International Journal of Information Security (2024) 23:3217–3239
https://doi.org/10.1007/s10207-024-00887-z

REGULAR CONTRIBUTION

A study on privacy and security aspects of personalised apps

Stylianos Gerasimou[1] · **Konstantinos Limniotis**[1,2]

Accepted: 3 July 2024 / Published online: 18 July 2024

Abstract
This paper studies personalised smart apps, from a data protection and security point of view. More precisely, having as a reference model the provisions stemming from the General Data Protection Regulation, we investigate whether such apps, whose philosophy is based on the provision of personalised services, adopt appropriate data protection techniques, focusing especially on aspects from the data protection by design and by default principles, as well as on their security features. Our analysis over ten popular such Android apps illustrates the existence of several privacy concerns, including the facts that several data processes are by default enabled without requesting users' consent, as well as that several data processes are not well justified or sufficiently transparent to the users. Moreover, interestingly enough, the apps studied are not free of known security weaknesses.

Keywords Android · App security · Personal data protection · Privacy · Personalised apps

1 Introduction

In the era of big data, the smart mobile ecosystem plays a significant role, since huge amounts of data are being shared and further processed for various purposes [1]. Especially the COVID-19 pandemic highly affected technological progress, leading to widespread adoption of fields like e-commerce, distance learning and working, digital entertainment, etc. [2–4]. According to a recent research based on a survey [5], we are now at the point where the adoption of new technologies in the above areas is becoming prevalent, constituting a critical component for the business, since companies need to continue to invest in digital technologies to remain competitive, whilst at the same time consumers have highly increased their preference to online channels.

The above progress has also increased the demand for the so-called personalised services—especially through smart applications. The ultimate purpose of these applications is to provide personalized information to the users, as well as services based on their habits, interests, preferences, geographic coordinates and other factors. It is well-known that users indeed tend to choose such services [6]. However, for the provision of all these services, a (possibly extensive) collection and further process of users' personal data is inevitably carried out. For example, personalisation typically yields to user's profiling; this in turn entails many concerns on the privacy and personal data protection for the users, taking also into account the relevant legal provisions that are applicable per case [7]. More specifically, from a data protection point of view, the default settings of an app should be the most privacy friendly and this becomes highly challenging when the app is supposed to be able to provide personalised services—i.e., which should be the proper default settings in terms of personal data protection (e.g., is it proper to have tracking/advertising services enabled by default without the user's consent)? These privacy concerns are further accentuated by the inherent privacy issues that are typically present in the smart ecosystem, regardless the type of the services provided, such as the high-risk permissions that the apps ask, as well as the embedded trackers that they may have and the non-transparency of the overall processes [8]. Very recently, in the process of the writing of this paper, Meta was forced, by a competent Data Protection Authority, to change its policy in Europe regarding personalised advertisements through its products (see Sect. 6), which further illustrates the impor-

✉ Konstantinos Limniotis
konstantinos.limniotis@ouc.ac.cy ; klimniotis@dpa.gr

Stylianos Gerasimou
stylianos.gerasimou@st.ouc.ac.cy

[1] School of Pure and Applied Sciences, Open University of Cyprus, 2220 Latsia, Nicosia, Cyprus

[2] Hellenic Data Protection Authority, Kifisias 1-3, 11523 Athens, Greece

tance of the subject, as well as that it still constitutes a very challenging field.

This paper focuses on analyzing several popular Android apps that provide personalised services in terms of their underlying personal data processes. More precisely, our aim is to investigate the following: (a) which permissions are required by the apps, as well as whether these permissions are fully justified, (b) whether there exist data transfers to third parties and for what purposes, (c) whether the information provided to the user with respect to their underlying data processing is sufficient, (d) whether there exist security concerns stemming from the use of such apps. Hence, our ultimate goal is to focus on specific aspects of the so-called data protection by design and by default principles, as envisioned in the General Data Protection Regulation (GDPR) which is being considered as a model for other regulations to follow in terms of rights and principles (see, e.g., [9]).

It should be stressed that personalisation as a generic feature spans the entire mobile ecosystem, since plenty of apps provide (some) personalised services independently from their category; for example, apps for news, weather, games, social networking etc. usually come along also with personalised services. In this work, we focus particularly on apps for which personalisation is a basic feature, in terms that we may assume that the user does expect to enjoy personalised services. For example, if we consider the Netflix app (which is one of the apps being studied in this work), it is logical to assume that a typical user is aware from the very beginning than the app will make suggestions depending on her/his preferences, being an essential feature of the service provided.

1.1 Research questions

This paper focuses on privacy and security aspects of personalised apps.

Q1. How transparent are the data processes performed in the context of providing personalised services? Is there clear and comprehensive information on the underlying processes of personal data that takes place?
Q2. What types of personal data (including device data) are being processed, according to the permissions required? Does this data process satisfy the data minimisation principle?
Q3. Are personal data that are being processed for personalised services being shared with third parties? Are the purposes for this sharing clearly defined?
Q4. Do the underlying data processes require the user's consent? If yes, is it freely given and specific?
Q5. Are efficient measures in place to prevent security attacks?

It should be noted that all the above research questions are strongly related with the fulfilment of the so-called data protection by design and data protection by default principles, as provisioned in the GDPR (see Sect. 2.1).

1.2 Structure of the paper

The paper is organized as follows. First, Sect. 2 sets the background via providing: (a) the relevant legal requirements for personal data protection stemming from the GDPR, (b) the well-known privacy and data protection issues in Android apps in general and (c) the notion of personalised apps. Section 3 refers to relevant previous works in the field. Next, Sect. 4 describes the methodology adopted to address our research questions, presenting also the testing environment as well as the corresponding apps that have been chosen as use cases for our study. The main results of our work are given in Sect. 5, being the main part of the paper, which presents all the results of our analysis through the various tools, in conjunction with the study and evaluation of the corresponding privacy policies. More precisely, this section includes: (a) a presentation of the high-risk permissions that the apps we study require, (b) a presentation of the third-party trackers that these apps use, (c) a description of the content of the corresponding privacy policies of the apps, followed by a discussion of whether these policies are in line with our findings concerning the permissions and the trackers; moreover, we identify several other weaknesses in the privacy policies, concerning either their clarity or whether they describe excessive personal data processes, (d) analysis of potential security weaknesses of the apps studied. A discussion of our overall findings is given in Sect. 6. Finally, concluding remarks are provided in Sect. 7.

It should be pointed out that this work is not (and should not be considered as) a legal evaluation of the corresponding personal data processes.

2 Preliminaries

2.1 The notions of privacy and personal data protection–legal framework

The rights to privacy and personal data protection has been recognised as a fundamental human right by several international treaties (such as the United Nations Declaration of Human Rights, the Charter of Fundamental Rights in European Union etc.) The main relevant legal instrument in Europe, but also applicable for any organisations providing services to citizens being in Europe, is the so-called General Data Protection Regulation or GDPR [10]. As it is stated in [11], the intentionally global reach of the GDPR has led companies around the world to adjust their privacy

practices—and countries around the world to update their privacy laws.

According to the definitions in the art. 4 of the GDPR, the term *personal data* refers to *any information relating to an identified or identifiable natural person, that is a person who can be identified*. Due to this definition, the notion of the personal data is quite wide; for example, device and network identifiers should be also considered as personal data since they may allow the identification of a user (if possibly combined with other information). Moreover, the same article in the GDPR defines the *personal data processing* as any operation that is performed on personal data, including the *collection, recording, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination* etc. Additionally, the entity that *determines the purposes and means of the processing of personal data*, is the so-called *data controller*, which is the main entity entitled with many legal (and, actually, technical) responsibilities for ensuring personal data protection. For example, in our paper we study smart apps that are being provided by specific companies; since these companies process users' (i.e., personal) data, these companies constitute the data controllers for all such processes. Moreover, the GDPR defines the he *data processor* as *the entity which processes personal data on behalf of the controller*. In our context, if a company providing a smart app has also a contract with another company to facilitate (part of) the process—e.g., to perform analytics—then the latter is a data processor.

