IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 10, 2020, accepted February 4, 2020, date of publication February 18, 2020, date of current version February 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2974911

Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers

MAJID HATAMIAN, (Student Member, IEEE)
Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt, 60323 Frankfurt, Germany
e-mail: majid.hatamian.h@ieee.org

This work was supported by the H2020 Marie Skłodowska-Curie EU Project through Privacy&Us under Grant 675730.

ABSTRACT With the rapid growth of technology in recent years, we are surrounded by or even dependent on the use of technological devices such as smartphones as they are now an indispensable part of our life. Smartphone applications (apps) provide a wide range of utilities such as navigation, entertainment, fitness, etc. To provide such context-sensitive services to users, apps need to access users' data including sensitive ones, which in turn, can potentially lead to privacy invasions. To protect users against potential privacy invasions in such a vulnerable ecosystem, legislation such as the European Union General Data Protection Regulation (EU GDPR) demands best privacy practices. Therefore, app developers are required to make their apps compatible with legal privacy principles enforced by law. However, this is not an easy task for app developers to comprehend purely legal principles to understand *what* needs to be implemented. Similarly, bridging the gap between legal principles and technical implementations to understand *how* legal principles need to be implemented is another barrier to develop privacy-friendly apps. To this end, this paper proposes a privacy and security design guide catalog for app developers to assist them in understanding and adopting the most relevant privacy and security principles in the context of smartphone apps. The presented catalog is aimed at mapping the identified legal principles to practical privacy and security solutions that can be implemented by developers to ensure enhanced privacy aligned with existing legislation. Through conducting a case study, it is confirmed that there is a significant gap between what developers are doing in reality and what they promise to do. This paper provides researchers and developers of privacy-related technicalities an overview of the characteristics of existing privacy requirements needed to be implemented in smartphone ecosystems, on which they can base their work.

INDEX TERMS App, developers, GDPR, guideline catalog, privacy engineering, smartphone apps.

I. INTRODUCTION

Despite the benefits resulting from mobile applications (apps), the massive collection of users' personal data has raised serious privacy concerns. Users are often unaware of data collection practices of apps and unknowingly make a compromise against their own privacy for financial and functional benefits. This is also due to the lack of proper transparency notices and privacy indicators in app markets that would make users aware of privacy practices of apps and could assist them in an informed privacy decision-making process [1]. As the main producer of apps, developers are demanded by law [2], [3] to fulfill privacy and security principles. This is highly important, as privacy and security design decisions made by developers may directly/indirectly influence users' privacy decision-making process [4].

Although increasing mobile users' privacy awareness is gently being explored [5]–[9], there exists a need to increase the privacy awareness of app developers and assist them in designing privacy and security preserving apps. Several studies [10]–[13] showed that privacy unawareness of app developers is responsible for designing and developing security- and privacy-unfriendly apps. For instance, Peng *et al.* [12] highlighted the effectiveness of assigning risk scores to apps by initiating feedback mechanisms to encourage developers to reduce the risk that an app introduces

The associate editor coordinating the review of this manuscript and approving it for publication was Peter Langendorfer.

to a given smartphone. The authors in [11], [14] also signaled the absence of privacy-aware app development practice which leads to a growth in the total number of over-privileged apps asking for more permissions than needed for their proper functionality. This gets even more critical when it comes to pre-installed apps as they have more power to control and customize Android phones through platform-defined higher protection level permissions such as *Signature* and *SignatureOrSystem* level permissions. Also, they cannot be (easily) uninstalled by users. It was also shown that such apps are an obvious threat to users' privacy as they are oftentimes over-privileged [14]. Therefore, developers of such apps must more seriously take privacy principles into account and they must accept their responsibility to protect end-users.

To protect users, regulators are increasingly demanding app developers to design their apps in a secure- and privacy-enhancing way. In addition, privacy and security shall be embedded in the design phase of IT products such as mobile apps [15] not only at an individual level, but also industrial/enterprise level [16]. However, designing and developing security- and privacy-friendly apps is not an easy task for developers due to their limited knowledge of legal and technical aspects of privacy and security principles. Also, due to the comprehensiveness and diverse nature of available regulatory documents, it is highly challenging for developers to easily and quickly grasp the most relevant privacy and security principle guidelines needed to be followed.

Previous studies are mainly focused on users' privacy awareness and app developers' privacy awareness is not a well-explored research direction yet. Thus, it is of particular importance to provide up-to-date guidelines and instructions aligned with recently adopted regulations and privacy principles to further support app developers for designing security- and privacy-friendly apps. Regulations such as the European Union General Data Protection Regulation (EU GDPR), ePrivacy Directive and Regulation are already calling for actions to somehow revamp this situation. But there is still a huge gap between the legal nature of privacy and security principles (in the context of smartphone apps) and the technical implementation of those principles [17]. In other words, a privacy engineering perspective is needed to fill the gap between secure mobile app development and legal privacy principles needed to be followed by developers. There are already guidelines on principles needed for mobile apps that can be helpful to increase the privacy awareness of mobile app developers. However, such guidelines are suffering from serious issues. Hence, their usefulness and applicability are quite limited. For instance, they are sometimes written in a very vague language. Also, they sometimes suffer from purely legal definitions – which are hard to follow by developers who do not have legal knowledge – and incompleteness in covering relevant principles. In some cases, they are not compatible with recent privacy and security changes in mobile operating systems (OSs).

This paper introduces *App Developers Guide* as a guide catalog considering an engineering view to assist app developers in understanding, following, and applying essential privacy and security principles in smartphone ecosystems. The guide catalog consists of the most relevant privacy and security principles extracted through an intensive literature review considering the relevant national and international regulatory documents. This catalog is supposed to serve as a guide for app developers before, during, and after app design and development phases. It also comprises technical language definitions to make the legal principles more understandable for developers. The contributions resulted from this paper are summarized as follows:

1) extracting and proposing a guide catalog consisting of the most relevant privacy and security design principles in the context of smartphone apps aiming at supporting Privacy-by-Design [15] and assisting app developers in applying good privacy practices before, during and after app design and development phases. The catalog also went through data protection expert discussions to examine its relevance to data protection practices of smartphone apps;
2) extracting the most recent and relevant technical guidelines to assist developers in mapping the identified legal principles to practical privacy and security solutions;
3) providing an understanding of what smartphone apps promise and what they do in reality by considering their privacy policy texts and personal data access patterns.

The rest of this paper is organized as follows: Section II provides an understanding of smartphone ecosystems and gives an insight into the relevant legal privacy principles. Section III introduces and describes the research design including the taken steps for the extraction of *App Developers Guide*. Section IV proposes a classification scheme to map the reviewed privacy principles to technical implementation guidelines based on the characteristics of reviewed principles detected in the literature. Through real-world experiments, Section V then discusses current issues associated with what mobile app developers promise (based on the proposed mapping in this paper) and what they do in reality and it gives insights into the potential revitalization. Finally, Section VI provides conclusions and summarizes this paper.

II. SMARTPHONE ECOSYSTEMS AND PRIVACY PRINCIPLES

To have a better understanding of current smartphone ecosystems, Section II-A provides an overview of the existing stakeholders. Followed by this, the relevant privacy principles with a focus on European law are further discussed in Section II-B.

A. SMARTPHONE ECOSYSTEMS

The term "smartphone ecosystem" comprises smartphones' hardware and software platforms including apps running on top of the platform, as well as infrastructural components such as app markets (e.g., Google Play, App Store) [18]. There are several key elements in a given smartphone ecosystem as follows:

- *Users* are the endpoint of smartphone ecosystems. As the final consumers, services/utilities provided by apps are delivered to users.
- *Smartphones* are multi-purpose devices equipped with sensing and recording capabilities such as camera, microphone, fingerprint recognition, proximity sensors, gyroscope, accelerometer, and more. These are embedded into the hardware made available to apps and the OS. Mobile OSs already embedded mechanisms to control and limit the amount of personal information accessed by users' installed apps. For instance, in Android, apps can request access to the device's resources through permissions. Depending on the resource types, consent from users is required. Android defines four types of permissions[1]: *Normal*, *Dangerous*, *Signature*, and *SignatureOrSystem*. *Normal* level permissions allow access to resources that are considered low-risk, and they are granted during the installation of any package requesting them. The *Dangerous* level permissions are supposed to access resources that are considered to be high-risk. In this case, the user must grant permission. So-called *Signature* level permissions grant access only to packages with the same author. Finally, *SignatureOrSystem* level permissions grant access only to those apps that are in a dedicated folder on the Android system image or that are signed with the same certificate. They are used for special situations where multiple vendors have apps built into a system image and need to share specific features explicitly because they are being built together. Every app has an `AndroidManifest.xml` file that contains information about that particular app (e.g., its name, author, icon, and description). It also provides information about the required permissions that are requested by the developer. In iOS, developers are allowed to gain access to the device's resources by registering their apps via some privacy keys in a property list called *Information Property List* (`info.plist`). Developers are asked to statically declare the intent to access a certain sensitive resource. This declaration includes the privacy key and purpose string (explaining why access to such a sensitive resource is needed by the app) registered in `info.plist`.
- *Apps* are the main source of delivering services/utilities to users such as navigation, e-health, e-learning, transportation, etc. To successfully deliver such services, they evidently need to access certain data types and permissions such as camera, phone number, email address, outgoing calls, etc.
- *Developers* contribute to the mass market (app stores) of apps by developing apps for smartphones, mobile devices, etc.
- *App stores* are rich sources of apps and they directly or indirectly communicate with app developers and users.
- There are also other entities in smartphone ecosystems, such as operators that create and maintain wireless services over cellular networks, third-parties and advertising networks that display targeted/non-targeted ads to users, smartphone manufacturers, and so on.

