mobile phones. Hereby, the permission interface to control the data access does not provide any explanation about how permissions work, what data they access, and if this is in the scope of the intended use of the app or not. For Android applications, the control over permissions is often very challenging because no flexibility or control options are offered for certain permissions to deny access to personal information [18]. For iOS users, the situation is different, as an opportunity to turn specific permissions off after the installation is provided. However, also for the iOS case, no information is given on how data will be used, and what data can be accessed by which permissions [46].

Over the past years, much research effort has been put into improving privacy permission interfaces to integrate them into the decision-making process of users. Multiple privacy permission interfaces have been designed to provide information about suspicious privacy practices of apps and add warning signs [19, 24, 26, 26]. Hereby, Kelley et al. [21] developed a privacy permission interface that lists information of data being collected and not collected. After running a user study, they found that the provided additional factual information about the access of apps on personal information affected user's awareness of potential privacy breaches. Most prior work has focused on presenting additional factual information about data use to get the users involved in more transparent decision-making [46]; another research stream, including mechanisms of soft paternalism, has evolved by using privacy nudges [5, 6, 19, 26].

2.2 Information Transparency and Privacy Nudges

In general, nudges aim towards positive reinforcement and indirect recommendations to positively affect the behavior and decision-making of people in a lot of different fields, such as behavioral economics, political theory, and behavioral sciences [11]. What is referred to as a nudge is any component of choice architecture that changes people's behavior predictably. It is also important that a privacy nudge does not restrict any alternatives and significantly affect their economic incentives. The user intervention must be simple and inexpensive to avoid to qualify as a nudge. Hereby, nudges are distinct from requirements, which are not covered by the mechanism of soft paternalism [2].

Privacy nudges can also be used to negatively influence the behavior of users in order to motivate a user behavior that accommodates the economic goals of the service provider [2, 11]. In the domain of privacy bounded rationality, asymmetric information, cognitive and behavioral biases often lead to privacy decisions that are not aligned with the actual privacy preferences [21, 25, 46]. As a result of this, information and transparency have often been used in previous studies to enhance users' privacy awareness. Multiple ways have been examined, ranging from providing explicit textual and also visual information [9, 25, 45] and warning icons when suspicious use of data is observed [33]. Another example of a soft paternalism mechanism is privacy by default.

A recent privacy update from Apple showcases that privacy by default can greatly influence on how users allow access to their sensitive personal information [35]. Often users are not aware of their privacy settings, and *nudging* the user towards more privacy-conscious decisions yield be an effective measure towards permissions settings that better align with privacy concerns and expectations of the user [5, 6, 25]. Thus, the representation of permissions needs to be optimized to facilitate understanding and the overall privacy decision-making process.

Some research attempts have been made to design privacy nudges based on permission requests of various applications [5, 6, 25]. Inconsistent findings have been reported influencing effects of varying sharing context Almuhimedi et al. [6], the device where a service or app is used [7], and the usage domain of an app [2]. For example, no significant effects on privacy awareness could be detected for video-call and messenger apps, but for apps in the domain of weather or fitness significant differences can be examined [3]. Also, permission requests have been used to design privacy nudges to raise awareness and help users to interpret the meaning of requested permissions more easily. One approach is to provide the user with the number of app permissions compared to other apps with similar functionality [24]. Another approach was proposed by Sharma and Bashir [36] by collecting permission requests of apps and comparing them with the functions of the app. In this approach, the count of unnecessary permission requests that was not required for the app were presented. Furthermore, Kelley et al. [21] optimized the representation of permissions and included them in the decision-making process of whether to use an application or not to simplify the user's understanding of the permissions. Furthermore, Almuhimedi et al. [6] have found that presenting information for each permission can nudge the user towards more privacy-protecting behavior in choosing apps that request fewer permissions. In a follow-up experiment, Almuhimedi [5] designed a permission manager which allows users to modify and select permissions when sufficient information about the usage of personal information is given. Positive effects on privacy awareness and risk perception could be examined when using the permission manager. Another approach proposed by Hatamian et al. [17] focuses rather on the technical and legal analysis of permission requests itself and provides some insights on whether permissions comply with the legal requirements stated in the GDPR. To the best of our knowledge, the legal analysis of video-call and communication apps has not been used as a foundation for designing privacy nudges yet. Therefore, we combine the technical analysis of permission requests [18, 25, 36] with the legal analysis proposed by Hatamian et al. [17] to design a permission request manager based on the findings of Almuhimedi [5], which can be used throughout the installation process of applications. The permission manager aims to provide adequate control mechanisms to grant access to personal information only for reasonable permissions.

3 METHODOLOGY

3.1 Nudge Design

3.1.1 Permission Request Technical Analysis. For the technical analysis, ten apps are chosen, based on their popularity on the Google App Store and their current relevance for personal and business matters (see Table 1). Only Android apps are selected for the analysis and user study, as the tools for the technical evaluation of permission requests are only provided for Android apps.

The technical analysis of the permission requests is based on Google Scraper, a JavaScript-based tool, and the MobSF framework to fetch the permission requests of previously selected apps. The Google Scraper is used to analyze the permissions requested by any

Table 1: Description of used apps.

No.	App name (URL)	# DLs
1	Google Maps (URL)	+10B
2	WhatsApp Messenger (URL)	+5B
3	Telegram (URL)	+1B
4	Zoom Cloud Meetings (URL)	+500M
5	Pokemon GO (URL)	+100M
6	Signal Private Messenger (URL)	+100M
7	AccuWeather: Weather Radar (URL)	+100M
8	eToro: Crypto. Stocks. Social. (URL)	+10M
9	Luca (URL)	+10M
10	Der Spiegel- Nachrichten (URL)	+5M

app which has been published on the Google Play Store. The Google Scraper uses a simple key-value principle, where the name of the permission serves as a key and the type of permission as value. With the Google Scraper, the list of permissions the ten apps request is fetched and prepared for further analysis. In the next phase of the technical analysis the MobSF is used, which is an extensive tool for penetration testing to exploit and analyze any vulnerabilities of different devices. The MobSF allows for scanning the permission requests of any app (Android or iOS) and returns a report which categorizes the permissions into *dangerous* or *normal* permissions. Hereby, the MobSF makes use of the pre-defined categories of the Android App universe.