The GDPR sets the basic principles that need to be in place when personal data are being processed, setting specific obligations for the data controllers. The basic principles include, amongst others (see art. 5 of the GDPR):

- The transparency of the processing—namely, the individuals should be fully informed, upfront the processing and in a comprehensive and easily understood and accessible way, that their data will be processed, as well as by whom (i.e., who the data controller is), for which purposes, what exactly types of user's data will be processed etc.
- The purpose limitation, i.e. the personal data that are being collected for a specific purpose (which, of course, should be legitimate and transparent) shall not further processed in a manner that is incompatible with this purpose.
- The data minimisation, which refers to the need to ensure that the personal data that will be collected shall be limited only to what is necessary in relation to the purposes for which they are processed—i.e., no excessive personal data should be collected.
- The data security, which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through appropriate technical or organisational measures.

Moreover, any processing of personal data requires a lawful basis, as they are described in the art. 6 of the GDPR (in simple words, there exist specific preconditions in order to have a lawful personal data processing, whilst at least one of them needs to be in place). In the smart mobile ecosystem, a typical lawful basis is the user's consent—i.e. the process is allowable because the user agrees with it. However, a user's consent is being considered as valid if, according to the art. 4 of the GDPR, is *a freely given, specific, informed and unambiguous indication of the user's agreement to the processing of his or her personal data, given by a statement or a clear affirmative action*. For example, bearing in mind that Android applications require specific permissions to get access to specific data from our device, the fact that a user allows these permissions does not necessarily mean that we have a valid user's consent, since the user knows that if she/he does not allow access, the app will not work—and, thus, the user may not be free to object to the process.

The GDPR sets specific obligations for any data controllers, in the context of the so-called accountability principle. Amongst them, the *data protection by design* and *data protection by default*, as determined in the art. 25 of the GDPR, are of high importance, since they constitute important challenges involving various technological and organisational aspects [12]. In simple words, data protection by design means that the fulfilment of the data protection principles (i.e., transparency, purpose limitation, data minimisation, valid lawful basis, data security etc.) should be integrated into the processing activities from the early design stage right through the life cycle, whereas the data protection by default implements the rule to set the default settings properly so as to limit the data processing to what is necessary for its purpose [13].

With respect to transfers of personal data outside the European Union (EU), the GDPR imposes specific restrictions in order to ensure that, at the destination, the level of protection of individuals remains the same. More precisely, such a data transmission can be permitted only if specific conditions are in place, as they are being provisioned in the Chapter V of the GDPR. These obligations with respect to data transfers also span the transparency of the process—i.e., if a data controller needs to transfer data outside the EU then, apart from ensuring that this is allowable based on the GDPR's restrictions, the controller must also inform the individuals about this transfer, explaining also why this transfer is allowable according to the relevant GDPR's provisions.

Finally, it should be stressed that, depending on the techniques used, tracking of a mobile user may fall into the scope of the legal framework relying in the provisions of the so-called ePrivacy Directive (Directive 2002/58/EC) which, as *lex specialis*, take precedence over the general provisions of the GDPR. Very recently, the European Data Protection Board (EDPB), a legal body established in the GDPR, has

issued guidelines for exactly the processes concerning tracking that fall under the e-Privacy Directive (see [14], which is currently under public consultation). The e-Privacy Directive currently applies only to the European Union. Again though, the informed consent is a prerequisite, as a lawful basis, for many of the cases of data processing, whilst the aforementioned data protection principles still need to be in place.

2.2 Privacy and data protection issues in Android applications

The Android system is being considered as the most popular platform, taking 70.16% of the mobile operating system market share [15]. However, despite the fact that it constantly seems to improve the mechanisms adopted for protecting the privacy of its users, data protection and privacy issues still occur. Such issues could be summarised as follows:

1. In Android systems, each app asks for specific permissions at run time (for example, an app may require network access or access to geolocation data or to the camera). These permissions are classified to several protection levels, based on their severity; for our work, the so-called *dangerous permissions* are of importance (see, e.g., [16]), which include permissions corresponding to device data or resources involving the user's private information, or could potentially affect the user's stored data or the operation of the device or applications. The user typically does not have the option to object to such permissions, since otherwise the app cannot work; however, it is questionable whether the permissions required are always necessary, based on what the user expects from the app.
2. Granting such permission to an app may also directly mean that other third parties also get such permissions—namely, these parties whose software libraries have been used by the app. This happens because, in the Android platforms, third-party libraries inherit the privileges of the host app.
3. Permissions for accessing sensitive resources are related with specific protected Application Programming Interface (API) methods; namely, if an app needs to utilise such a method, then the corresponding permissions are defined in its manifest. However, the exact correlation between Android Software Development Kit (SDK) API methods and permissions has been formulated as a challenging problem, not being straightforward (see, e.g., [17]).
4. There is no sufficient mechanism to allow users control their data processing. For example, deceptive designs and manipulative patterns aiming to "force" users provide their consent (such as pre-checked boxes) are highly problematic.
5. The mobile devices are typically always activated, storing a lot of personal data for a long period of time. This also includes many different types of identifiers, such as device hardware ID, stored files, metadata [8] or digital fingerprints (see, e.g., [18]) that can be used by mobile apps to easily track the users—which could be also performed in a non-transparent way.

The above are general data protection issues arising in the smart mobile ecosystem; these though are further accentuated in the framework of smart apps providing personalised services, since in these cases a user's profile is somehow by default being built. The notion of personalised apps is subsequently discussed.

2.3 Personalised applications

A large number of smart applications have the ability to be customized according to the needs and desires of the user. Such a customization is based on specific choices of the user, which can be done manually by the user herself/himself (i.e., though specific options from the app's menu). On the other side, personalisation is a dynamic process that occurs in real time in order to meet the specific requirements of each user, which are being somehow inferred by her/his overall activity. Personalisation, being part of the app's operating process, is based on the user's psychological need to feel that is being treated in a unique manner. As it has been defined, personalisation refers to *the degree to which information is tailored to meet the needs of the individual user* [19]. In this context, notifications, recommendations, discounts, offers, etc. can be part of the user personalisation related processes, when they are tailored to the user. Hannah Levenson's example [20] shows the difference between customization and personalisation in a simple way. When we order a pizza with pineapple during our visit to a pizzeria, we actually have a case of customization. But when the pizzeria knows the type of pizza the customer wants and prepare it, it is a personalised experience.

Personalisation is primarily based on data collection. Data collection is necessary for a system to understand its users in terms of who they are, what they want, what they need, what preferences they have, etc. Such data may include user's age, gender, interests, profession, location, time frame of application use, device used, likes and dislikes, shopping time, shopping history etc. After collecting the necessary data, the application will try to recognize patterns among the data and categorize them into groups of users. Such a categorisation typically makes it easier to provide personalised services; especially when the user makes use of social networks in order to be registered to an app, the personalisation is further facilitated.

Personalised push notifications also play a big role in personalising the application. These are automated notifications sent by an app to the user when the app is not

open. Developers of personalised smart apps, towards keeping users engaged, are faced with the challenge of sending relevant push notifications. An example of push notifications are notifications based on the user's geographic location. For example, the user may automatically receive recommendations from the application for restaurants in the area she/he is in which she/he is likely to prefer since the application has already combined data based on the user's preferences.