[1] https://developer.android.com/guide/topics/permissions/overview, Accessed: 09.01.2020

B. RELEVANT LEGAL PRINCIPLES

In early 2016 the EU decided on the GDPR [2]. Since May 25, 2018, it is directly applicable in all Member States. The same date the German BDSG-neu [19] came into force, complementing the GDPR in its opening clauses, which have to be defined on a national level. The GDPR applies "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (Art. 3 (1)). The element of importance here is whether the person whose personal data is being processed, is within the EU or not. In this context, personal data is defined as "any information relating to an identified or identifiable natural person", also called *data subject* (Art. 4 (1)). This definition is rather broad, resulting in difficult legal discussions on whether a specific data type is to be regarded as personal data or not. However, due to the highly personal nature of smartphones, any data collected from them may be classified as personal data as stated in Recital 24 of the Directive on privacy and electronic communications 2002/58/EC (ePrivacy Directive) [20] of the European Parliament and Council: "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms".

This includes not only data like private pictures or messages but also device's identifiers, location or even metadata [21]. Notably, the GDPR still applies if the data is pseudonymized as it is still regarded as personal data. However not if it is anonymized since it is not recognizable from other data (more details in Section IV-B) [21]. Special treatment is conferred to data which is categorized as sensitive data, such as racial or ethnic origin, political opinions, biometric or health data or similar (Art. 9 (1), GDPR). Thus, neither pictures nor metadata are classified as sensitive data, but since they may reveal such, they must be treated with caution [21]. Since the processing of such data would create "significant risks to the fundamental rights and freedoms" of the data subject, the collection and processing of such data types are only allowed under certain exceptions, e.g., explicit consent (Art. 9 (2), GDPR). However, if the processing is disproportionate, the consent is considered to be invalid [21]. Moreover, prior to the consent, users must be provided with clear and comprehensive information about their actions [2], [20], [22]. The consent must be gained before processing personal data (Art. 5 (3), GDPR). Additionally, in order to

be able to make an informed decision, consent must also be specific (to the data that is processed), freely given (data subjects must have the choice to refuse the processing of personal data), and obtained by active choice [21], [23]. Lastly, users must be given the option to easily and effectively withdraw their consent [22]. Special protective measures are also laid on the processing of children's data. Many app stores offer a large assortment of apps targeted at children. However, children are considered to have little or no knowledge of the risks associated with the usage of smartphones. Hence, the processing of children's data is only lawful if the child is over the age of 16 or if consent is given by the holder of parental responsibility and only to the extent it is explicitly given (Art. 8 (1), GDPR). Data controllers are further asked to provide information in an understandable language to children [22]. As throughout this paper certain privacy-related terms are used a lot, for better understanding their definitions are clarified as follows (defined by Art. 4 of the GDPR):

- **Data controller** means the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law.
- **Data processor** means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.
- **Data subject** is an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, etc.

Typically, the data controller is thus the app provider, whereas the app developer is typically a data processor. In cases where the app provider is the same person as the app developer, she is regarded as the data controller. In legal terms, the data controller is the most important entity, since she must guarantee compliance with legislation [21]. If data-driven functionalities such as advertisement networks are integrated into an app, several data controllers might be at place. There might as well exist several data processors, for instance, if cloud services are used, which process personal data [21]. Throughout this paper, the terms ''data subject'' and ''user'' are used interchangeably. The same also applies to ''data controller'', ''data processor'', ''app provider'', and ''app developer''.

In both the EU GDPR and the BDSG-neu several data protection principles are incorporated as a basis [24]. They are defined in Art. 5(1) of the GDPR and are presented in the following:

1) LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Art. 5 (1a) GDPR states that when processing personal data, it should happen in a ''lawfully, fairly and a transparent manner'' towards the data subject. This implies that it should be laid open to what data is collected for what purpose, which systems and processes are used, where data is being transferred, who is legally responsible for data in what phase and how to contact that person [22], [24]. This is highly important as it may help data subjects and supervisory authorities to identify deficits and if necessary, take appropriate actions. Since this is of great importance in the GDPR, a whole chapter (*Chapter 3*, GDPR) has been dedicated to the rights of data subjects. For instance, the right to access and correct personal data, the right to object to the processing of their data, the right to erasure, the right to data portability and the right to object automated individual decision-making are captured here among many other rights (Art. 12-23 GDPR). When it comes to smartphone ecosystems, as part of the principle of transparency, the app provider should clearly inform users about the processing of their data prior to app installation. This information must, however, also be accessible from within the app [22]. Furthermore, it is required to notify users in the case of a data breach, if there is a high risk to the rights and freedoms of users (Art. 34, GDPR). Additionally, users need to get informed on the safeguards, that have been taken into consideration to protect data if it is processed outside of the EU (Art. 13 (1f), Art. 14 (1f), GDPR).

2) PURPOSE LIMITATION

Personal data is suitable to be used in various contexts. The more detailed such data sets become (possibly also through the aggregation with public data) and the more informative value they contain, the more interesting they get for other parties [24]. Therefore, Art. 5 (1b) GDPR limits the collection and processing of personal data to ''specified, explicit and legitimate purposes''. The processing for further purposes, which are incompatible with the original ones, is only granted in specific situations such as archiving purposes for the public interest. (Art. 5 (1b), GDPR).

3) DATA MINIMIZATION

This principle goes hand in hand with the principle of purpose limitation and is especially interesting when dealing with big data applications [24], where huge amounts of personal data are collected to analyze customers. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (Art. 5 (1c), GDPR). It is also closely interrelated to the concept of Privacy-by-Design, which has become an obligation set in Art. 25 GDPR. Hence, it should be analyzed whether the processing of a specific type of personal data is required and if so, to what extent it is necessary, by which entities and persons it should be done, to what extent they should gain control over the data, and over what period of time [24].

4) ACCURACY

Accuracy states that all personal data shall be accurate and kept up to date. Furthermore, every reasonable step must be taken to ensure that inaccurate personal is erased or rectified without delay, in having regard to the purposes for which they are processed (Art. 5 (1d), GDPR).

5) STORAGE LIMITATION

Personal data must be kept in a form which permits the identification of data subjects for no longer than necessary for the purposes for which the personal data is processed. The data may only be stored for longer periods in explicit situations, e.g., for archiving purposes in the public interest (Art. 5 (1e), GDPR). Accordingly, this means not only the deletion of personal records when the data subjects are no longer active, but also the erasure of individual data fields and attributes if they are not strictly needed (anymore) [24].

6) INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. To do so, appropriate technical or organizational measures should be taken into account (Art. 5 (1f), GDPR). This implies that the data being processed must remain intact, complete, up-to-date and that only authorized persons – even with the organization of the data controller – may gain access [24].

7) ACCOUNTABILITY

The principle of accountability requires data collectors to demonstrate how they comply with data protection regulations (Art. 5 (2), GDPR). When personal data is being processed, data collectors are required to carefully document all decision-making procedures with respect to the ongoing data processing such as maintaining specific documentation on what personal data is processed (how, for how long and for what purposes) and conducting data protection impact assessment to tackle data protection issues (more details in Section IV-F)

8) PRIVACY-BY-DESIGN

Although Privacy-by-Design is not a principle under Art. 5(1), the GDPR pays special attention to it as a frequently-discussed concept related to data protection (Art. 25, GDPR). Privacy-by-Design focuses on embedding data protection through the technology design life cycle [15]. In other words, regardless of the purposes that an IT product targets, Privacy-by-Design ensures that a given IT product is designed with privacy as a priority. Privacy-by-Design is also highly connected to the Principle of Least Privilege (PoLP) [25]. According to this principle, ''every program and every user of the system should operate using the least set of privileges necessary to complete the job''. This principle is strongly asking developers/programmers to give apps the minimum number of permissions necessary for providing a certain functionality/service. For instance, a flashlight app simply needs to access the device's sensor to properly deliver its desired functionality. Hence, such an app does not need to access sensitive information, such as contact list, location, phone number, etc. Accordingly, PoLP is directly tied to Privacy-by-Design and ''data minimization'' as well.

III. APP DEVELOPERS GUIDE: RESEARCH DESIGN

This section elaborates on all the steps that were taken into account to extract, compile and provide *App Developers Guide* aiming at assisting app developers in exercising good privacy practices before, during and after designing smartphone apps. Fig. 1 summarizes a high-level diagram regarding the methodological steps of *App Developers Guide*.