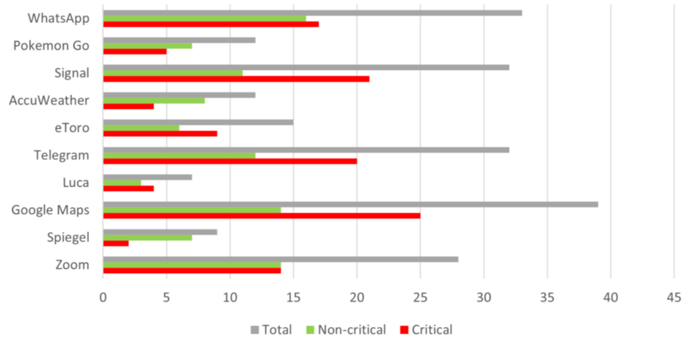


Figure 1: Results of the technical analysis of permission requests.

In a more detailed permission request analysis for Covid-19 contact tracing apps [20] describe three types of Android permissions: *install-time*, *run-time*, and *special* permissions. *Install-time* permissions are permissions which automatically granted during install time and can be further differentiated into two sub-types can be identified including *normal* and *signature* permissions. *Normal* permissions allow access to low-risk resources during the install-time, whereas *signature* permissions access more sensitive resources and also have to be granted during install-time. *Signature* permissions are important when the app is accessing specific permissions on the so-called *signature* level [20].

For the following analysis, *normal* and *signature* permissions will be excluded, as the nudge design is based only on *critical* and *non-critical* permission requests, which are further defined in the following. As an addition to the categorization through the MobSF, the list of permissions for each app is compared with the privacy policy of the respective app, to verify if the privacy policy includes information about the requested information extracted by the permission requests. Permissions that are not mentioned in the privacy policy, but access sensitive information, are further categorized as *critical* permissions. On the contrary, *non-critical* permissions are mentioned in the privacy policy of the respective app and are in the scope of the intended use and purpose of the app. In Figure 1, the results of the technical analysis are summarized. The total number of permissions and the number of *critical* and *non-critical* permissions are presented for each of the previously selected apps. The results show that Google Maps requests 25 critical permissions, such as access to the precise location, access to camera and images, and permission to modify or record audio. Also, communication apps, which are perceived to be rather a privacy-preserving, such as Signal (21 *critical permissions*) and Telegram (20 *critical permissions*), have a higher number of *critical permissions* compared to the gaming app Pokemon GO (only 5 *critical permissions*) or the news app of Spiegel Online (only 2 *critical permissions*).

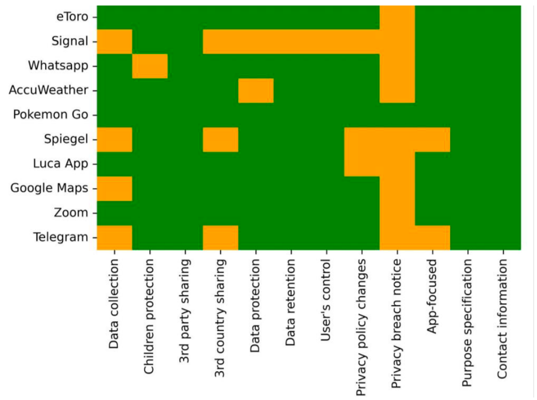


Figure 2: GDPR Analysis: green are privacy policies compliant with the GDPR principles, and orange if there might be a potential conflict.

3.1.2 Permission Request Legal Analysis. In the next phase, the compliance of the selected app with the legal requirements is analyzed. As a foundation for the legal analysis, the findings of [16] are used, a benchmarking analysis of the GDPR, resulting in 12 privacy policy principles. The principles have been extracted based on keyword- and semantic-based search techniques [20]. A description of the resulting principles can be found in appendix A. The privacy policy of an app is a legal document that entails information about how app providers use, collect, disclose and manage data collected through the apps. Within the legal analysis respective privacy policy of each app is compared with the 12 resulting privacy principles to verify if the stated privacy policy of the apps complies with the GDPR. In Figure 2 the results of this legal analysis are presented[1]. From Figure 2 it is visible that the requirement of a privacy breach notice is not fulfilled most often, followed by the data collection

[1] The compliance analysis has been conducted by using the GDPR principles defined by [16]. However, the legal analysis was conducted without a legal expert. Therefore, the results of the legal analysis might include some flaws.

principle (non-compliance of 4 apps), third-country sharing, and privacy policy changes (non-compliance of 3 apps).

Based on the technical and legal permission request analysis only two apps were chosen for the user study. The selection of the two apps was made based on a qualitative assessment. Due to the current pandemic, Zoom has experienced a great increase in usage due to the shift from offline to online meetings [43]. Similarly, the communication app Telegram has experienced a new level of popularity during the pandemic [10]. Due to the increased usage and popularity of these two apps, partially caused by the current pandemic, we decided to integrate these as examples for a more privacy-friendly application (Zoom) and a rather ambiguous example when it comes to critical permissions and compliance with the GDPR principles (Telegram). Thus, the following nudge design is based on the critical permission requests of both apps, Zoom and Telegram, and their GDPR compliance analysis. A detailed description of the permission can be found in Table 2[2].