Apart from the push notifications, apps also use in-app messages that can be personalised. In addition, the application can inform and praise the user if he completes certain processes (milestones). Under the assumption that the application already knows the user's interests, needs and purchase history, it is obvious that the options and recommendations it will display will be indeed based on the user's wishes.

From the above, it becomes evident that personalisation yields by default privacy and data protection concerns, due to the fact that a somehow profiling of the user is being developed by the app's provider, which in turn could be also shared with other third parties. The way that this user's profile is being created may not be fully transparent to the user, whereas it is questionable what other conclusions about the user can be derived by the overall process, apart from those related with the provision of personalised experience.

3 Previous work

Due to the proliferation of smart apps in our daily lives, the relevant underlying privacy and data protection issues are being widely studied for many years—see, e.g., [16, 21–32]. More precisely, the third-party tracking is being studied in [21], as well as in [30]; in the later, automated methods to detect third-party advertising and tracking services at the traffic level, evaluating them under the framework of the relevant privacy policies, are developed and presented. Mobile advertising libraries are being studied in [26], illustrating that malicious ads can infer users personal data. The important notion of the so-called *intra-library collusion* is being discussed in [27], which occurs when a single library is embedded in more than one app on a device; then this library inherits the whole sets of permissions acquired by each app, thus leveraging to a larger set of permissions than any other single app in the user's device (and the user is not aware of this). More recently, especially with respect to third party trackers, a study shows that most Android apps engage in third-party tracking, but few obtained consent before doing so [32]. Data protection concerns for specific types of apps, in terms of high-risk permissions required and data leakages to third parties are being studied in [16, 24, 25]. Privacy issues of apps targeted to children, with respect to identifying violations of the COPPA (i.e., the Children's Online Privacy Protection Act in the United States), is being studied in [28]. The inconsistencies between privacy policies and the actual data processes are being studied in [22]. The non-anonymity of the so-called anonymous apps is studied in [29]. The users concerns on the privacy tools themselves that are being used to analyze text or images and detect personal data leakages, with the aim to alert the users, is demonstrated in [23]. Recently, the special issue of the location privacy is studied in [31], stemming from the fact that users use smart transportation systems to move around in smart cities, producing a huge amount of mobility data.

The majority of the research works are focused on Android systems; however, as it has been recently illustrated in [33], third-party tracking and sharing of user identifiers is commonly being met in both Android and iOS ecosystems, and thus neither platform is clearly better than the other for privacy (for example, both platforms raise concerns on non-data-minimising configuration of tracking libraries).

In this complex environment, personalised apps need also cautious attention; although users are indeed interested in getting efficient personalised experience (for example, to have improved shopping experience), they are simultaneously concerned about their privacy when using such services [34]. A comprehensive survey on the privacy risks, in conjunction with proposed solutions, for targeted advertising in a mobile environment is presented in [35]. In [36], a model on consumer interaction with smart technologies in shopping malls is proposed, aiming to address the roles of personalisation and privacy concerns. However, despite the concerns regarding privacy, users tend to use personalised services (see, e.g., [37, 38])—an issue that has been defined as *privacy paradox* [39]. Therefore, it becomes evident that studying privacy and data protection issues arising especially from the use of personalised apps is of high importance.

Towards studying privacy and security aspects of Android apps, several tools have been developed performing either static analysis (i.e., the source code is being checked) or dynamic analysis (i.e., the application is being examined while it's running). A classical tool is the so-called PScout [40], being used for statically analysing Android's permissions; as it is shown in [40], there is a trade-off between enabling least-privilege security with fine-grained permissions. This tool though has been used for old versions of Android, namely up to the 4.1.1.4 version, so the relevant output lists of permission maps is partially outdated. Other known static analysers include the TrustDroid [41] for detecting data leakages (mainly from a security point of view), the FlowDroid [42] which analyzes the app's code and configuration files to find potential privacy leaks, and the Axplorer [43] which performs static analysis of Android OS source code to derive an improved permission map. Finally, the AIDetector [44] also performs static analysis, but with the aim to detect vulnerable applications in terms of security.

There are other tools performing dynamic analysis such as the ScanDroid [45] that assesses the Android API for information leaks based on dynamic time warping, the KAUdroid [46] which collects permission usage on phones with the aim to present the relevant information through a web user interface so as to raise awareness to the users of how third-party applications tend to abuse their trust, the Corwdroid [47] which focuses explicitly on detecting malware through dynamic analysis of an app, the Andromaly [48] which is a host-based malware detection systems through analysing apps, the TaintDroid [49] which performs a system-wide dynamic analysis, the Copperdroid [50] which also focuses on detecting malware. Another tool that is related with malware detection is the Anactijax [51], which is capable of generating automatically activity injection test cases for assessing whether an application is vulnerable or not to such type of attacks.

There are also tools exploiting simultaneously both static and dynamic analysis. These include the AppRay [52] which analyses apps according to user-specific security requirements, the Tdroid [53] and EspyDroid+ [54] which aim to detect malicious apps, as well as the Dypermin [17] which aims to to compile the permission map for any given Android version.

4 Description of the research methodology

This section presents the main goals of the current research, as well as the methodology that has been adopted to address our goals.

4.1 Contribution of this work

In this paper, we investigate specific aspects concerning personal data protection and privacy, focusing explicitly on apps providing personalised services (i.e., on apps that they are specifically designed for providing such services). This is a field of high importance, especially due to the challenges occurring when personalised services are to be evaluated in terms of their privacy features and safeguards. More precisely, these challenges stem from the fact that it is inherently difficult to establish the fulfillment of the data protection by default principle in such services.

Compared to other approaches, this paper employs both static and dynamic analysis, through well-known publicly available tools, for identifying the high-risk permissions that the apps require, as well as embedded trackers; these issues are in turn being evaluated according to what the corresponding privacy policy states, in conjunction with the relevant provisions stemming from the GDPR (and this is an aspect that is not being highlighted in other relevant works—only to few of them [16, 28, 30]). To this end, the privacy policies are being examined in terms of comprehensiveness and readability, whilst the processes having the user's consent as legal basis are being scrutinized so as to identify whether the consent obtained is indeed valid or not. We also check for possible software security issues in the apps, towards establishing a more complete view on what overall data protection concerns exist (and such security issues are not studied in [16, 28, 30]).

During the process of writing the initial draft of the paper, significant relevant developments took place in Europe, highlighting the importance of this field. More precisely, according to a decision of the European Data Protection Board (EDPB) [55], which is a legal body being established by the GDPR, the company Meta shall stop providing tailored advertisements to the European users of its platforms since this process was being performed without the users consent (which, according to the EDPB, is the only legal basis that can be in place for such a processing). Hence, it becomes evident that this work highly contributes in this active field through studying similar aspects for many popular apps.

4.2 The methodological approach

Towards examining a specific app in light of the above objectives, our methodological approach consists of the following steps (see also Fig. 1):

1. Identify the high-risk permissions that the app requires; this is performed by using both static and dynamic analysis of the app.
2. Identify the embedded trackers (third parties); again, this is performed by using both static and dynamic analysis.
3. Examine the privacy policy, towards evaluating whether the underlying data process is transparent and comprehensible to the users, as well as to see whether the data protection by design and by default principles are being reflected within these policies. To this end, we also particularly examined whether there is any discrepancy between what the privacy policy states and our findings from the previous steps.
4. Identify software security weaknesses.

The final evaluation is obtained on the basis of all the above outcomes.