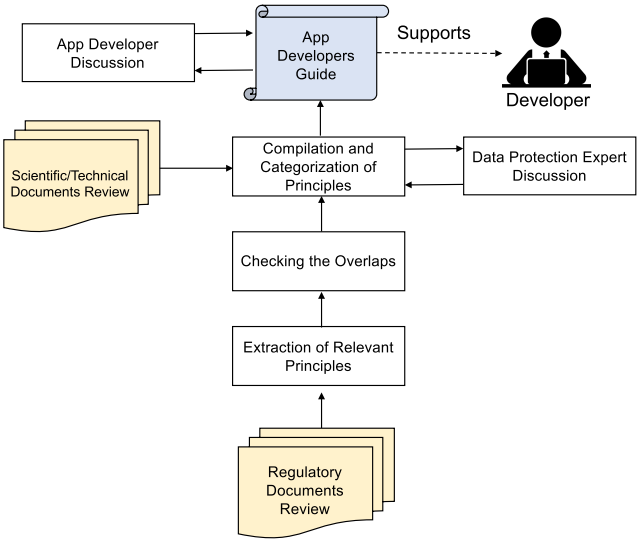

FIGURE 1. Methodological steps of *App Developers Guide*.

In the first phase, a regulatory document review was conducted to develop a preliminary set of relevant principles. For this, guidelines on how to handle privacy and data security in smartphones, published by acknowledged institutions and authorities have been examined. The largest source of suitable publications for the development of privacy and security design principles are the EU institutions. The most important documents are the GDPR and ePrivacy Directive and Regulation [2], [20], [26] by the European Commission, Council and Parliament. Of particular interest is furthermore the ''Article 29. Opinion 02/2013 on Apps on Smart Devices'' [22], a document published by the Data Protection Working Party, as an independent European advisory body on data protection and privacy. As the name of the document suggests, it is a comment on Art. 29 of the Data Protection Directive, explaining in more detail its effects on the processing of personal data by apps on smart devices (in particular smart mobile devices). Other EU recommendations of interest can be found in the ''Guidelines on the Protection of Personal Data Processed by Mobile Applications Provided by European Union Institutions'' [23] which is directed at the EU institutions, developing and distributing their own mobile apps. As they are required to act as role models, these guidelines can also be helpful for other app developers. In particular, they deal with the question of how to process personal data in mobile apps while complying with data protection obligations set out by the EU. Furthermore, two publications by the European Union Agency for Cybersecurity (ENISA) offered advice on how to protect privacy in mobile

environments [21], [27]. The first document is intended for app developers, giving advice on how to design apps in a secure manner. The second one has taken an app developer-centric approach, providing a meta-study on privacy and data protection in mobile apps in compliance with the GDPR.

Besides those supranational institutions, several national bodies have set out their recommendations, as well. For instance, the German Federal Office for Information Security (BSI, German: Bundesamt für Sicherheit in der Informationstechnik) [28] has deeply investigated the functionality of mobile services, considering the possible security risks and it gives advice on countermeasures. Furthermore, the ''Standard Data Protection Model'' authorized and acknowledged by the German Conference of the Independent Data Protection Authorities of the Bund and the Länder [24] has been taken into account. It presents a methodology to assess the efficacy of data protection with respect to European and German federal data protection regulations. It is intended for data controllers, giving advice on how to manage data protection measures enabling supervisory authorities to provide better transparency [24]. Also, the UK Information Commissioner's Office (ICO) ''Privacy in Mobile Apps: Guidance for App Developers'' [29] has been taken into consideration. The ICO is an independent authority in the UK (sponsored by the Department for Digital, Culture Media and Sport), which aims at upholding information rights and promoting ''openness by public bodies and data privacy for individuals''. As the title states, it deals with practical aspects of the protection of smartphone users' privacy by app developers. From outside the EU, ''Privacy on the Go: Recommendations for the Mobile Ecosystem'' [30] from the California Department of Justice has been analyzed. It presents recommendations not only for app developers, but also app platform providers, advertising networks, and others. Other than the guidelines set out by the European countries, it builds on the California Online Privacy Protection Act (COPPA) which first came into force in 2004. Additionally, a workshop summary by the National Institute of Standards and Technology (NIST) of the US Department of Commerce entitled ''Public Safety Mobile Application Security Requirements'' [31] has been examined. It covers the takeaways of the workshop, where experts provided their knowledge on privacy and security requirements for public safety mobile apps. Being developed by the EU institutions, these public safety apps are required to be developed in an exemplary manner. Hence, the document provides useful recommendations for the development of apps in general. Moreover,''Mobile Privacy: A Better Practice Guide for Mobile App Developers'' developed and published by the Office of the Australian Information Commissioner (OAIC) [32] was investigated. The document is aimed at supporting app developers for embedding enhanced privacy practices in their products and services. In addition to these governmental publishers, other sources, i.e., one non-profit organization and one commercial provider of security solutions, have been taken into consideration [33], [34].

Based on the information extracted from the literature review phase, relevant principles were extracted, and the overlaps between them were checked to ease the process of final compilation. Further, technical recommendations and requirements were carefully reviewed, and those were fitting the identified legal privacy and security principles were extracted. It is worth mentioning that, the identified legal privacy and security principles have been revised with the help of data protection experts (with a special focus on the recently adopted GDPR). Finally, the principles and their corresponding technical recommendations went through discussions with a group of app developers in the form of a moderated session. This way, the expert opinion was gathered and helped to improve the understanding of recommendations.

IV. CLASSIFICATION OF PRIVACY PRINCIPLES

In this section, the results of the *App Developers Guide*, including the identified privacy principles and their respective technical implementation guidelines are introduced. As defined in [35], the term classification is used to characterize the systemic properties and forms of interaction. Such a classification provides a well-structured overview facilitating the understanding of workflow as shown in Fig. 2. The following subsections detail each extracted class.

A. PURPOSE LIMITATION AND DATA MINIMIZATION

Mobile apps are constantly sharing data (including sensitive ones) to different parties ranging from remote servers to other apps. It is of particular importance to pay attention to both aspects as the latter is sometimes underestimated by developers. Thus, additional protection and control mechanisms should be anticipated and developed to avoid illegal calls from other apps [34]. The GDPR states that personal data shall be ''collected for specified, explicit and legitimate purposes and not further processed in a manner that is incom-

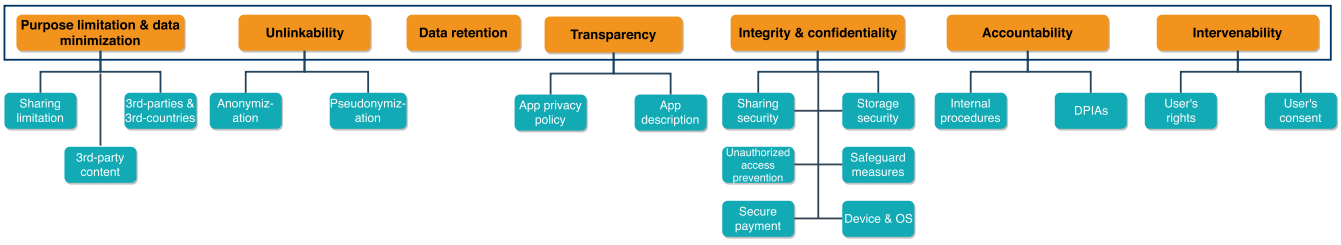

FIGURE 2. Classification of the reviewed legal principles and their mapping to technical implementation guidelines.

patible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89 (1), not be considered to be incompatible with the initial purposes'', Art. 5 (1b). When data is collected from users in mobile app ecosystems, such data has to be considered as personal data as in the meaning of the GDPR. Additionally, the relevant data to the smartphone itself, such as the device's identifier is also categorized as personal data [21]. Therefore, to fully comply with the GDPR Art. 6 (4) (''data processing for incompatible purposes should be avoided unless it is on the basis of a specific set of criteria in the GDPR''), developers must only process data when the app has a specific lawful purpose for doing so. To overcome such challenges, the following sub-principles and their respective technical recommendations need to be considered by developers.

1) SHARING LIMITATION

The transmission of personal data to third-parties must be avoided unless such transfer is necessary for the purpose. Also, developers need to appropriately limit the amount of personal data being shared with other apps. Hence, an app that has been granted permission-protected resources must not leak them to other apps. Moreover, data sharing must be isolated by default unless explicitly specified or otherwise chosen by the user. The following recommendations can be helpful to fulfill this sub-principle:

- *Only data which is required for the proper functionality of the app must be collected and disclosed.*
- *Cryptographic protocols need be initialized to minimize data collection without having data flow to service providers.*
- *Apps must not communicate personal data to a third-party or other apps unless this transfer is aligned with the purpose.*
- *Data sharing with other apps must be restricted, e.g., by implementing an Android Content Provider.*
- *The use of fine location data and/or sharing such data with third-party apps must be minimized and limited to specified purposes.*
- *If an app is intended for children under the age of 13 or if a developer is knowingly collecting personal data from children under such an age, he/she may have additional obligations under federal law.*

2) THIRD-PARTIES AND THIRD-COUNTRIES SHARING

When sharing data with third-parties, the legal standards of the country where the third-party resides plays an increasingly important role. Considering Art. 13 (1f), 14 (1f) of the GDPR, data transfer to other countries is only lawful, where a similar level of protection as provided by the GDPR is guaranteed. Whether this is the case needs to be assessed by the European Commission and can be done on the basis of a country, territory, specified sector, or international organization. Besides these restrictions on where to share personal data, Art. 13 (1f), 14 (1f) require data controllers to adopt appropriate safeguards and means followed by contractual arrangements with the recipient of the personal data approved by the European Commission. The following recommendations can help to fulfill this sub-principle:

- *Rigorous code analysis must be conducted to make sure that apps do not intentionally/unintentionally transfer sensitive data to remote servers and any other external entities.*
- *The use of SMS and MMS as a mean for transferring sensitive data such as security tokens must be as minimized as possible as they might be invaded.*
- *End-to-end secure channel such as TLS must be enforced when sending sensitive information over the internet.*
- *The data received from third-parties must be validated before processing them within an app, including local apps, OS services as well as data received over the network.*

3) THIRD-PARTY CONTENT

Developers are required to be mindful of third-party components used in their app design and development phases. Such components may impose serious privacy and security risks by leaking sensitive data on purpose or by accident [21]. This is highly critical as an app provider or developer (in the role of a data controller) is legally responsible for making sure that third-parties process sensitive data lawfully, fairly and transparently [21]. However, this is quite challenging due to the architectural limitation of existing permission manager models in mobile apps as they do not give the possibility to developers to separately grant sensitive permissions to a given app and its integrated third-party components. The following recommendations can help developers to fulfill this sub-principle:

- *The reliability and authenticity of third-party components (libraries, codes, etc.) must be carefully checked before using them (e.g., by auditing codes and libraries for security issues).*
- *After integrating third-party components, regular security updates must be applied.*
- *Following good privacy practices, developers should use custom keyboards for receiving inputs from users (usernames, passwords, credit card details, etc.) as third-party keyboards may not be reliable.*
- *Whenever third-party servers (outside the EU) are used as a back-end, developers must be aware that the corresponding regulations applied to third-country data sharing practices are enforced.*
- *The overall architectural design of apps should allow developers to replace those third-party components that are either violating data protection principles or not behaving as initially promised.*

B. UNLINKABILITY

Unlinkability is closely tied to anonymization and pseudonymization. Recital 26 of the GDPR defines anonymous information as ''. . . information which does not relate to

an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable''. As it can be inferred from the definition, anonymization and pseudonymization techniques are used to increase the ambiguity of data in case the deletion of personal data is not possible [27]. It is worth mentioning that, as anonymized personal data is not distinguishable from any other type of data, therefore, the legislation is not applied to it. However, this is not the case for pseudonymized data as it is still a subset of personal data as stated by Art. 4 (5) the GDPR. Pseudonymization is defined as ''the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person''.

Depending on the situation and type of personal data that app developers are going to process, they may have to use either anonymization or pseudonymization. For example, in clinical application domains where the tests need to be repeated and compared several times, it is difficult or almost impossible to use anonymization. But pseudonymization may work because it is still possible to link and re-identify different data by having additional information.

1) ANONYMIZATION

Anonymization irreversibly destroys any way of identifying users. In general, there are two different approaches to anonymization. The first approach is based on *randomization* while the second is based on *generalization* [36].

Randomization techniques alter the accuracy of data to destroy the chances of linking personal data to individuals. *Noise addition* is one of the subsets of randomization techniques and its main goal is to change those attributes (in a given data set) that may have an adverse impact on individuals. For instance, a data set of a fitness app that contains users' heartbeat values could be anonymized by randomly adding or subtracting a number between 1 and 10 to the heartbeat records, and then removing the attached name records. This would enable the developer to know the average heartbeat of users (within a margin of error) but would prevent an adversary from learning their real heartbeat values. *Permutation* is another subset of randomization techniques. It consists of shuffling the values of attributes in a table so that some of them are artificially linked to different users. Such swapping ensures that the range and distribution of values remain the same but correlations between values and individuals will not.

Generalization techniques, on the other hand, are based on generalizing users' attributes by altering scales or orders of magnitude, e.g., coarse location permission rather than fine location permission. *K-anonymity* is a subset of generalization techniques and it aims at preventing users from being singled out by grouping them with, at least, k other individuals. In other words, attributes are shared by k users. Therefore, it should be no longer possible to single out an individual within a group of k users. *L-diversity* is an extension of k-anonymity and it tries to minimize the frequency of equivalence classes with poor attribute diversity so that an attacker with background knowledge on a specific user is left with a remarkable doubt.

2) PSEUDONYMIZATION

Pseudonymization substitutes the identity of users in such a way that additional information is required to re-identify users. *Hashing* and *tokenization* are widely-applied subsets of pseudonymization techniques [36].

Hashing is a form of pseudonymization that exploits mathematical algorithms to transform personal data into fixed-length obscure alphanumeric strings, known as hash values. The hashing of plain text into hash values is intended to be a one-way data transformation process, as a hashing algorithm is not reversible. The main goal of hashing is to validate plain text inputs by hashing a plain text input value using a defined hashing algorithm. The generated hash value is then checked against a previously calculated and stored hash value. If the hash values are the same, it is likely that the plain text input and previously hashed plain text are the same. Such a technique should be used to protect passwords stored in databases, i.e., app developers should always store password hash values instead of plain text passwords.

Tokenization is widely used in payment processing solutions such as Apple Pay[2] or PayPal.[3] In such techniques, a piece of data is replaced with a unique token that acts as a stand-in which can be used to retrieve the original value. For instance, a user's credit card number is represented by a token. When making a purchase, the merchant receiving payment only has access to the token, rather than the actual credit card number. Since Apple Pay knows the relationship between the token and credit card number, it can take the transaction information, retrieve the credit card number based on the token, and process it like a normal purchase.

C. DATA RETENTION

Developers are required to be clear about the retention period and they should limit it only to the amount of time needed to provide the desired service. Thus, any personal data should be instantly deleted (including stored data on the remote servers) after the expiration of the retention period. Additionally, any confidential data including users' credentials, such as passwords, credit card details, etc. must be successfully deleted upon app uninstallation from the device and any other storage medium.

D. TRANSPARENCY

Transparency is one of the key principles of the GDPR (see Section II-B1). When it comes to smartphone apps, developers are required to be clear and explicit about their

[2]https://www.apple.com/apple-pay/, Accessed: 09.01.2020
[3]https://www.paypal.com/, Accessed: 09.01.2020

data access, collection, process, and transfer practices. Also, developers are responsible for determining the internal rules once data collection purposes change. This also entails the communication of such changes to users before they come into effect. Furthermore, any incident regarding users' personal data shall be promptly communicated to them, e.g., in case personal data breach happens, users and the respective Data Protection Authority must be immediately informed (this also includes the potential occurred risks and possible countermeasures). To further raise users' awareness and attention, using real-time contextual information (audio and video) is highly recommended. Ultimately, to further improve transparency, a clear, comprehensive, understandable, and legitimate privacy policy text should be accessible to users. It is important to note that, if developers and data controllers are the same entity, then clear instructions must be provided to users enabling them to understand how they can contact developers to file compliant, withdraw consent, ask for the record of personal data collection, etc. Two relevant sources of providing transparency-enabling information to users are app privacy policy and app description (both published on app markets).

1) APP PRIVACY POLICY

An app privacy policy is a statement or a legal document that gives information about the ways an app provider collects, uses, discloses, and manages users' data. An honest app provider is required to fulfill the following privacy policy principles.

a: DATA COLLECTION

Smartphones contain a considerable amount of sensitive personal data. Hence, app developers must only collect and process the data that is strictly necessary (data minimization) for the purposes for which it has been collected (purpose limitation). The legal foundation is set in Art. 5 (1) and Art. 6 GDPR. While the former article states the general principles of processing personal data, the latter indicates when processing is lawful, including when consent is given, when it is necessary for the performance of a contract or compliance with a legal obligation, to protect vital interests of user or another natural person, and when processing is necessary for a task carried out in the public interest or for legitimate interests pursued by the controller or by a third-party. However, this applies if and only if such interests do not override the interests or fundamental rights and freedoms of users. Monetizing purposes, i.e., advertising, are not classified as necessary and therefore need to be based on another legal ground. Similarly, the processing of data to develop new features and services is not specific enough to comply with this section [21].

b: CHILDREN PROTECTION

According to the GDPR, information related to children must be treated with the utmost caution, as children ''may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing of personal data'' (Rec. 38 GDPR). This implies that services targeted at children are obliged to provide information in clear and plain language that children can understand easily (Rec. 58 GDPR). Art. 8 GDPR defines that the processing of children's data is only lawful where the child is at least 16 years old. The data processing of younger children is only legitimate if and to the extent, a parent or legal guardian has given consent. However, this article has an opening clause, allowing member states to set a lower age for those purposes, yet not below 13 years.

c: THIRD-PARTY SHARING

Given the extensive data collection and sharing practices in mobile apps, the principle of transparency is of great importance for users to understand how their data is being used. Furthermore, the significance of this aspect is even greater for smartphone apps, since third-party components (that might collect data as well) are often integrated into an app's development phase. The legal basis lies in Art. 13 (1e) GDPR, stating that the recipients or categories of recipients of personal data must be revealed to users.

d: THIRD-COUNTRY SHARING

When sharing data with others, not only the technical security level is of importance, but also the legal standards of the country where the third-party resides. This is of particular importance for the EU citizens since many countries outside the EU may have lower privacy protection regulations. Therefore, the GDPR dedicates its *Chapter 5* to provisions on transfers of personal data to third-countries or international organizations. The transfer of data to other countries is only lawful, where a similar level of protection as provided by the GDPR is guaranteed. In fact, the protection of data travels with the data itself. Thus, if app providers share personal data with servers located outside the EU, they shall mention in their privacy policy text how they deal with third-country data sharing practices.