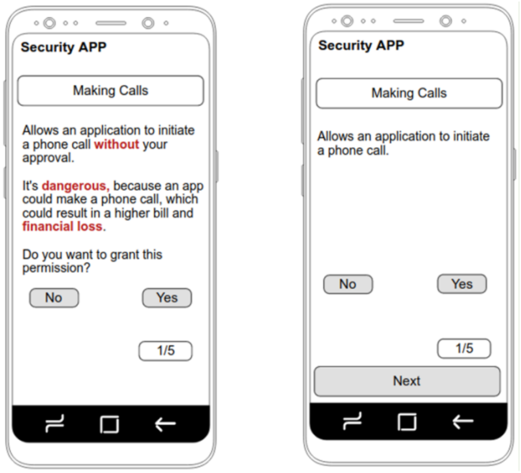
3.1.3 Permission Request Manager and Nudge Design. When warning users about potential privacy risks using known metaphors makes them more aware of the consequences and leads to more security-protective decisions [2]. Nowadays, many real-world concepts are used as metaphors to make it easier for users to interact with a complicated system using concepts they can recognize [39]. A famous example from everyday life is the Nutrition-Score used in front-of-pack food labeling. It shows an overall score for the nutritional values of beverages and food. The assessment is made on a five-level scale and is inspired by the concept of a traffic light. Red stands for the lowest nutritional value and green for the highest. This makes it easier to spot the healthy option and nudge users towards buying it [12]. Moreover, Chantal et al. [12] discuss studies that have investigated the effect of the Nutrition-Score. It is compared with other concepts, for example, the Multiple Traffic Light (MTL), in which no overall score is printed, but the individual ingredients are presented in traffic light color-coding. They find that the Nutrition-Score as a summarized overall score in traffic light colors is the best identified and understood approach. Similarly, implementing concepts based on the traffic light semantic can be found in security and privacy-related matters. For example, user interface representations of risk or warning following the red/amber/green mode proved to be effective in previous studies [39]. Based on that, this paper is going to use the traffic light semantic in the nudge design in order to make permission requests easily understandable for the average user [6]. Similarly, Tan et al. [41] showed that permission requests that include explanation are remarkably more likely to be approved by users.

Furthermore, Shih et al. [37] conducted a study that showed that users share the most when permission requests contain no information about data access or purpose. They also found that 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. Moreover, Almuhimedi [5] investigates whether permission managers, which allow users to review and modify the apps' permissions, help users make better privacy decisions. The study confirms that users are mostly unaware of mobile app data collection practices. Furthermore, a permission manager, which is enhanced by the delivery of privacy nudges, increases user awareness of privacy risks associated with apps and motivates users to adjust their app settings. In this study, we extend the nudge design from Almuhimedi [5] by adding further information about GDPR compliance of the app's permission and the traffic light metaphor. To examine the effect of the visual and information nudges the permission manager is

Table 2: Description of permissions.

Permission	Descriptions
ACCESS_COARSE_LOCATION	Allows the app to get the user's approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where the user is.
ACCESS_FINE_LOCATION	Allows the app to get the user's precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where the user is, and may consume additional battery power.
ACCESS_NETWORK_STATE	Allows the app to view information about network connections such as which networks exist and are connected.
GET_ACCOUNTS	Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed (e.g. Goolge - Account Name: bob@gmail.com).
INTERNET	Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.
READ_CALL_LOG	Allows the app to read the user's phone's call log, including data about incoming and outgoing calls. This permission allows apps to save the user's call log data, and malicious apps may share call log data without the user's knowledge.
READ_CONTACTS	Allows the app to read data about the user's contacts stored on your phone, including the frequency with which the user called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save the user's contact data, and malicious apps may share contact data without the user's knowledge.
READ_PHONE_STATE	Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any *PhoneAccounts* registered on the device
READ_PROFILE	Allows the app to read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others
RECORD_AUDIO	Allows the app to record audio with the microphone. This permission allows the app to record audio at any time without your confirmation.
WRITE_CALENDAR	Allows the app to add, remove, change events that you can modify on your phone, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge.
WRITE_EXTERNAL_STORAGE	Allows the app to write to the SD card.

[2] http://androidpermissions.com/



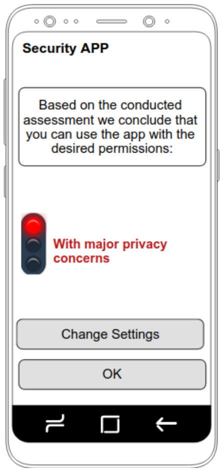
Allows an application to initiate a phone call without your approval.

It's dangerous, because an app could make a phone call, which could result in a higher bill and financial loss.

Do you want to grant this permission?

Allows an application to initiate a phone call.

Figure 3: Comparison of experimental (left) and control group (right) of permission manager example.



Based on the conducted assessment we conclude that you can use the app with the desired permissions:

With major privacy concerns

Figure 4: Example of traffic light display for the experimental group.

designed in two versions: (1) for the control group with only plain information and without the traffic light metaphor (instructions about accepting the respective permission request are given beforehand for the control group); and (2) version for the experimental group, where additional information about GDPR compliance and the color scheme of the traffic light was used (see Figure 3).

The traffic light metaphor is used as a color scheme to highlight text-based information, but also to give a final indication if the granted permissions comply with the GDPR principles (see Figure 4):

- **Red**: if there are permissions granted, which do not comply with the GDPR,
- **Amber**: if there are permissions where the GDPR principles e.g. purpose specification are not clearly addressed or followed,
- **Green**: if there are no violations of GDPR principles