4.3 The testing environment

For the purpose of our research, we relied on some well-known software tools that suffice to analyse smart apps in terms of their data protection features—namely:

– The Exodus Privacy web tool (hereafter referred to as Exodus) [56], supported by a French non-profit organi-

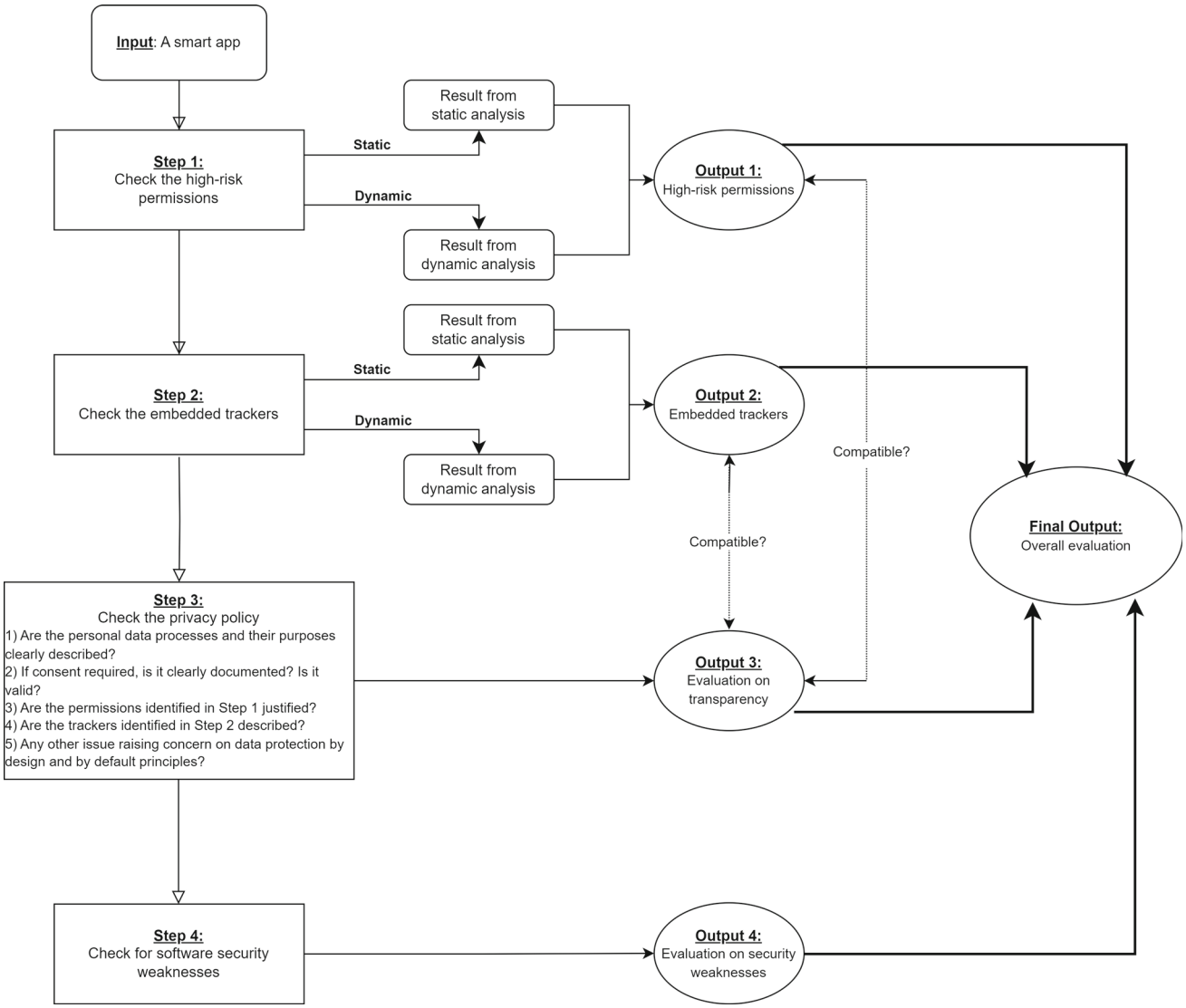

Fig. 1 Flowchart of the methodological steps

zation, that can statically analyze Android applications by looking for embedded trackers and listing them as an output report. In addition, this tool presents the permissions that are being requested by an app and highlights the dangerous permissions.

– The TrackerControl for Android (hereafter referred to as TrackerControl) [57], which is an Android app that allows users to monitor and control the data collection in mobile apps about user behaviour (tracking). To achieve this, this tool uses both dynamic as well as static analysis with the ultimate goal to reveal the companies behind tracking and identify the purposes of tracking, such as analytics or advertising.
– The ImmuniWeb Community Edition—Mobile App Security Test (hereafter referred to as ImmuniWeb) [58], which is an online tool focusing, amongst others, on identifying mobile app security vulnerabilities and weaknesses. The ImmuniWeb employs Dynamic Application Security Testing (DAST) so as to monitor applications during their runtime.

The tests were performed on a Xiaomi Mi 9T Pro mobile device being used in Cyprus with MIUI Global 12.5.2 (RFKMIXM) with Android 11 software (version RKQ1.200826.002), as well as on the Genymotion emulator in which a Samsung Galaxy S10 virtual device was created, being rooted.

4.4 Selection of apps

After setting up the testing environment, we proceeded by analysing several apps providing personalised services; as

stated in Sect. 1, our main focus is those apps whose personalised services constitute their main feature. More precisely, we focused, for our research purposes on the following ten apps, taking into account their popularity as well as the need to span a wide space of application types/categories: (1) Airbnb, (2) Amazon (Shopping), (3) Facebook, (4) Instagram, (5) (Google) Maps, (6) Netflix, (7) Nike Training (Club App), (8) Spotify, (9) TikTok and (10) Waze. These apps have millions of users which proves their ability not only to attract users but also to retain them. More precisely, Facebook, Instagram, Google Maps and Amazon Shopping are among the apps Americans can't "live without" [59]. According to [60], the world's top three apps in terms of downloads for 2022 are TikTok, Instagram and Facebook, while Spotify is in the 8th place. Therefore, the above applications have been selected so as to cover a wide range of categories and services such as social media platforms, e-commerce, entertainment, fitness and navigation, whilst being, at the same time, of high popularity.

5 Results

We subsequently present the results of our analysis. The analysis took place within the period January–March 2023.

5.1 Permissions analysis

Using the Exodus Privacy tool, we investigated the dangerous permissions that are being required by each app. As shown in Fig. 2, the app that requires the smallest number of dangerous permissions is the Netflix app (requiring two such permissions), whilst on the other side, the Airbnb, TikTok and Waze apps require the largest number of dangerous permissions (16, 17 and 16 respectively).

It can be seen that all apps, except Netflix and Spotify, require access to the user's contacts through the `READ_CONTACTS` permission request. Moreover, all of the apps examined, apart from the Google Maps and Nike Training, require the dangerous `RECORD_AUDIO` permission, which is typically used to record audio from the user's device (and, as we will see next, the privacy policies do not always clarify the necessity for this permission). Additionally, it should be pointed out that the Airbnb app is the only one of the apps examined that requires the dangerous `CALL_PHONE` permission which allows an app to make calls without requiring any user's action (and, again, as we will see next, the purpose for such a process is not well-defined in the relevant privacy policy).

Finally, all apps require the `WRITE_EXTERNAL_STORAGE` permission, for which the Google is recommending that should not be used by the developers for applications that will be used on Android 10 or later (see, e.g., [61]).