e: DATA PROTECTION

As mobile apps may access sensitive information, the loss or theft of a smartphone, as well as data transfer, impose extreme risk on users' privacy. The next principle, therefore, deals with data protection. This concern is met in the GDPR in Art. 32, which states that the data controller must implement appropriate technical and organizational measures to ensure appropriate security. This is of particular importance in smartphone ecosystems since they are typically linked to a huge amount of data transfer. The aspect of data protection is also closely correlated with Privacy-by-Design.

f: DATA RETENTION

The retention of data is a delicate issue, as app providers may want to retain data as long as possible to enable future transactions and purposes. However, this is often not in the interest of users, particularly not for sensitive data as available in smartphones (e.g., personal information from dating

apps or health data from fitness apps). To protect users, the principle of data minimization and storage limitation in combination with transparency take effect. Accordingly, Art. 13 (2), 14 (2) of the GDPR state that the data controller must inform users for what period their data is retained. This is strictly required as users have ''the right to be forgotten'', which is set in Art. 17 of the GDPR. This article states that users do not only have ''the right to obtain from the controller for the erasure of personal data'', but also data controller must erase personal data if it is ''no longer necessary in relation to the purposes for which it was collected'' (principle of purpose limitation) and if users withdraw consent. However, in some cases, the retention of data for a certain period is lawful, e.g., if there exists a legal obligation to do so (e.g., the German Fiscal Code requires companies to store accounting records for a period of 6 to 10 years).

g: USER'S CONTROL

As previously stated, the objective of the GDPR is to enable users to retain control over their personal information (user's control). Accordingly, the whole *Chapter 3* of the GDPR is dedicated to the rights of users. The most important rights are the right to information and access to personal data; the right to rectification; the right to erasure (see the previous principle); the right to restriction of processing; the right to data portability; and the right to object and automated individual decision-making. By Art. 13 (2), 14 (2) of the GDPR, app providers are required to provide these rights to users to ensure fair and transparent data processing (principle of lawfulness, fairness and transparency Art. 5 (1a)).

h: PRIVACY POLICY CHANGES

To further ensure lawful, fair, and transparent processing of data, app providers should inform users in a transparent and understandable way about privacy policy changes. This obligation is derived from Art. 12 of the GDPR.

i: PRIVACY BREACH NOTIFICATION

Besides Art. 12 GDPR, which lays the basis of informing users, this principle is based on Art. 34 GDPR where it is stated that if a data breach occurs that results in a high risk to the rights and freedoms of users, the data controller must inform users without undue delay. In this notification, the data protection officer must be named and likely consequences of the data breach as well as the measures taken to mitigate the effects are described. The same is applicable for the notification of the supervisory authority, which must be done not later than 72 hours after the detection of a personal data breach.

j: APP-FOCUSED

This principle is not particularly named in the GDPR. However, it can be subsumed under the principle of lawfulness, fairness, and transparency. Sometimes a privacy policy is not exclusively written for a specific app, but multiple services provided by the same app developer (data controller). For instance, Sunyaev *et al.* [37] identified five reoccurring scopes of privacy policies, namely privacy policies for a single app, for multiple apps, for a back-end app, for a developer homepage or for all developer services. They also found that several privacy policies of apps did not have an app-related scope at all. This was also triggered in our data protection expert discussions as an important principle to be considered to examine the extent to which an app privacy policy focuses on the app's data protection practices (e.g., sensitive permission requests).

k: PURPOSE SPECIFICATION

This principle is closely related to the data collection principle. While the focus of data collection is on what data is collected, this principle refers to the clear statement of data collection purposes. Besides the legal basis for data processing, app providers are required to specify data collection purposes according to Art. 13 (1c), 14 (1c) GDPR. This is not only important under the aspect of lawfulness, fairness, and transparency, but also the principle of purpose limitation to prevent exploitation of personal data for other use cases.

l: CONTACT INFORMATION

Contact information is linked to the principle of lawfulness, fairness, and transparency. According to Art. 13 (1a), 14 (1a) GDPR, users have the right to be informed about the actual identity of data collectors, i.e., app providers. This includes the name of the app provider, if it is a legal entity, its legal representatives as well as its postal address. The latter must be provided to give users the possibility to file a formal complaint.

2) APP DESCRIPTION

The app description is another element that can enable app providers to generate transparency-supporting information to users. The app description is an app market optimized product definition where app developers describe the main characteristics and details of their apps. The app description is a very relevant piece of information that can play an important role in a user's decision-making process. Therefore, developers need to be clear and concise when explaining how their app works and why people need it. It is also highly important to make a logical connection between an app description and the claimed permission declaration list by developers on the app market (e.g., Google Play Store). For instance, if the app is a restaurant finder and it requests to access the user's contact list, this should be clear in the app description to a certain extent by adding sentences like ''*share your favorite restaurant with your friends!*''. This would allow developers to follow best transparency practices as app description should be written in such a way to enable users to grasp the fundamental services/utilities offered by the app. This way, users can make better informed privacy decisions by comprehending the rationale behind requesting certain sensitive permissions.

E. INTEGRITY AND CONFIDENTIALITY

Art. 5 (1f) of the GDPR states that, ''personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (*integrity* and *confidentiality*)''. Developers must make sure that the app's integrity is preserved intact by checking resources for potential modifications. One way is to restrict writing and modification permissions. In addition, all the developer's features should be disabled including debugging privilege [38]. To avoid reverse engineering (or to make it harder), data encryption and code obfuscation mechanisms should be established. Also, developers must make sure that the app's confidentiality is ensured. One way is to offer strict and secure authentication processes. Detecting and mitigating vulnerabilities are also essential to protect users against external factors (malware and hacking [39]). The following subprinciples can help to ensure integrity and confidentiality:

1) SHARING SECURITY

Potential sources of private data leakage should be anticipated and protected by developers. This also comprises caches and temporary storage, including address books, gallery files, etc. which are a possible source of privacy leakage. A typical example here is unauthorized access to pictures tagged with users' location allowing information to be shared in unintended ways. Developers are strongly recommended to assume that any kind of shared storage is untrusted. This way, storing any unencrypted cached data in such a readable directory should be avoided.

2) STORAGE SECURITY

Enforced by the GDPR Art. 5 (1e), the implementation of appropriate technical and organizational measures to safeguard the rights and freedoms of users is highly important. Hence, app developers have to adopt and apply up-to-date protection and encryption mechanisms for data storing purposes. This is mainly because insecure storage is not only a risk factor when the device is stolen, but also when another app accesses unencrypted raw data [34]. To ensure a good protection level, storing and processing sensitive data on the server-side is preferred than the client-side (with the maximum level of protection ensured on the server-side). Storing any sensitive data such as users' credentials, location information, etc. on the device's storage in an unencrypted form must be avoided.

3) UNAUTHORIZED ACCESS PREVENTION

To enhance trust between client-server communications, unauthorized access prevention is essential. This means that the user (who is running an app) should be securely authenticated through appropriate authentication mechanisms. The following considerations need to be taken into account to ensure such measures:

- *Provisioning plays a critical role as apps need to implement secure provisioning of cryptographic keys to a set of devices corresponding to a user. This provisioning includes device registration and/or push notification registration that would enable users to have multiple devices registered.*
- *Storing passwords in cache, logs or app binary must be avoided.*
- *Since client-side security controls are capable of being invaded, authentication and authorization controls should be implemented on the server-side. Also, in case passwords are stored locally on the device, it is necessary to use strong encryption and key-store mechanisms provided by the OS.*
- *In case a password-based authentication mechanism is adopted, a strong password policy should be enforced, considering length, special characters, password duration, etc.*
- *Appropriate measures must be enforced to avoid brute-force attack against authentication controls, e.g., questions about the user's profile, informing user once a failed login attempt is detected and enforcing account lockout for a certain time frame.*
- *For apps accessing and processing highly sensitive data, e.g., health data, it is essential to implement additional authentication controls. For this, unreliable channels such as voice mails and phone numbers must be avoided.*

4) SAFEGUARD MEASURES

Safeguard measures are an indispensable part of app design, development, and maintenance phases. To avoid situations in which an insecure mobile interface may compromise users' privacy and may lead to unauthorized access to the device, the following recommendations need to be considered:

- *Both static and dynamic code analysis techniques [40] must be adopted to detect potential security and privacy flaws.*
- *Weak encryption algorithms with short key lengths must be avoided [41].*
- *Since cached data are normally stored on the device, such data could possibly be transferred to remote locations and misused. Thus, they must only be used in HTTPS connections.*
- *Vulnerability management is an imperative part of an app maintenance phase. A proper vulnerability management mechanism must be followed to ensure that users are informed in a timely manner to install new updates as soon as provided.*
- *The final version of an app's code (ready-to-publish version) must be clean (e.g. it must not contain test methods).*

5) SECURE PAYMENT

Many apps are nowadays supporting and offering in-app purchasing which is basically referring to buying goods and services from inside an app on a smartphone or tablet by

stimulating users for upgrades to the paid version by offering additional services. Such a feature enables developers to provide their apps for free. Therefore, developers are responsible for ensuring secure payment mechanisms in their apps by considering the following recommendations:

- *Appropriate control mechanisms should be anticipated to detect suspicious usage patterns in paid-based services. When there is a remarkable change in a user's location, profile, etc., then using re-authentication controls is strongly recommended.*
- *Whenever there is a cost implication relevant to a certain app functionality, users must be adequately and transparently informed, e.g., through easy-to-understand messages.*
- *In-app payment measures must be designed and developed based on the OS/device vendor guidelines.*

6) DEVICE AND OS

Security and privacy measures are not always tied to the app itself, but also the device and OS as the main operating platform for designing, implementing, and embedding security and privacy protection measures. In fact, based on their features, they may enable/limit developers to implement certain protection mechanisms. Thus, it is highly important to take the following recommendations into account:

- *Using outdated components that are no longer supported by the device's and/or OS's vendor must be avoided.*
- *When asking for sensitive inputs from users, auto-correction and auto-suggestion, as well as cut, copy and paste functionalities must be disabled.*
- *Screen captures for app interfaces that may contain sensitive data must be avoided, e.g., banking apps.*
- *Input field masking must be used for entering passwords.*
- *For apps dealing with highly sensitive data (health-based apps, banking apps, etc.), it is necessary to request for user re-authentication when the app state changes, e.g., changing state from running in the background to running in the foreground.*
- *Accessing sensor-related data such as microphone, GPS, camera, body sensor, etc. must be minimized. Such data must not be collected automatically.*
- *Apps need to be executed within the users' privilege (root access is not acceptable).*

F. ACCOUNTABILITY

Accountability is one of the key principles of the GDPR and it requires app developers to demonstrate how they comply with data protection regulations. This includes careful documentation of all decision-making procedures with respect to the ongoing data processing and conducting Data Protection Impact Assessments (DPIAs) to tackle data protection issues.

1) INTERNAL PROCEDURES

When personal data is being processed, app developers are required to carefully document all decision making procedures with respect to the ongoing data processing such as maintaining certain documentation on what personal data is processed (how, for how long and for what purpose). The following recommendations can help to achieve this goal:

- *A security report handling point (address) must be implemented and maintained aiming at enabling users to contact app developers/providers conveniently.*
- *All the required procedures must be anticipated and established in case a data breach happens (including a communication channel to react to reports on security and privacy issues).*
- *Following best privacy and security practices, developers must document all privacy and security-relevant policies, processes, operations and testing corresponding to their developed apps. This also includes the documentation of risk assessment and management procedures, compliance with regulations and requirements (e.g., the GDPR), a record of users' consent, objections, contracts with external service providers and third-parties from which the data is collected or transferred to, etc.*

2) DPIAs

As stated by Art. 35 GDPR, DPIAs are a set of processes that can help to identify and minimize data protection risks. Due to the sensitive nature of personal data accessed, collected, processed, and transferred by mobile apps which is likely to result in a high risk to individuals, app providers are required to do DPIAs. Although different DPIAs methodologies have been proposed [42]–[45], this paper mainly focuses on [43] which is in turn based on the GDPR. In principle, DPIAs comprise three main elements, including preparation, evaluation, and reporting and safeguards. In the preparation step, app providers first determine whether DPIAs are needed. Accordingly, a list comprising incidents when DPIAs are necessary should be established including exempt data processing types. Essential questions that need to be answered here are:

Q1: *What is the target of the DPIAs evaluation? Describe the system, identify relevant data and data flows.*
Q2: *Which actors are involved in the systems? What roles and permissions do these actors have?*
Q3: *Which data flows are present? How do actors interact with them?*

In the evaluation step, app providers need to identify the protection goals, potential attackers, stimulants, objectives, and evaluation criteria. Afterward, the risk evaluation is carried out. In the final step, i.e., reporting and safeguards, a concrete plan for risk management needs to be prepared and established (based on the risk evaluation results). This is also required by Art. 35(7d) GDPR as DPIAs must contain measures to remedy the risks identified, including safeguards, security mechanisms, and measures to protect personal data.

G. INTERVENABILITY

Intervenability demands data collectors to make sure that users are granted their essential rights. Intervenability is also highly connected to the user's consent as any data processing must be based on that.

1) USER'S RIGHTS

The GDPR defines the user's rights as the right to be informed (Art. 15), the right of access (Art. 15), the right to rectification and erasure (Art. 16, 17), the right to restrict processing (Art. 18), the right to data portability (Art. 20), the right to object (Art. 21), and the rights in relation to automated decision making and profiling (Art. 22). Hence, developers should carefully take these rights into consideration while designing apps. In fact, the overall architectural design of apps should allow users to practice these rights [21]. To address this principle, the following recommendations can be helpful:

- *While users are interacting with the app's interfaces, they should be given a chance to learn and practice their rights (access, rectification, erasure, giving and withdrawing consent, and portability). Also, developers must embed mechanisms to enable users to understand where to get help for their questions or problems.*
- *Inessential personal data must not be asked. Users must be enabled to delete personal data where appropriate.*
- *Users must be able to change authentication tokens (e.g., passwords). Also, they must be able to disable unwanted push notifications.*
- *Users must be clearly informed in case of an app's functionality limitation due to the permission request rejection.*
- *Users must be able to change the pre-configured "privacy-by-default" setting.*

2) USER'S CONSENT

For any personal data processing request, the user's consent must be asked. Such processing will be invalid if developers fail to ask for the user's consent [21]. A typical issue with a consent request is the vagueness of such a request. In fact, developers sometimes provide blurry information concerning the purposes of data processing. Therefore, users are not well-informed of the potential negative consequences of giving their consent. Hence, developers should essentially avoid putting pressure on users (take it or leave it approach) [21], [23]. The following recommendations can be of help for an efficient user consent request procedure:

- *Whenever any data collection, sharing and processing take place, users must be adequately and explicitly informed. For such purposes, developers must also clarify what kind of personal data will be collected from a user; who will be the potential recipients of data; where data will be hosted and stored and for how long. Additionally, developers are required to make sure that they are not collecting more types of data than actually needed.*
- *Developers must enable users for consent withdrawal at any time requested by them. It is important to inform users about the potential consequences of revoking consent in terms of an app's functionality.*
- *Developers are required to maintain a record of a user's consent concerning the processing of his/her personal data from time to time to make it available upon request.*
- *Asking for a user's consent for processing his/her personal data must be separated from asking consent for other aspects of services offered by developers.*

V. DOES WHAT APP DEVELOPERS PROMISE MATCH REALITY? A CASE STUDY ON ANDROID HEALTH APPS

To investigate the compliance of mobile apps with respect to the extracted privacy policy principles (see Section IV-D1), a case study was conducted to analyze the extent to which the promises made by app developers in app privacy policies match the actual actions done by them. For this case study, the top 20 Android health apps on the Google Play Store were selected. Such a selection is rationalized as follows: (1) Such apps are sometimes underestimated by users. As compared with other popular app categories such as *Lifestyle*, users are not well-aware of the negative consequences of using privacy-invasive health apps; (2) As a result of the extreme proliferation of gadgets and physical activity trackers (such as FitBit), users are currently surrounded by such technologies. Such a technological trend is highly dependent on wireless communications between gadgets and smartphones (i.e. health/fitness-based apps) that may impose privacy risks [46]; (3) In contrast to other general-purpose app categories, health apps are directly dealing with special users' sensitive data such as body sensors which are classified as highly sensitive (Art. 4(13), (14), (15) and Art. 9 and Recitals (51) to (56) of the GDPR) [2].

In the following (as shown in Fig. 3), the analysis results regarding the promises (made in privacy policy texts by developers) and actions (permission usage in reality) on this selected set of apps are discussed.

A. STEP 1: PROMISES (PRIVACY POLICY) ANALYSIS

The privacy policy text of each app in the data set was investigated to infer the coverage of each privacy policy principle presented in Section IV-D1. As can be seen in Table 1 and detailed in Fig. 4, there is a lot of incidents (92) shown by × where the apps failed to mention how they comply with the identified privacy policy principles (principles are shown by P1–P12 in Table 1). As the analysis shows, in several instances, developers failed to clarify the compliance of data protection practices of their apps with different principles. For instance, "Privacy Policy Changes" (12 apps failed), "Third-Country Sharing" (9 apps failed), "Contact Information" (9 apps failed), and "Data Retention" (9 apps failed) are the least covered principles, and no apps covered "Privacy Breach Notification" at all. On the other hand, the most covered principles are "Data Collection" (17 apps covered),

TABLE 1. Coverage of privacy policy principles by the top 20 apps within the *Health & Fitness* category: no coverage (×), coverage (✓).