3.2 Experimental Design

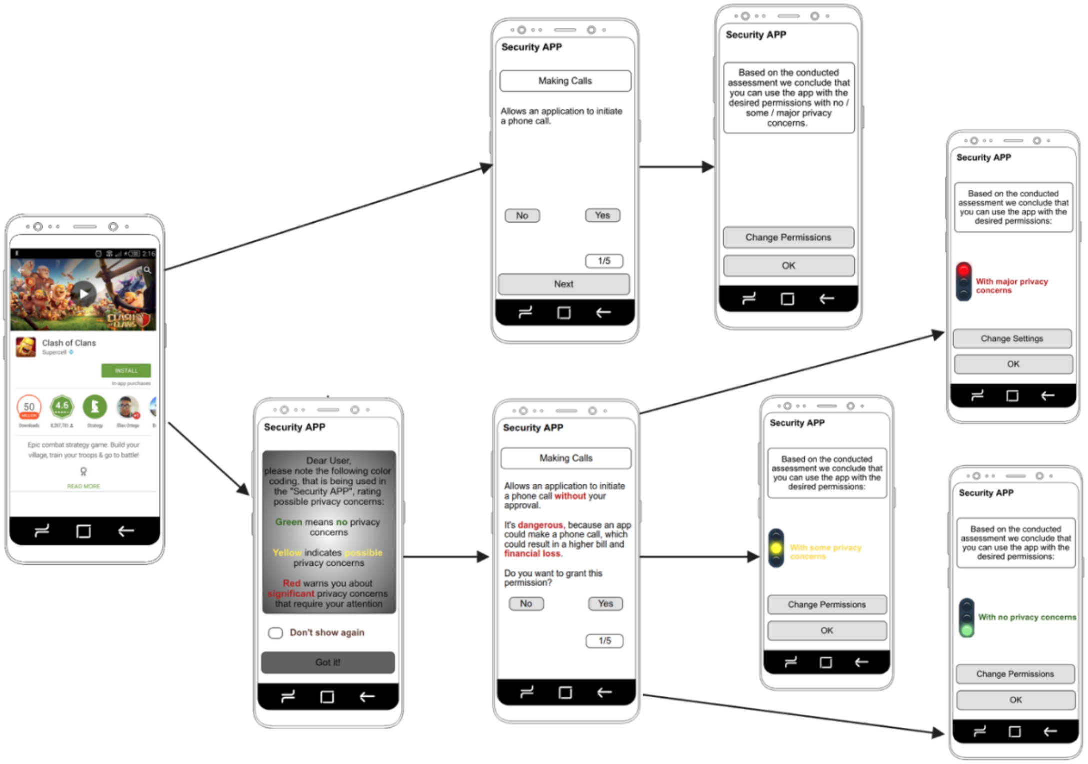
When measuring the influence of the information and visual nudge on privacy awareness, the privacy awareness questionnaire was asked before and after the permission manager app part of the experiment.

3.2.1 *Privacy Awareness and Literacy.*

The privacy awareness questionnaire was adapted from previous surveys [8, 14, 34], consisting of items measuring online privacy awareness, privacy concern, and perceived control (the questionnaire items can be found in Appendix B). A 7-point Likert scale is used for the privacy awareness items, as this scale has been used in the previously validated questionnaire items in Barth et al. [8], Díaz Ferreyra et al. [14], Pötzsch [34]. Additionally, a privacy literacy questionnaire was incorporated in the study to examine if privacy literacy positively correlates with privacy awareness and the number of accepted permission requests. Empirical research has shown that there are disparities in internet users' online privacy attitudes and online privacy behavior [8, 14, 29]. Even though concern about data collection and sharing practices is expressed, users share personal and sometimes intimate information on various online platforms [29]. According to Trepte et al. [44], the inconsistency of privacy attitudes and online privacy behavior can be partially explained by a *knowledge gap hypothesis*, stating that people are concerned about their online privacy but lack the required knowledge to act accordingly. To further explore the relation of privacy awareness, privacy behavior, and privacy literacy in the context of the privacy nudges in a permission request manager environment, we adopt the Online Privacy Literacy Scale (OPLIS) from [44] to measure various dimensions of privacy literacy. The privacy literacy encompasses four dimensions concerning literacy about data collection, literacy of legal aspects of data protection, literacy about technical aspects of data protection, and literacy about data protection strategies. Each dimension is measured by five multiple-choice questions. Furthermore, questions about the used operating systems (iPhone, Android, or other) are added to the demographics section to explore if the usage of certain operating systems correlates with higher privacy awareness, privacy literacy, or the number of accepted permissions.

3.2.2 *Experimental Workflow.*

The overall design of the study is based on a simulation of an app installation process. The participants were asked to download an application via the permission manager app in a web app mockup (see Figure 5). When choosing an application (here either Zoom or Telegram) the experimental group received information and visual nudge, explaining the meaning of the color scheme of the traffic light metaphor. The participants were asked to click through the different permissions and either accept or reject them. For each permission, potential privacy threats have been communicated with the traffic light metaphor and explanations for the experimental group, but only plain and limited information was given to the control group. After accepting or rejecting the permissions the final indication was shown to the experimental group, if the granted permissions contain any privacy infringements which are not GDPR compliant, whereas the control group received only plain information if the app can be used with high, some, or no privacy concern.



Allows an application to initiate a phone call.

Based on the conducted assessment we conclude that you can use the app with the desired permissions with no / some / major privacy concerns.

Dear User, please note the following color coding, that is being used in the "Security APP", rating possible privacy concerns:

Green means no privacy concerns

Yellow indicates possible privacy concerns

Red warns you about significant privacy concerns that require your attention

□ Don't show again

Allows an application to initiate a phone call without your approval.

It's dangerous, because an app could make a phone call, which could result in a higher bill and financial loss.

Do you want to grant this permission?

Based on the conducted assessment we conclude that you can use the app with the desired permissions:

With major privacy concerns

With some privacy concerns

With no privacy concerns

Figure 5: Workflow of the study design.

The permission manager could not be easily integrated into existing survey platforms. Therefore, we developed a custom web app mockup based on three components (see Figure 6): (1) the web app itself, which is built using the reactive JavaScript framework *Svelte*[3] and hosted on *Netlify*[4]; (2) backend functionalities have been implemented by using serverless *Netlify Functions*[5]; and (3) the database to store the user entries provided and managed by *Fauna*[6]. The survey website was created for both desktop and mobile viewing. Also, a progress bar was implemented to show the participants how far they are and prevent aborting the study just before they almost finished. The web app mockup featured an app-store-like screen to simulate the usual installation process of an app. The app mockup was shown in full-screen on smartphones and inside a smartphone-frame in the desktop version. Additionally, to ensure that there is roughly an equal number of participants in the control and experimental group, the web app performs a request to the backend every time a participant reaches the web app mockup section. A boolean flag (named *control*) is used to indicate if the current participant receives the control or experimental group web app mockup. Every time a participant submits the questionnaire, the boolean flag gets flipped, such that the next participant receives the other version of the web app mockup. Only if two requests are made at the exact same time both participants get the same version (e.g. both get the experimental group version) of the web app mockup. The experiment has been conducted in accordance with the rules of the ethics committee of Faculty IV of the Technical University [will be announced after blind review has been finished].