Apart from the Exodus Privacy tool, we also used the ImmuniWeb Community Edition program, in order to investigate the dangerous permissions required by each app. Interestingly enough, there exist some small variations between the findings obtained from these two tools. More precisely, based on the findings from the ImmuniWeb:

- The Amazon Shopping, the Facebook and the Nike Training apps also require a permission, additionally to those illustrated in Fig. 2, regarding calls management (i.e., the `CALL_PHONE` permission). However, the ImmuniWeb tool has not identified, for the Nike Training app, the `GET_ACCOUNTS` permission.
- The Google Maps app also requires, additionally to the permissions illustrated in Fig. 2, the `MANAGE_ACCOUNTS` and `USE_CREDENTIALS` permissions.
- The Spotify app also requires, additionally to the permissions illustrated in Fig. 2, the `USE_CREDENTIALS` permission.
- The TikTok app also requires, additionally to the permissions illustrated in Fig. 2, the `AUTHENTICATE_ACCOUNTS` and `GET_TASKS` permissions.
- The Waze app also requires, additionally to the permissions illustrated in Fig. 2, the `AUTHENTICATE_ACCOUNTS`, the `MANAGE_ACCOUNTS` as well as the `USE_CREDENTIALS` permissions.

The above differences between the findings from the two different programs could be possibly explained—at least to some extent—from the fact that Exodus performs static analysis whilst ImmuniWeb utilises dynamic analysis. Both approaches have their own advantages and disadvantages; the main advantage of static analysis is that all the code is analyzed, whilst in dynamic analysis some sources of code may not be executed, depending on whether specific conditions occur or not [62]. On the other side, static analysis may yield false positives (i.e. it may exhibit a permission that does not necessarily trigger the execution of the relevant activity), whilst dynamic analysis is free of true positives [17]; of course, since permissions are in fact correlated with protected Application Programming Interface (API) methods, a dynamic analysis cannot ensure full coverage of all API methods [17].

It should be clarified that dangerous permissions do not violate the data protection requirements per se; however, it is essential that the app providers fully justify the necessity for requiring these permissions, whereas these should also granted under the fulfilment of the data protection by default principle. As it will be subsequently discussed, it is questionable whether this is indeed the case.

	Airbnb	Amazon	Facebook	Instagram	Maps	Netflix	Nike Training	Spotify	TikTok	Waze
ACCESS_BACKGROUND_LOCATION					✓					✓
ACCESS_COARSE_LOCATION	✓	✓	✓		✓		✓		✓	✓
ACCESS_FINE_LOCATION	✓	✓	✓	✓	✓		✓			✓
ACCESS_MEDIA_LOCATION	✓		✓	✓			✓			
ACTIVITY_RECOGNITION					✓					
BLUETOOTH_ADVERTISE								✓		
BLUETOOTH_CONNECT	✓							✓	✓	✓
BLUETOOTH_SCAN	✓							✓		✓
CALL_PHONE	✓									
CAMERA	✓	✓	✓	✓			✓		✓	✓
GET_ACCOUNTS	✓	✓	✓	✓	✓		✓	✓		✓
READ_CALENDAR			✓						✓	✓
READ_CONTACTS	✓	✓	✓	✓	✓		✓		✓	✓
READ_EXTERNAL_STORAGE	✓	✓	✓	✓	✓		✓	✓	✓	✓
READ_PHONE_NUMBERS				✓						
READ_PHONE_STATE	✓		✓	✓				✓		✓
RECORD_AUDIO	✓	✓	✓	✓		✓		✓	✓	✓
SYSTEM_ALERT_WINDOW			✓						✓	✓
WRITE_CALENDAR			✓						✓	
WRITE_CONTACTS			✓							✓
WRITE_EXTERNAL_STORAGE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WRITE_SETTINGS	✓								✓	✓

Fig. 2 The dangerous permissions required by each app, according to the Exodus Privacy tool

5.2 Trackers analysis

5.2.1 Analysis through the Exodus

With respect to the trackers used by each app, the analysis through the web tool Exodus illustrated that only the Facebook app does not use any trackers. However, both trackers used by the Instagram, which is owned by the same company as the Facebook, are related to Facebook, whereas there are also Facebook related third parties in other apps. It is worth noting that all applications, except those mentioned above, make use of the Google Firebase Analytics tracker. We subsequently present in detail which trackers have been found for each app:

- Airbnb: *Bugsnag, Facebook Login, Facebook Share, Google Analytics, Google Firebase Analytics*
- Amazon Shopping: *Amazon Advertisement, Amazon Analytics, Google AdMob, Google Firebase Analytics*
- Instagram: *Facebook Flipper, Facebook Login*
- Google Maps: *Google Firebase Analytics*
- Netflix: *Bugsnag, Google Firebase Analytics*
- Nike Training: *Branch, Google AdMob, Google Firebase Analytics, New Relic, Optimizely, Singular, Urbanairship*
- Spotify: *Branch, Facebook Login, Facebook Share, Google AdMob, Google CrashLytics, Google Firebase Analytics*
- TikTok: *AppsFlyer, Facebook Login, Facebook Share, Google Firebase Analytics, VKontakte SDK*
- Waze: *Google AdMob, Google CrashLytics, Google Firebase Analytics*

5.2.2 Analysis through the TrackerControl

We also utilised the TrackerControl tool, being installed into our device, in order to examine which trackers can be found through this tool. Interestingly enough, there exist small variations on the corresponding findings, compared to the above. More specifically:

- Airbnb: The TrackerControl has additionally identified, apart from the 5 trackers mentioned above, the *Google AdMob* and the *Google Play Install Referrer* trackers. Moreover, the output report states that data are being sent to the U.S.A. and the Germany. The largest amount of outgoing traffic corresponds to the Akamai International B.V., which—as it turned out—provides (amongst others) cloud services, whilst the Airbnb is one of its clients.
- Amazon Shopping: The TrackerControl has additionally identified, apart from the 4 trackers mentioned above, the *AWS Kinesis* and the *Google Play Install Referrer* trackers. Moreover, the output report states that data are being sent to the U.S.A., the Germany and the Ireleand. The main outgoing traffic is being transmitted towards the Amazon company, as expected.
- Facebook: The TrackerControl illustrated that there exist trackers within the app, despite the fact that the analysis through the Exodus Privacy had not identified any such tracker. Most of the trackers identified belong to the

Facabook's company Meta Platform Inc. (i.e., they are no third-party trackers), whilst the tool illustrated data have been transmitted only to one company, namely the Meta Platforms Inc. However, the *Google AdMob* and *Google Analytics* trackers have been also captured through this tool. Moreover, the output report states that data are being sent to the Germany.
- Instagram: The findings from the TrackerControl fully coincide, with respect to the trackers, with the findings from the Exodus. The output report states that data are being sent to the the Germany, whilst the only company as a recipient is—as expected, the Meta Platforms Inc.
- Netflix: The findings from the TrackerControl fully coincide, with respect to the trackers, with the findings from the Exodus. The output report states that data are being sent to the U.S.A.
- Nike Training app: The findings from the TrackerControl fully coincide, with respect to the trackers, with the findings from the Exodus. The output report states that data are being sent to the U.S.A, the United Kingdom, the Germany and the France.
- Spotify: The TrackerControl has additionally identified, apart from the 6 trackers mentioned above, the *Google Play Install Referrer* tracker. Moreover, the output report states that data are being sent to the U.S.A. and the Germany and the Ireleand.
- TikTok: The TrackerControl has additionally identified, apart from the 5 trackers mentioned above, the *Google Play Install Referrer* tracker, whilst it has not identified the *VKontakte SDK* tracker that the Exodus has found. The output report states that data are being sent to the the U.S.A., the Germany and the Spain.
- Waze: The findings from the TrackerControl fully coincide, with respect to the trackers, with the findings from the Exodus. The output report states that data are being sent to the the U.S.A, whilst the only company as a recipient is, as expected, the Google LLC.