App #	App ID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
1	com.sec.android...	✓	×	×	×	✓	×	✓	×	×	✓	×	✓
2	com.google.and...	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×
3	com.sillens.sh...	✓	✓	✓	✓	✓	×	✓	✓	×	✓	×	✓
4	cc.pacer.and...	✓	✓	✓	×	×	×	×	×	×	✓	✓	×
5	com.myfitness...	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓
6	pedometer.step...	✓	×	×	×	×	×	✓	×	×	✓	×	×
7	com.stt.android	✓	✓	✓	✓	✓	×	✓	×	×	✓	✓	✓
8	com.fitness...	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓
9	com.fitbit...	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓
10	com.nike.plusgps	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
11	com.runtastic...	✓	×	✓	×	✓	✓	✓	✓	×	×	✓	×
12	com.popularapp...	✓	×	×	×	×	×	×	×	×	×	×	×
13	com.popularapp...	×	×	×	×	×	×	×	×	×	×	×	×
14	si.modula...	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
15	com.playsimple...	×	×	×	×	×	×	×	×	×	×	×	×
16	com.mapmyrun...	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓
17	com.macropinch...	✓	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓
18	com.fitness22...	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×
19	com.endomondo...	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓
20	comm.cchong...	×	×	×	×	×	×	×	×	×	×	×	×

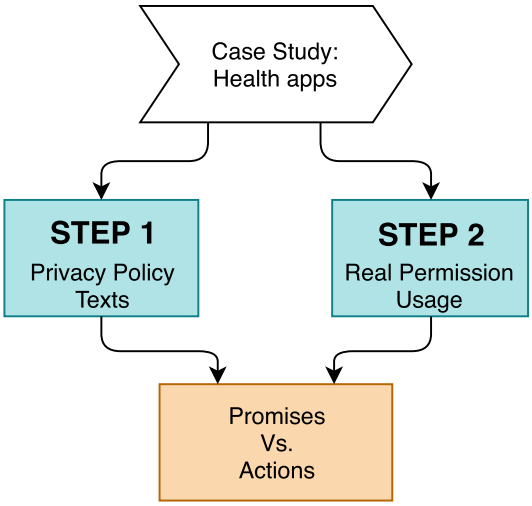

FIGURE 3. High level overview of the promises vs. actions analysis of Android apps.

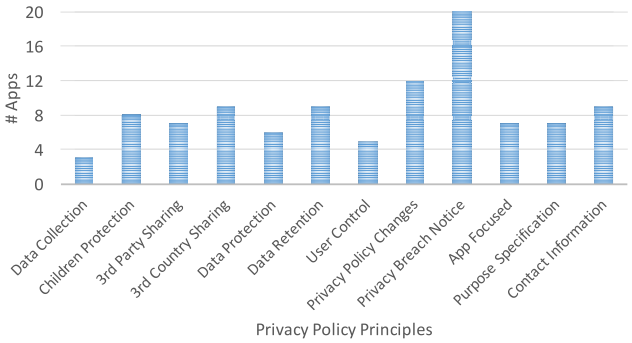

FIGURE 4. Number of apps failed to comply with the identified app privacy policy principles.

"User's Control" (15 apps covered), and "Data Protection" (14 apps covered), respectively.

The relation between sensitive permission requests by apps within the data set and their privacy policy notice was investigated to infer whether or not app developers claim in their privacy policies that they are going to use certain sensitive permissions. As shown in Table 2, a great number of incidents (52) was found that shows app developers have failed to clarify the need for requesting certain sensitive permissions in their written privacy policy texts (shown by×).

B. STEP2: ACTION (REAL PERMISSION USAGE) ANALYSIS

We monitored the permission access patterns of apps within our data set. The apps were installed on several devices that had a pre-configured data capture tool described in [47], [48] to record API accesses from the OS. The collected logs were then analyzed and interpreted to determine apps permission access patterns. Next subsection elaborates on the identified mismatches found between *STEP1* and *STEP2*.

C. IDENTIFIED MISMATCHES BETWEEN PROMISES AND ACTIONS

Fig. 5 illustrates and compares the number of apps that failed to specify the need for requesting sensitive permissions in their privacy policy texts, but accessed those permissions in reality (blue bar chart) and apps who clarified the need for requesting sensitive permissions and accessed those permissions (green bar chart). Both cases are problematic from a privacy perspective. The former shows that app developers do not tend to rigorously clarify the need for permission requests in their privacy policy texts, and in parallel, they request to access those permissions in reality. This indicates that what they promise in privacy policy texts does not necessarily match what they do. The investigation shows that for

TABLE 2. Purpose specification of permission requests in app privacy policy text: clarified in the policy: ✓, not clarified in the policy:×, not using that permission: N.

App #	CAMERA	SMS	CONTACTS	LOCATION	PHONE	AUDIO	SENSOR
1	×	×	✓	✓	×	×	✓
2	N	N	✓	✓	N	N	✓
3	×	N	×	N	N	N	×
4	×	N	✓	✓	×	N	✓
5	×	N	×	✓	✓	N	✓
6	N	N	×	N	N	N	N
7	N	N	N	✓	×	N	N
8	×	N	×	✓	N	N	N
9	×	×	✓	✓	✓	N	N
10	×	N	✓	✓	✓	×	✓
11	N	N	✓	✓	N	×	✓
12	N	N	N	N	×	N	N
13	N	N	×	×	N	×	N
14	×	N	×	✓	✓	N	×
15	×	×	×	×	×	×	×
16	×	N	×	✓	×	N	N
17	×	N	N	✓	×	×	✓
18	×	N	N	✓	N	N	N
19	N	N	✓	✓	✓	N	✓
20	×	N	×	×	×	N	×

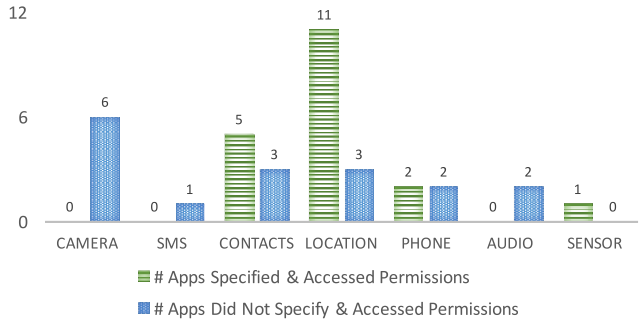

FIGURE 5. Identified mismatches between what apps promise and what they do.

all the analyzed permissions (except BODY_SENSOR) apps are not fully honest in their privacy policy texts, however, they access those permissions in reality. As an example of such permission accesses, we can refer to CAMERA (6 apps), CONTACTS (3 apps), LOCATION (3 apps), PHONE_STATE (2 apps), RECORD_AUDIO (2 apps), and SMS (1 app). The behavior of the second group of apps (green bar chart) is not aligned with the "data minimization" principle. Since in this experiment the apps were not being used (they were in idle mode), accessing such sensitive permissions is not well-justified. This is mainly because apps are supposed to be task-specific (accessing permissions when needed). But in this case, the accelerometer and step detector sensors were not active. Such resource accesses indicate the potential violation of Art. 5 (1(c)) of the GDPR which states that "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimization)". In addition, this is also not aligned with the PoLP [25] which indicates that "every program and every user of the system should operate using the least set of privileges necessary to complete the job".

D. DISCUSSION

The results of this case study confirm that models on privacy policy practices of mobile apps are problematic and regulations become necessary when users do not have the chance to get correct and full information about data collection practices of apps. Thus, it is argued that app developers should carefully specify the need for requesting sensitive permissions in their privacy policy texts. Additionally, app privacy policies need to be severely revisited by their developers as it was observed that there is a substantial number of privacy policies that do not focus on apps' data sharing and collection practices, rather unrelated contents. By simplifying access to data protection goals and principles of smartphone apps, the presently *App Developers Guide* can potentially assist mobile app developers in providing more privacy-friendly services considering the whole life cycle of apps.

VI. CONCLUSION

In this paper, the importance of app developers' privacy awareness was studied. App developers were provided with contributions to design privacy-friendly mobile apps. Based on intensive regulatory document examinations, security- and privacy-friendly app design guidelines were presented aiming at assisting developers in following good privacy and security practices before, during, and after app design and development phases. The results revealed that there is still a significant difference between what app developers promise (in app privacy policy texts) and what they do in

reality (real permission usage). By structuring mobile apps' privacy and security principles into a technical guide catalog, the results achieved from this paper can support app developers to comprehend, adopt and apply regulation-friendly mobile app design practices.

The achieved results must be interpreted with caution and a number of limitations should be borne in mind. Since this research was conducted in Europe, the most focus was on EU-relevant legislation and the importance of their adoption by mobile app developers. Moreover, the data may contain an implicit bias toward relevant EU privacy regulations and attitudes. While the data capture tool measures static permission declaration and actual use during run-time, it will be difficult to estimate the reasons for and intentions behind the particular permission use. Therefore, not all permission uses may relate to an actual privacy risk. Furthermore, since both app's versions and privacy policy texts get updated regularly, reproducibility is challenging in such a setting. Therefore, it will be difficult to re-create the exact test setting. Additionally, the examined app set was mainly taken from the most downloaded apps on the Google Play Store as a very small subset of the millions of apps available in various app markets. A more extensive case study could provide more insights into the validity of the results. However, as the top 20 apps are usually judged as a measure of the app downloads on app markets [49], it can be argued that the findings may exert to the apps with the greatest impact on users.

REFERENCES

[1] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg, "A multilateral privacy impact analysis method for Android apps," in *Privacy Technologies and Policy*, M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, and A. Bourka, Eds. Cham, Switzerland: Springer, 2019, pp. 87–106.

[2] *Eu General Data Protection Regulation*. Accessed: Jan. 10, 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/txt/html/?uri=celex:32016r0679

[3] *Eu-U.S. Privacy Shield*. Accessed: Aug. 12, 2018. [Online]. Available: https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/

[4] I. Shklovski, S. D. Mainwaring, H. H. Skuladottir, and H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," in *Proc. the 32nd Annu. ACM Conf. Hum. Factors Comput. Syst. (CHI)*, Toronto, ON, Canada, 2014, pp. 2347–2356.