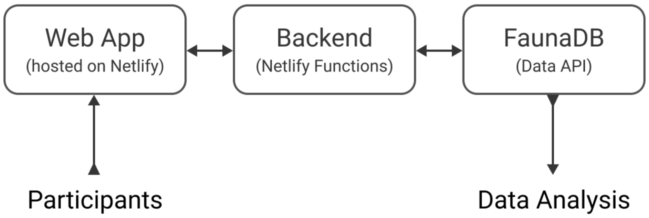


Figure 6: Backend and frontend components

4 RESULTS

Overall, 70 participants took part in the survey where 38 participants took part in the control group and 32 in the experimental group[7]. The participation was voluntary and the responses have been collected in a period over one week through the experiment platform described in Section 3 (see Figure 6).

[3] https://www.svelte.dev
[4] https://www.netlify.com
[5] https://www.netlify.com/products/functions
[6] https://www.fauna.com

[7] Due to early drop outs of participants in the questionnaire, the answers have not been partially used for the analysis. Thus, there is an unequal amount of participants in the experimental and control group.

4.1 Demographics

The mean age of the participants is 26 years, the oldest participant being 52 and the youngest participant 18 years old. Most of the participants have a high school diploma (31) or bachelor's degree (21), master's degree (8), or are doing an apprenticeship (8). Only two participants have a doctoral degree. 33 participants identify as female, whereas 32 identify as male. Five participants did not want to indicate their gender preferences. Most of the participants (57) are living in a big city (over 250.000 inhabitants), whereas only a few participants are living either in a small city (4) or countryside (1). Additionally, information about the importance of the operations system (OS [Android, iOS, or other]) was asked during the survey, where the participants could indicate if the OS is either unimportant to them (19) or important (43). When comparing the OS importance with the selected OS in use (Android 43, iOS 25, other 2), it can be assumed that for most of the participants, Android is the OS of preference. However, the total number of accepted permissions is not significantly different between iOS (163 accepted permissions) and Android (162 accepted permissions).

4.2 Privacy Awareness and Privacy Literacy

The internal consistency of the overall privacy awareness questions can be measured with Cronbach's α, which is .79 for the overall privacy awareness measure, which indicates good internal consistency. The internal consistency changes when the different dimensions of privacy awareness are analyzed separately. The Cronbach's α increases for:

(1) the dimension of privacy awareness to .81,
(2) the dimension of privacy concern to .83,
(3) the dimension of privacy control to .83.

The internal consistency of the privacy awareness dimensions is reasonably good and can be taken for further analysis. However, for the OPLIS scale, the Cronbach's α is 0.65, which is only a moderate consistency but still acceptable. Moreover, the privacy literacy score was calculated based on the number of correct answers in accordance with the validation of the OPLIS scale Trepte et al. [44].

For the evaluation of privacy awareness, a privacy awareness score was created based on the 7-point Likert Scale by calculating the average score for the overall privacy awareness and the separate item batteries, such as privacy control and privacy concern. In order to verify if the privacy nudges lead to higher privacy awareness and accepting less permission requests, the privacy awareness questions before and after the nudge has been presented are analyzed for the experimental group in comparison with the control group. When comparing between-group differences privacy awareness did not increase for the experimental group after the nudges were presented. Privacy awareness only increased for the control group but not significantly (see Figure 7 and 8).

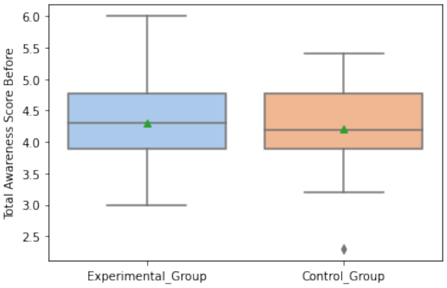


Figure 7: Privacy Awareness before the nudge.

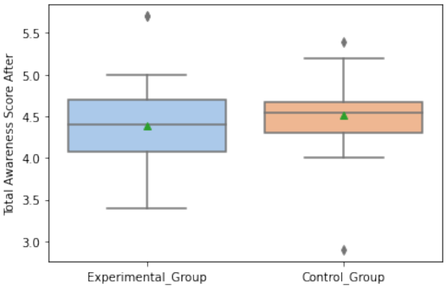


Figure 8: Privacy Awareness after the nudge.

However, when comparing within-group differences of privacy awareness, the Wilcoxon-Signed-Rank Test (due to violation of assumptions for parametric methods) showed significant differences when comparing the total privacy awareness of the control group ($Z = 99.0$ $p = .002$, when applying Bonferroni correction the new alpha level being $\alpha = .008$) (see Figure 7 and 8 only comparing control group results), but no significant differences could be found for the experimental group. Further significant differences can be found for the control group when comparing privacy concern before and after the privacy nudges have been presented ($Z = 77.0$: $p = .001$, when applying Bonferroni correction (new alpha level being $\alpha = .008$), indicating that the plain nudge increased privacy concern for the control group, but the visual and more comprehensive information nudge for the experimental group did not (see Figures 9 and 10).

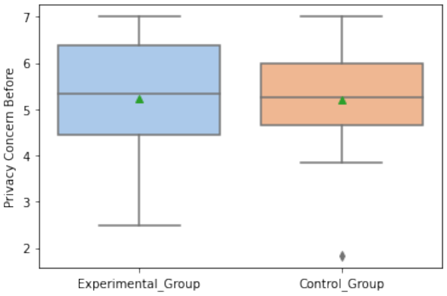


Figure 9: Privacy Concern before the nudge.