5.2.3 Discussion

When studying the permissions required by an app, in conjunction with the trackers that the app uses, we should take into account the so-called *intra-library collusion* threat [27]; for example, according to the Fig. 2, if a device has simultaneously installed the Airbnb, the Maps, the Spotify and the TikTok apps, which all of them include the Google Fierebase Analytics as a tracker, then the provider of this tracker (i.e., the Google in this case) also inherits the permissions granted to all these host applications—which actually includes almost all the high-risk permissions shown in Fig. 2 (apart from only two).

The user, when installs and grants permissions to apps that she/he uses, is typically not informed for this issue; as we will see in the sequel, such information cannot be extracted from the corresponding privacy policies.

5.3 Examination of the privacy policies

We next examine the privacy policies of the apps studied, in order to investigate if the information provided with respect to the underlying personal data processing is complete, clear and comprehensive, as well as in line with our previous findings. More precisely, our basis for the evaluation of each privacy policy, inspired by the GDPR's provisions, is the following set of features:

1. A clear description of all personal data being collected, as well the corresponding purposes for this collection and the lawful basis, should be provided; this information should be given for each distinct purpose, so as to have a mapping between data processing purposes and the corresponding personal data needed to achieve these purposes.
   - This description of processes needs to be compatible with our corresponding experimental findings (i.e., it should allow justifying each permission being asked by the app).
   - Ideally, the policy should state explicitly why and when each permission is being asked.
2. In cases that the lawful basis is the user's consent, it should be clear that the process is not enabled by default, as well as that the user may freely provide her/his consent.
   - Additionally, for cases that the user should expect that her/his consent is needed for a process, the policy should not state that the process has a different lawful basis—i.e., that the process takes place without the user's consent.
3. Sufficient information should be provided with respect to the third parties (i.e., who they are, which types of data they collect, for which purposes).
   - This information should be compatible with our experimental findings.

Hence, according to the above baseline, we focused on the following aspects when studying the privacy policies:

- Does the policy describe explicitly and clearly which personal data are being collected and for which purposes?
- In cases that some personal data are being collected only upon user's specific free consent, are they clearly documented?
- Are all app's permissions, as they have been identified by our analysis, justifiable by the processes described in the policy?

– Is sufficient information provided on which data and for which purposes are being collected by third parties? How precise is the information provided with respect to who are these third parties? Is this information in line with our corresponding findings?
– Does the policy describe a personal data process that seem to be not in line with the data protection by design and by default principles?

We subsequently present our main findings from this study.

5.3.1 Airbnb (checked when the last update was on January 25, 2023)

– The Airbnb's privacy policy, although written in clear language, does not provide fully transparent information, since it uses many times expressions like "we may collect" which introduce confusion of whether the relevant personal data are being actually collected or not (e.g., the policy states that some personal data are being automatically collected by using the Airbnb platform and the relevant payment services, which may include geolocation Information); apparently, this also raises concerns on whether the data protection by default principle is fulfilled.
– The purposes of the data processes are being described in a generic way—i.e. there is no an explicit mapping of what personal data are being collected for each desired purpose. Therefore, the user cannot be fully aware of what type of personal data are being used for which purpose, whilst it seems that some data processes are by default enabled without being necessary (e.g., analysing user's preferences for personalised advertising), thus rising again concerns on the data protection by default principle. In this respect, it is also not clear for all cases which data processes rely on user's explicit consent.
– The content of the privacy policy seems to not fully justify all the permissions that are being required (see, e.g., indicatively the `CALL_PHONE`, `RECORD_AUDIO` and `WRITE_EXTERNAL_STORAGE` permissions, whilst even the `READ_CONTACTS` permission is not justified, since it is not clear if it is always required or not).
– With regard to the embedded trackers, there is no explicit reference of what types of data the third parties collect and for which purpose—such information can be only somehow inferred by the relevant generic purposes (e.g., performing analytics is one purpose that is being mentioned in the policy), but this information is not sufficient for the user to identify which third parties collect personal data and for which exactly purposes.
– Finally, according to the privacy policy, even personal data of individuals that do not use the Airbnb app may still be processed by the company—and this clearly introduces major data protection risks.

5.3.2 Amazon shopping (checked when the last update was on August 11, 2023)

– The Amazon Shopping app on Google Play refers, with respect to the privacy policy, to the general Privacy Policy of the Amazon company. This should be considered as somehow problematic since it may confuse the user with respect to what explicitly this app does with her/his personal data.
– The user is aware of what types of personal data are being collected for specific purposes. However, the description of these types of data are quite generic in some cases. For example, the policy refers to the collection of health and fitness data for the app's functionality—without providing other clarifications on this; even worse, these types of data are being shared with third parties, without mentioning whether this data sharing is optional (and, if yes, under which circumstances) or not. Moreover, the company collects, and also shares with third parties, device or other identifiers for several purposes, including—amongst others—advertising or marketing. However, it is not clear which exactly are these other types of identifiers that are being processed, whilst, similarly to the health data, there is no statement whether this data collection and further sharing with third parties is optional or not. In this respect, it is also not clear for all cases which data processes rely on user's explicit consent.
– The content of the privacy policy seems to not fully justify all the permissions that are being required (see, e.g., the `WRITE_EXTERNAL_STORAGE` and the `READ_CONTACTS` permissions, whilst even the `CALL_PHONE` permission that has been identified by one tools seems to be not justifiable).
– With regard to the embedded trackers, there exist references on which types of data are being shared with third parties, as well as the relevant purposes—whilst these purposes are in line with the trackers that have been found by our analysis. However, it is still not clear which exactly data are being collected by each party, whilst, as also stated above, it is also not clear whether this data collection is performed on an optional basis or not).

5.3.3 Facebook/Instagram (checked when the last update was on September 7, 2023)

Although the link through the Google Play leads to separate websites for each app, it can be readily seen that only minor differences occur between the two privacy policies, resulting in the conclusion that both apps have the same privacy policy.

- The fact that both apps share the same privacy policy raises some concerns on the transparency of the processing, especially taking into account that our analysis illustrated that these apps do not require the same permissions—i.e., it seems that different data processes are being performed by each app.
- The user is aware of what types of personal data are being collected for specific purposes, as well as for the corresponding legal bases—whilst such information is also given for the users who do not use these apps but their data will be processed e.g., through the contact uploading or contact syncing feature available on Facebook, Messenger or Instagram ("Contact Uploading"). However, in cases that the user's consent is being mentioned as the lawful basis for the process, it is questionable if this is indeed the case; for example, the most recent privacy policy states that personalised advertisements rely on user's explicit consent, whilst this was not the case during the period that our experiments took place, since in that period the privacy policy was stating that the company was processing user's data for the aim to provide tailored advertisements, so as to ensure that ads are appropriate for users and the devices they use.
- The content of the privacy policy seems to not fully justify all the permissions that are being required (see especially the `WRITE_EXTERNAL_STORAGE` permission, required by both apps).
- With regard to the embedded trackers, there exist references on which types of data are being shared with third parties, as well as the relevant purposes. However, it is interesting to point out that the privacy policy actually implies that several types of trackers are expected to be present (all for legitimate purposes) but our analysis has not actually indicated the presence of trackers. Hence, it is somehow unclear on which exactly are the third parties collecting personal data for the various purposes that are described in the policy.