[5] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "'Little brothers watching you': Raising awareness of data leaks on smartphones," in *Proc. 9th Symp. Usable Privacy Secur.*, New York, NY, USA, 2013, pp. 12:1–12:11, doi: 10.1145/2501604.2501616.

[6] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst. (CHI)*, Paris, France, 2013, pp. 3393–3402.

[7] S. Rosen, Z. Qian, and Z. M. Mao, "AppProfiler: A flexible method of exposing privacy-related behavior in Android applications to end users," in *Proc. 3rd ACM Conf. Data Appl. Secur. Privacy*, New York, NY, USA, 2013, pp. 221–232, doi: 10.1145/2435349.2435380.

[8] K. Crager, A. Maiti, M. Jadliwala, and J. He, "Information leakage through mobile motion sensors: User awareness and concerns," in *Proc. 2nd Eur. Workshop Usable Secur.*, 2017, pp. 1–15.

[9] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, New York, NY, USA, 2014, pp. 951–960.

[10] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security APIs," *IEEE Secur. Privacy*, vol. 14, no. 5, pp. 40–46, Sep. 2016, doi: 10.1109/MSP.2016.111.

[11] V. F. Taylor and I. Martinovic, "To update or not to update: Insights from a two-year study of Android app evolution," in *Proc. the ACM Asia Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2017, pp. 45–57, doi: 10.1145/3052973.3052990.

[12] H. Peng, C. Gates, B. Sarma, N. Li, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Using probabilistic generative models for ranking risks of Android apps," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2012, pp. 241–252, doi: 10.1145/2382196.2382224.

[13] K. Marky, A. Gutmann, P. Rack, and M. Volkamer, "Privacy friendly Apps-making developers aware of privacy violations," in *Proc. Innov. Mobile Privacy Secur. (IMPS) Workshop*, 2016, pp. 46–48.

[14] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos, "Permission evolution in the Android ecosystem," in *Proc. the 28th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, New York, NY, USA, 2012, pp. 31–40, doi: 10.1145/2420950.2420956.

[15] A. Cavoukian, "Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph. D," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 247–251, May 2010, doi: 10.1007/s12394-010-0062-y.

[16] M. Hatamian, S. Pape, and K. Rannenberg, "Esara: A framework for enterprise smartphone apps risk assessment," in *ICT Systems Security and Privacy Protection*, G. Dhillon, F. Karlsson, K. Hedström, and A. Zúquete, Eds. Cham, Switzerland: Springer, 2019, pp. 165–179.

[17] N. Momen, M. Hatamian, and L. Fritsch, "Did App privacy improve after the GDPR?" *IEEE Secur. Privacy*, vol. 17, no. 6, pp. 10–20, Nov. 2019.

[18] X. Wei, "Understanding and improving the smartphone ecosystem: Measurements, security and tools," Ph.D. dissertation, Univ. California, New York, NY, USA, 2013, Art. no. 3610966.

[19] *Bundesdatenschutzgesetz (BDSG)* Accessed: Jan. 10, 2019. [Online]. Available: http://www.gesetze-im-internet.de/bdsg_2018/

[20] *Directive 2002/58/ec of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*, Official Journal of the European Communities, 2002, pp. 37–47.

[21] *Privacy and data protection in mobile applications. a study on the app Development Ecosystem and the Technical Implementation of GDPR*, ENISA, Heraklion, Greece, 2017.

[22] *Article 29. Opinion 02/2013 on apps on Smart Devices. 00461/13/en wp 202*, Data Protection Working Party, Brussels, Belgium, 2013.

[23] *Guidelines on the Protection of Personal Data Processed by Mobile Applications Provided by European Union Institutions*. Accessed: Oct. 8, 2018. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/16–11-07_guidelines_mobile_apps_en.pdf

[24] *The standard data protection model. a concept for inspection and consultation on the basis of unified protection goals*, Konferenz der unabhfärngigen Datenschutzbehförrden des Bundes und der Lfärnder, Kühlungsborn, Germany, 2016.

[25] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proc. IEEE*, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[26] *Data Policy and Innovation: Proposal for an Eprivacy Regulation*. Accessed: Oct. 8, 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[27] *Smartphone Secure Development Guidelines*, ENISA, Heraklion, Greece, 2016.

[28] *Mobile endgerfärte und mobile applikationen: Sicherheitsgeffährhrdungen und schutzmaβnahmen*, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 2006.

[29] *Privacy in Mobile Apps: Guidance for App Developers*, UK Information Commissioners Office, Wilmslow, U.K., 2013.

[30] K. D. Harris,*Privacy on the go: Recommendations for the Mobile Ecosystem*. Sacramento, CA, USA: California Department-Justice, 2013.

[31] M. Ogata, B. Guttman, and N. Hastings, "Public safety mobile application security requirements," in *Proc. Nat. Inst. Standards Technol.*, Jan. 2015, pp. 1–48.

[32] *Mobile Privacy: A Better Practice Guide for Mobile app Developers*, The Office of the Australian Information Commissioner (OAIC), 2014.

[33] A. J. Blumberg and P. Eckersley, "On locational privacy, and how to avoid losing it forever," *Electron. Frontier Found.*, vol. 10, pp. 1–7, 2009.

[34] *A Developer's Guide to Securing Mobile Applications*, VASCO Data Secur., Chicago, IL, USA, 2014.

[35] E. K. Jacob, "Classification and categorization: A difference that makes a difference," *Library Trends*, vol. 52, pp. 515–540, Jun. 2004.

[36] *Opinion 05/2014 on Anonymisation Techniques*, Data Protection Working Party, Brussels, Belgium, 2014.

[37] A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, "Availability and quality of mobile health app privacy policies," *J. Amer. Med. Inform. Assoc.*, vol. 22, pp. 28–33, Aug. 2014.
[38] H. Lu, X. Helu, C. Jin, Y. Sun, M. Zhang, and Z. Tian, "Salaxy: Enabling USB debugging mode automatically to control Android devices," *IEEE Access*, vol. 7, pp. 178321–178330, 2019.
[39] W. Wang, M. Zhao, Z. Gao, G. Xu, H. Xian, Y. Li, and X. Zhang, "Constructing features for detecting Android malicious applications: Issues, taxonomy and directions," *IEEE Access*, vol. 7, pp. 67602–67631, 2019.
[40] T. Cho, H. Kim, and J. H. Yi, "Security assessment of code obfuscation based on dynamic monitoring in Android things," *IEEE Access*, vol. 5, pp. 6361–6371, 2017.
[41] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, and J. F. D. Jr, "Advanced encryption standard (AES)," in *Proc. Federal Inf. Process. Stds. (FIPS)*, Dec. 2001, pp. 8–12.
[42] *Privacy Impact Assessment (PIA): How to Carry out a PIA*. Commission Nationale de l'Informatique et des libertés, Paris, France, 2015.
[43] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A process for data protection impact assessment under the european general data protection regulation," in *Privacy Technologies and Policy*. Cham, Switzerland: Springer, 2016, pp. 21–37.
[44] S. J. De and D. Le Métayer, "Priam: A privacy risk analysis methodology," in *Data Privacy Management and Security Assurance*, G. Livraga, V. Torra, A. Aldini, F. Martinelli, and N. Suri, Eds. Cham, Switzerland: Springer, 2016, pp. 221–229.
[45] S. W. Brooks, M. E. Garcia, N. B. Lefkovitz, S. Lightman, and E. M. Nadeau, "An introduction to privacy engineering and risk management, in federal information system," NIST, Gaithersburg, MD, USA, Tech. Rep. 8062, 2017.
[46] M. Hatamian, J. Serna, and K. Rannenberg, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets," *Comput. Secur.*, vol. 83, pp. 332–353, Jun. 2019.[Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818313051
[47] M. Hatamian, A. Kitkowska, J. Korunovska, and S. Kirrane, "It's shocking!": Analysing the impact and reactions to the a3: Android apps behaviour analyse," in *Data and Applications Security and Privacy*, F. Kerschbaum and S. Paraboschi, Eds. Cham, Switzerland: Springer, 2018, pp. 198–215.
[48] M. Hatamian, J. Serna, K. Rannenberg, and B. Igler, "Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps," in *Proc. 14th Int. Conf. Trust Privacy Digit. Bus. (TrustBus)*, Lyon, France, 2017, pp. 3–18.
[49] N. Zhong and F. Michahelles, "Google play is not a long tail market," in *Proc. the 28th Annu. ACM Symp. Appl. Comput.*, New York, NY, USA, 2013, pp. 499–504, doi: 10.1145/2480362.2480460.

MAJID HATAMIAN (Student Member, IEEE) is currently pursuing the Ph.D. degree in computer science with Goethe University Frankfurt, Germany. He is a Research and Teaching Assistant with Goethe University Frankfurt. His research interests are in wireless communications, security and privacy in peer-to-peer networks, nano-communications, and machine learning techniques. His current focus is on privacy risk analysis in smartphone ecosystems. He has received several scientific awards, including the Best Student Paper Award at IFIP SEC 2019.