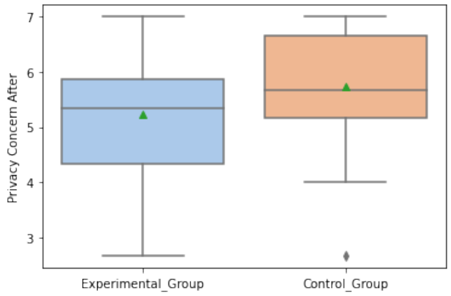


Figure 10: Privacy Concern after the nudge.

Only the total awareness score showed a significantly negative correlation with the number of accepted permissions for the experiment group with Spearman Correlation ($r = -.604, p < .001$), indicating that the higher the total privacy awareness, the lower the number of accepted permissions. Furthermore, the total awareness score showed a positive correlation with the overall privacy literacy score ($r = .442, p < .001$), indicating that the higher the total privacy awareness is, the higher the privacy literacy (see Figure 11).

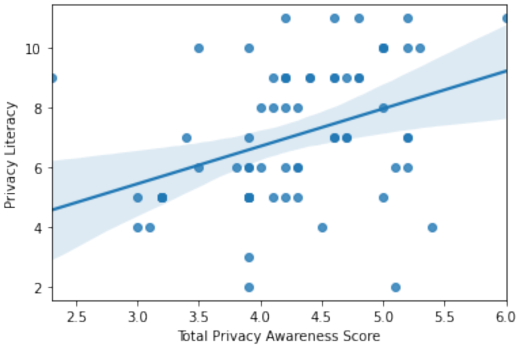


Figure 11: Correlation of total privacy awareness and privacy literacy.

Additionally, total privacy awareness and education showed a significant positive correlation ($r = .42, p < .001$), indicating that the higher the education level, the higher the total privacy awareness.

4.3 Permission Requests

When analyzing the different permission requests, there are significant differences between the accepted permissions between Telegram and Zoom. Only the permissions which are requested by Zoom and Telegram are considered (see Table 3). The permissions READ_CALL_LOG, READ_PROFILE, RECORD_AUDIO, and WRITE _CALENDAR have been removed, as they are only requested from either Zoom or Telegram. A chi-square test of independence shows that there is a significant association between the download scenarios of Telegram and Zoom and the number of accepted permissions ($X^2(7) = 149.59, p < 0.001$). Hereby, the most frequently accepted permissions are access to INTERNET connection, access to contacts READ_CONTACTS and ACCESS_NETWORK_STATE. These permissions are rather reasonable in the scope of the intended use of Telegram and Zoom. On the other hand, the least accepted permissions are ACCESS_FINE_LOCATION, GET_ACCOUNTS, and READ_PHONE_STATE, which clearly relate to personal information collected when the permissions are accepted. From Table 3, a tendency can be inferred that the participants tend to accept permissions where a clear purpose specification to the intended use or the app is visible.

Table 3: Number of accepted permissions (NaN meaning permission was not asked for the application)

Permission	Telegram	Zoom	# accepted permissions
ACCESS_COARSE_LOCATION	12	11	23
ACCESS_FINE_LOCATION	11	9	20
ACCESS_NETWORK_STATE	17	19	36
GET_ACCOUNTS	9	11	20
INTERNET	50	54	104
READ_CALL_LOG	7	NaN	7
READ_CONTACTS	25	17	42
READ_PHONE_STATE	11	11	22
READ_PROFILE	10	NaN	10
RECORD_AUDIO	30	NaN	30
WRITE_CALENDAR	NaN	10	10
WRITE_EXTERNAL_STORAGE	22	14	36

5 DISCUSSION

The analysis of the results show that the stated research questions can be answered as follows:

RQ1: *How do information nudges and known metaphors influence privacy awareness and user acceptance of app permissions?*
Privacy awareness increased after the privacy nudges were displayed but increased significantly for the control group only. This result indicates that the plain visual and information nudge might be more effective in communicating possible critical permission requests. However, when comparing the number of accepted permissions, the increased privacy awareness did not show a significant negative correlation with the overall number of accepted permission. Even though the privacy awareness increased, the behavior in terms of rejecting permissions did not comply with the increase in privacy awareness for the control group. Only for the privacy awareness of the experimental group, a significant negative correlation was found with the number of accepted permissions, possibly indicating that the information displayed as a visual nudge might have an effect on privacy behavior in terms of the number of accepted permissions. A limitation of the study might be, that the control group also received an information nudge, which only provided very brief information about the requested permissions but might have been more effective in communicating the associated risk in terms of the length of the text. The assessment of this potential shortcoming, the study needs to be repeated with more participants and two experimental groups; one experimental group receiving

the visual and information nudge, one experimental group only receiving the plain information nudge, and one control group not receiving any nudge. Moreover, the web app mockup was only a simulation of downloading an application. In a real-life scenario, the participants might show a different permission acceptance behavior when their real data is requested.

RQ2: *Does privacy literacy positively correlates with privacy awareness and lead to fewer accepted permissions?*
Privacy literacy has a medium positive correlation with higher privacy awareness. However, when analyzing the association with the number of accepted permissions, no negative correlations were identified, indicating less accepted permissions when privacy awareness or privacy literacy increases. The mismatch of increased privacy awareness and privacy literacy and privacy behavior can often be observed and further confirms the *Privacy Paradox* [23].

Furthermore, a continuous scale of representing the GDPR compliance and the associated danger of accepting the permission request can be an interesting addition to the categorization of GDPR compliance and danger in the three traffic light categories. A comparison of a more fine-grained analysis of the dangers associated with each permission request is left for future research.

Overall, the findings show that communicating privacy principles and associated risks of data sharing is still a challenge, where further research can be done in order to design adequate privacy nudges which foster privacy-conscious decision-making. The analysis of the permission requests can further be grouped into more clear data types, which would reduce the number of permissions the user needs to click through and communicate the risks of sharing various data types on a more aggregated level.