5.3.4 Google map (checked when the last update was on December 15, 2022)

The privacy policy of the Google Maps app refers to the general privacy policy of the company Google LLC. This generic privacy policy describes how the company collects, uses and protects personal information.

- The fact that the app refers to the generic Google's privacy policy raises some concerns on the transparency of the process, taking into account that the company provides several different types of services/applications in various fields.
- The privacy policy, although written in clear language, does not provide fully transparent information, since it uses expressions like "we may collect" which introduce confusion of whether the relevant personal data are being actually collected or not, as well as whether the data protection by default principle is fulfilled. For example, the policy states that the company may collect the following types of data: approximate and precise location information (for purposes that include personalisation and tailored advertisement), messages (for purposes that include analytics), photos and videos, audio (for purposes that include analytics and personalisation), contacts (for the purposes of the functionality of the app, personalisation and account management), web browsing (for the sole purpose of advertising or marketing) and device or other IDs (for purposes that include analytics, advertisement or marketing, personalisation).
- The user is aware of what types of personal data are being collected for specific purposes. However, the description of these types of data are quite generic in some cases (see, e.g. generic references to identifiers), whilst even the purposes are not explicitly given (e.g., such generic purposes are personalisation or app functionality). The corresponding lawful bases for each data process is not given and, thus, it is not clear which data processes rely on user's explicit consent (for example, it seems that the app processes the browsing history of the user for advertisement purposes, without requesting her consent for this, as well as the user's contacts without clarifying why this process is necessary and when).
- The content of the privacy policy seems to not fully justify all the permissions that are being required (see especially the `WRITE_EXTERNAL_STORAGE` permission, whilst the `GET_ACCOUNTS` permission raises the same concern on accessing user's contacts as mentioned above).
- The policy states that no data are being shared with third parties; indeed, our analysis did not find any third-party tracker.

5.3.5 Netflix (checked when the last update was on November 21, 2022)

- The Netflix privacy policy, although written in clear language, does not provide fully transparent information, since it does not explicitly state for which purposes the personal data are being collected—i.e. there is no an explicit mapping between data processes and relevant

purposes. Similarly, the relevant lawful bases are also not explicitly associated with the corresponding processes.
- It seems that several personalised services are by default enabled, not relying on the user's free consent, thus rising again concerns on the data protection by default principle. For example, the company uses information to provide, analyze, administer, enhance and personalize its services and marketing efforts. Such information can be used to provide the user with customized and personalized viewing recommendations for movies, TV shows, and games that may be of interest to her/him (collectively "content") and to provide localized content. As it is also mentioned in the policy, the company's content recommendations system *strives to predict what the user will be in the mood to watch when she/he logs in*.
- Although the Netflix app does not ask for many dangerous permissions (actually, it asks for only 2 such permissions, namely the `RECORD_AUDIO` and the `WRITE_EXTERNAL_STORAGE` permissions), these permissions are not justified.
- There are no explicit references on third parties/partners.

5.3.6 Nike (accessed October 31st, 2023; no information of the last update was available)

The privacy policy of the Nike Training app has a link to the general policy of the Nike company that applies to all cases where the user interacts with the company through its websites, digital experiences, mobile applications, event stores and generally any other product that includes Nike's service platform.

- The fact that the app refer to the generic Nike's privacy policy raises some concerns on the transparency of the processing for this specific app.
- The privacy policy, although written in clear language, does not provide fully transparent information, since it uses expressions like "we may collect" which introduce confusion of whether the relevant personal data are being actually collected or not, as well as whether the data protection by default principle is fulfilled. For example, the policy states that the company may use the information that the user provides, as well as information from other Nike products or services, to personalize communications on products and services that may be interesting for her/him; in doing so, the company may combine the information the user provides with information that the company creates about the user's online activity, including internal insights and analysis.
- The user is aware of what types of personal data are being collected, but there is no a clear association (mapping) between the data processes and the corresponding purposes. Similarly, the corresponding lawful bases for each data process is not given (only a generic description of possible lawful bases is given, with indicative only examples of processes for each possible lawful basis).
- It is not clear which data processes rely on user's explicit consent. It is actually implied that many personalised services are not relied on user's consent, whilst even in cases that the user should provide her/his consent (which is not clear when happens, as stated above), concerns occur on the validity of the consent obtained. For example, the company states that the user may opt-out of personalized advertising and custom audiences by using the relevant settings in the platform, which implies that such tailored advertising services are by default enabled. Additionally, with respect to collecting the the user's location or sending push notifications, the policy states that user's consent for such processes can be obtained either through the platform or using the standard permissions available on the user's device.
- The content of the privacy policy seems to be in line with the (extensive set of) high-risk permissions that are being required; however, there exist permissions like the `WRITE_EXTERNAL_STORAGE` permission that is not being justified. In any case though, despite the fact the data processes that are described in the privacy policy seem to be in accordance with our findings on the permissions required, it is still not clear whether the data protection by default principle is in place (i.e., are these processes indeed necessary? Do they rely on user's consent or not?)
- The policy defines many possible third parties that are recipients of users' personal data; our analysis also indeed illustrates that the company shares data with many parties and in many countries. Although there is no evidence that a tracker found by our analysis is not justified according to what the policy states, the large number of third party trackers could be further elaborated within the privacy policy to enhance transparency.

5.3.7 Spotify (checked when the last update was on February 22nd, 2023)

- The privacy policy is clearly written and comprehensive. However, there are some points that need further clarification, especially with respect to personalised advertisements and other personalised services; more precisely, it is not clear whether these processes rely on user's explicit consent or not, thus raising concerns on the fulfilment of the data protection by default principle. It is worth mentioning that the policy describes, as a purpose of a data process, the so-called personalisation of a user's account, without though clarifying what it actually means—and, for this purpose, the lawful basis is not the user's consent

but the necessity of the processing for the performance of a contract.
- Our findings on app's permissions seem to be in line with what the privacy policy states; however, since there is no an explicit justification for each permission required, there are some concerns on the necessity of some permissions—especially (and similarly with all the other apps) for the `WRITE_EXTERNAL_STORAGE` permission. Moreover, regarding several permissions concerning the Bluetooth connection of the device, although the privacy policy explicitly states that information about Bluetooth connection is being collected, it is not clear if this process is by default enabled or it is up to the free choice of the user (note that Bluetooth data are being described, within the policy, in the context of technical types of data and, such technical types of data are typically collected, as again the policy implies, without the user's consent since it is considered as necessary for the purposes of the legitimate interests pursued by the company).
- The privacy policy describes in detail what categories of personal data are being shared with third parties, as well as for which purpose(s) per case; these third parties are being described as categories of recipients (e.g., marketing/advertising partners).

5.3.8 TikTok (checked when the last update was on May 4th, 2023)

- The policy is quite analytic, with room for improvement though especially on the exact types of data that are being processed for each purpose, as well as for the exact lawful basis for each purpose, since the policy refers, for almost all possible legal bases for the various purposes, to the same categories of personal data that are being processed (and, thus, introducing ambiguity). Moreover, by these descriptions it seems that almost all personalised services, apart from the tailored advertisements, are by default enabled, without requiring the user's consent. Hence, it is questionable whether the data protection by default principle is in place.
- According to what is being described in the policy, concerns are being raised on the fairness of the processing and, consequently, on the fulfillment of the data protection by design and by default principles. More specifically, the company collects content that the users aims to upload even if she/he changes her/his mind and does not proceed with the uploading (and it is questionable whether the users have expectations of such a processing), whereas each such content is being somehow scrutinised, allowing the company to extract features and get conclusions about it.
- The app also processes personal data of individuals that are not users of the app; this happens in cases that the app accesses the contacts of a user (where the contacts could be either in the phone list or in another social network) as well as in cases that a user is being "part" of a user's content.
- Some of the high risk permissions obtained by the app cannot be justified by the policy (see, e.g., the `WRITE_EXTERNAL_STORAGE` as well as the `BLUETOOTH_CONNECT` permissions).
- With respect to the sharing of personal data to third parties, it is mentioned that such third parties include—amongst others—advertisers (which get aggregate information from the company).