6 CONCLUSION

In this study, a multidimensional analysis of permission requests has been presented, in particular focusing on their system permission requests, their privacy policies, and adherence to existing regulations defined in the GDPR. Furthermore, the run-time permission requests are included in order to identify privacy and security issues associated with applications selected for the analysis. Based on the multidimensional analysis of permission requests, privacy nudges have been designed, including information and visual cues. The information nudge includes information about the permission request by communicating potential risks associated with accepting this permission. For the visual nudge the traffic-light metaphor was used indicating GDPR complicate of the requested permissions. In a user study, the influence of the designed nudges on privacy awareness and privacy literacy was examined, where privacy awareness only increased significantly for the control group after presenting a plain nudge but not for the experimental group. Additionally, privacy concern also increased significantly only for the control group after presenting the plain nudge, but not for the experimental group, indicating that the plain nudge might be more effective in communicating associated risks of accepting permission requests. The influence of the privacy nudges on privacy behavior (in terms of the number of accepted permissions) showed a significant negative correlation for the experimental group suggesting that the visual nudge might lead to more privacy-conscious behavior, but not to an increase of privacy awareness. However, this finding needs to be validated in further studies considering larger sample size and an additional control group, not receiving any privacy nudges. Further studies are considered to aggregate the permission requests into broader data types to increase the comprehensibility of the information provided. Additionally, usability aspects and cognitive load will be examined for different privacy nudges to improve the evaluation of nudges influencing privacy-conscious decision-making.

ACKNOWLEDGMENTS

The study has been conducted with the support of the DFG in the scope of the project MO 1038/28-1. The authors thank the students who took part in the module Advanced Study Projects in the Usable Privacy project in 2021.

REFERENCES

[1] 2020. Mobile Security Framework (MobSF). https://github.com/MobSF/Mobile-Security-Framework-MobSF

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[4] José Alemany, Elena Del Val, and Ana García-Fornes. 2020. Empowering Users Regarding the Sensitivity of their Data in Social Networks through Nudge Mechanisms.. In *HICSS*. 1–10.

[5] Hazim Almuhimedi. 2017. Helping Smartphone Users Manage their Privacy through Nudges. (2017).

[6] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.

[7] Fatma Alrayes and Alia Abdelmoty. 2016. Towards location privacy awareness on geo-social networks. In *2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST)*. IEEE, 105–114.

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

[9] Kristoffer Bergram, Valéry Bezençon, Paul Maingot, Tony Gjerlufsen, and Adrian Holzer. 2020. Digital Nudges for Privacy Awareness: From consent to informed consent?. In *ECIS*.

[10] Matthijs Blankers, Daan van der Gouwe, Lavinia Stegemann, and Laura Smit-Rigter. 2021. Changes in Online Psychoactive Substance Trade via Telegram during the COVID-19 Pandemic. *European Addiction Research* (2021), 1–6.

[11] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. Priv. Enhancing Technol.* 2016, 4 (2016), 237–254.

[12] Julia Chantal, Serge Hercberg, World Health Organization, et al. 2017. Development of a new front-of-pack nutrition label in France: the five-colour Nutri-Score. *Public Health Panorama* 3, 04 (2017), 712–725.

[13] Rachna Dhamija, J Doug Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 581–590.

[14] Nicolás E Díaz Ferreyra, Tobias Kroll, Esma Aïmeur, Stefan Stieglitz, and Maritta Heisel. 2020. Preventative Nudges: Introducing Risk Cues for Supporting Online Self-Disclosure Decisions. *Information* 11, 8 (2020), 399.

[15] Majid Hatamian. 2020. Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access* 8 (2020), 35429–35445.

[16] M. Hatamian. 2020. Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers. *IEEE Access* 8 (2020), 35429–35445.

[17] Majid Hatamian, Nurul Momen, Lothar Fritsch, and Kai Rannenberg. 2019. A multilateral privacy impact analysis method for android apps. In *Annual Privacy Forum*. Springer, 87–106.

[18] Majid Hatamian, Jetzabel Serna, and Kai Rannenberg. 2019. Revealing the unrevealed: Mining smartphone users privacy perception on app markets. *Computers & Security* 83 (2019), 332–353.

[19] Majid Hatamian, Samuel Wairimu, Nurul Momen, and Lothar Fritsch. 2021. A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical Software Engineering* 26, 3 (2021), 1–51.

[20] Majid Hatamian, Samuel Wairimu, Nurul Momen, and Lothar Fritsch. 2021. A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical Software Engineering* 26, 3 (2021), 1–51.

[21] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems.* 3393–3402.

[22] Jennifer King. 2012. How Come I'm Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations. *Smartphones and Privacy Expectations.(March 15, 2012)* (2012).

[23] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[24] Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2014. Using statistical information to communicate android permission risks to users. In *2014 Workshop on Socio-Technical Aspects in Security and Trust.* IEEE, 48–55.

[25] Tobias Kroll and Stefan Stieglitz. 2021. Digital nudging and privacy: improving decisions about self-disclosure in social networks. *Behaviour & Information Technology* 40, 1 (2021), 1–19.

[26] Rui Li, Wenrui Diao, Zhou Li, Shishuai Yang, Shuang Li, and Shanqing Guo. 2021. Android Custom Permissions Demystified: A Comprehensive Security Evaluation. *IEEE Transactions on Software Engineering* (2021).

[27] Helia Marreiros, Mirco Tonin, Michael Vlassopoulos, and MC Schraefel. 2017. "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization* 140 (2017), 1–17.

[28] Philipp K Masur, Doris Teutsch, and Sabine Trepte. 2017. Development and Validation of the Online Privacy Literacy Scale (OPLIS). *Diagnostica* 63, 4 (2017), 256–268.

[29] Philipp K Masur, Doris Teutsch, and Sabine Trepte. 2017. Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica* (2017).

[30] Tobias Mirsch, Christiane Lehrer, and Reinhard Jung. 2017. Digital nudging: Altering user behavior in digital environments. *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* (2017), 634–648.

[31] Nurul Momen, Majid Hatamian, and Lothar Fritsch. 2019. Did app privacy improve after the GDPR? *IEEE Security & Privacy* 17, 6 (2019), 10–20.

[32] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147.

[33] Irene Pollach. 2006. Privacy statements as a means of uncertainty reduction in WWW interactions. *Journal of Organizational and End User Computing (JOEUC)* 18, 1 (2006), 23–49.

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

[35] Alison DeNisco Rayome. 2021. *This iPhone setting can stop ads from following you across the web.* https://www.cnet.com/tech/services-and-software/iphone-privacy-setting-stop-ads-tracking-you/

[36] Tanusree Sharma and Masooda Bashir. 2020. Are PETs (Privacy Enhancing Technologies) Giving Protection for Smartphones?–A Case Study. *arXiv preprint arXiv:2007.04444* (2020).

[37] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* 807–816.

[38] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly* (1996), 167–196.

[39] Borce Stojkovski, Gabriele Lenzini, and Vincent Koenig. 2021. " 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.* 1235–1246.

[40] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. 2015. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* 22, e1 (2015), e28–e33.

[41] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. 2014. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 91–100.

[42] RH Thaler and CR Sunstein. 2009. Nudge: Improving Decisions About Health, Wealth, and Happiness. Penguin Books. (2009).

[43] Kometh Thawanyarat, Shannon Francis, Trudy Kim, Connor Arquette, Shane Morrison, and Rahim Nazerali. 2022. The Zoom Effect: A Google Trends Analysis. *Aesthetic surgery journal* 42, 1 (2022), NP76–NP82.

[44] Sabine Trepte, Doris Teutsch, Philipp K Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In *Reforming European data protection law.* Springer, 333–365.

[45] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research* 23, 4 (2012), 1342–1363.

[46] Bo Zhang and Heng Xu. 2016. 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.* 1676–1690.

A GDPR PRINCIPLES

The list of GDPR principles presented in Table A are summarized and used similarly in [20] and [17].

(1) **Data Collection**: Art. 5 (1) GDPR states the principles related to the processing of personal data. Most importantly, it is declared that personal data should be processed lawfully and in a transparent manner. The data should be accurate, adequate, and only collected for a specified and legitimate purpose. Generally, personal data should not be stored longer than is necessary for the purposes for which the data are processed. Art. 6 (1) GDPR explains when data processing is lawful. This includes, for example, when the user gives consent or if processing is important for performing a contract.

(2) **Third-Country Sharing**: The transfer of personal data to a third country can take place if the commission has decided that the third country guarantees a similar level of protection (Art. 45 GDPR). Furthermore, if an app provider intends on sharing personal data with third countries, it should be mentioned in the privacy policy how they will deal with third-country data sharing practices [17].

(3) **Purpose Specification**: According to Art. 13 (1c) of the GDPR app providers have to specify data collection purposes and communicate them to the user.

(4) **Third-Party Sharing**: When collecting data, the controller should inform the user of the recipients or categories of recipients of the personal data (Art 13 (1e) GDPR).

(5) **Children Protection**: Personal data of children should be given special protection because they might be less aware of the risks, consequences, and rights regarding the processing of their personal data. (Rec. 38 GDPR). Any information or communication regarding processing children's personal data, clear and plain language, that a child can easily understand, should be used (Rec. 58 GDPR).

(6) **Data Protection**: The controller and processor should implement proper organizational and technical measures to guarantee a sufficient level of security. (Art. 32 GDPR). This is especially relevant to smartphone ecosystems because they are typically associated with a huge amount of data transfer [17].

(7) **Data Retention**: Art. 17 of the GDPR states that users have the right to be forgotten. Thus, the controller should inform the users for which period their personal data will be stored (Art. 13 (2) GDPR).

(8) **Privacy Policy Changes**: Any changes in the privacy policy of an app should be communicated with the user to ensure transparent and fair processing of the data (Art. 12 GDPR).

(9) **User‘s Control**: Chapter three of the GDPR is devoted to the rights of users, including transparency and modalities,

information and access to personal data, rectification and erasure, right to object and automated individual decision-making, as well as, restrictions of processing. According to Art. 13 (2) GDPR, the controller should provide these rights to the users to ensure fair and transparent processing of the data.

(10) **Privacy Breach Notification**: Any personal data breach that might result in a high risk to the rights and freedoms of the users shall be communicated with them immediately. The nature of the breach and information about technical and organizational protection measures should be communicated in clear and plain language (Art. 34 GDPR).

(11) **App-Focused**: This principle is derived from the principle of lawfulness, fairness, and transparency. Privacy policies are often not exclusive for a certain app but written for multiple services provided by the same app developer [40].

(12) **Contact Information**: Users should be informed about the identity and contact details of data collectors. This includes the name and the postal address (Art. 13 (1a)).

B PRIVACY AWARENESS QUESTIONNAIRE

B.1 General Privacy Awareness

(1) *I am aware of the privacy issues and practices of the apps I use*

(2) *I follow the news and developments concerning privacy issues and privacy violations*

(3) *Most businesses don't handle the personal information they collect about consumers in a proper and confidential way*

(4) *I would be uncomfortable with companies having access to pictures on my device*

B.2 Privacy Awareness and Concern

(1) *Consumers lost all control over how personal information is collected and used by companies*

(2) *Existing laws and organizational practices don't provide a reasonable level of protection for consumer privacy today*

(3) *I am concerned that mobile apps are collecting too much information about me*

(4) *I am concerned that mobile apps may monitor my activities on my mobile device*

(5) *I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization*

(6) *I feel that as a result of using mobile apps, others know more about me than I am comfortable with*

B.3 Perceived Control

(1) *I believe I have control over who can get access to my personal information collected by a mobile application*

(2) *I think I have control over what personal information is released by a mobile application*

(3) *I believe I have control over how personal information is used by a mobile application*

(4) *I believe I can control my personal information provided to a mobile application*