5.3.9 Waze (checked when the last update was on January 1st, 2023)

- According to the policy, the personalised services related to advertisement purposes are by default enabled; the user may choose to change the relevant configurations through the app.
- The user is aware of what types of personal data are being collected, but there is no a clear association (mapping) between the data processes and the corresponding purposes. Similarly, the corresponding lawful bases for each data process is not given.
- There is no an explicit justification for each permission required and, thus, there are some concerns on the necessity of some permissions—such as (as also noticed in all the other apps) for the `WRITE_EXTERNAL_STORAGE` permission. Moreover, apart from the fact that some permissions are not (at least straightforward) justifiable, it is not clear whether they are being always asked or not. Note also that the policy states that app may read user's contacts in an anonymous manner (and, indeed, the `READ_CONTACTS` permission has been identified by our analysis) but it remains unclear whether the anonymisation that is being performed is sufficient.
- The policy makes a reference to advertisers and entities that belong to the Google group of companies, as partners for personalised advertising; our previous analysis indeed identified only the Google company as a third party.

5.3.10 Summary

Our previous analysis indicates that the privacy policies of the apps studied raise significant concerns with respect to the fulfilment of the data protection by design and by default principles. First, we see that the data processes are not clearly defined, whilst several high-risk permissions required by the apps are not justifiable by the privacy policies—and

	Airbnb	Amazon	Facebook	Instagram	Maps	Netflix	Nike Training	Spotify	TikTok	Waze
ACCESS_BACKGROUND_LOCATION					✓					✓
ACCESS_COARSE_LOCATION	✓	✓	✓		✓		✓		✓	✓
ACCESS_FINE_LOCATION	✓	✓	✓	✓	✓		✓			✓
ACCESS_MEDIA_LOCATION	✓		✓	✓			✓			
ACTIVITY_RECOGNITION					✓					
BLUETOOTH_ADVERTISE								✓		
BLUETOOTH_CONNECT	✓							✓	✓	✓
BLUETOOTH_SCAN	✓							✓		✓
CALL_PHONE	✓									
CAMERA	✓	✓	✓	✓			✓		✓	✓
GET_ACCOUNTS	✓	✓	✓	✓	✓		✓	✓		✓
READ_CALENDAR			✓						✓	✓
READ_CONTACTS	✓	✓	✓	✓	✓		✓		✓	✓
READ_EXTERNAL_STORAGE	✓	✓	✓	✓	✓		✓	✓	✓	✓
READ_PHONE_NUMBERS				✓						
READ_PHONE_STATE	✓		✓	✓				✓		✓
RECORD_AUDIO	✓	✓	✓	✓		✓		✓	✓	✓
SYSTEM_ALERT_WINDOW			✓						✓	✓
WRITE_CALENDAR			✓						✓	
WRITE_CONTACTS			✓							✓
WRITE_EXTERNAL_STORAGE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WRITE_SETTINGS	✓								✓	✓

Fig. 3 The dangerous permissions in conjunction with the privacy policies—the red color indicates that the relevant permission is not being reflected within the privacy policy

this, apart from being a transparency issue, may also be a data minimisation issue (i.e., an unnecessary permission that is being asked yields excessive data processing). More precisely, to examine, for each app, which exactly permissions are not being justified by the corresponding policy, we adopted the methodology used in [63]—i.e., we developed a set of relevant keywords (e.g. location, proximity, precise, approximate, track, movement, GPS, and so on) corresponding to each dangerous permission defined by Android, in order to check manually whether these keywords are present or not in the policies. The relevant findings are shown in Fig. 3; the red color indicates that the relevant permission is not being reflected within the privacy policy.

Note also that, even for the few additional high-risk permissions identified through the dynamic analysis only, we again noticed that none privacy policy has any relevant reference on these permissions.

Moreover, as illustrated above, in many cases there is no sufficient information on the third party trackers, whilst fo all cases concerns occur on the validity of the user's consent (i.e., it is not clear whether consent is required or not or, even in cases that the policy makes an explicit reference to consent, the corresponding dat process is by default enabled.)

Based on the above, we summarize all our main findings in Table 1; this Table though should be read in conjunction with the aforementioned analysis in order to ensure a comprehensive view of the overall status. For example, since none privacy policy provides a detailed information on why and when some permissions are requested, the corresponding column in the Table 1 concerning the justification of the permissions has a "No" value for all apps, despite the fact that for some apps this issue is more prevalent than in others (see Fig. 3). In a similar manner, all apps are characterized in the Table 1 as non-compliant with the requirement to process data upon a valid user's consent, but this seems to be ensured only for some of them; the remaining do not provide clear information on the matter (and this is a transparency issue, even if the consents obtained are, in fact, valid).

5.4 Security aspects

We also examined, through the ImmuniWeb Community Edition—Mobile App Security Test tool whether the examined smart apps have some security issues. More precisely, we focused on identifying whether this tool finds out major or medium security risks; this severity classification is based on the OWASP Mobile Top 10 List [64], which include various misconfigurations or weaknesses of the mobile apps that could allow an attacker, under specific circumstances, to compromise the mobile app's data security. This list, for the period that our experiments took place (i.e., March-April 2023) was the following:

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Lack of Cryptography

Table 1 Evaluating the personal data processes, based on the privacy policies

App	Clearly defined	Valid	Permissions	Precise info	Other issues
	Processes?	Consent?	Justified?	On Third Parties?	Identified?
Airbnb	No	No	No	No	Yes
Amazon Shopping	Partially	No	No	No	No
Facebook/ Instagram	Partially	No	No	Yes	No
Google Map	Partially	No	No	Yes	Yes
Netflix	No	No	No	No	No
Nike Training	No	No	No	Yes	Yes
Spotify	Partially	No	No	Yes	No
TikTok	No	No	No	Partially	Yes
Waze	No	No	No	Partially	No

Table 2 Security risks for the Airbnb app

Risk	Classification	Severity
Cleartext SQLite Database	M3 / CWE-312	High
Unencrypted http protocol	M3 / CWE-319	High
Exposure of potentially sensitive data	M2 / CWE-200	Medium
Hardcoded sensitive data	M10 / CWE-200	Medium
JS enabled in a webview	M10 / CWE-749	Medium

- M6: Insecure Authorization
- M7: Poor Client Code Quality
- M8: Code Manipulation
- M9: Reverse Engineering
- M10: Extraneous Functionality

In the presentation of the results that follow, we should consider that CWE (Common Weakness Enumeration) corresponds to the relevant unique identification number of a well-known community-developed list by MITRE of common software and hardware weakness types [65]. Hence, the classification is presented according to both OWASP and MITRE, whereas the severity for each risk is presented according to the evaluation that the ImmuniWeb has performed. Note that ImmuniWeb performs both static and dynamic application security tests.

5.4.1 The Airbnb app

During the analysis of the application, 5 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 2.

Table 3 Security risks for the Amazon shopping app

Risk	Classification	Severity
External data storage	M2 / CWE-921	Medium
JS enabled in a webview	M10 / CWE-749	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium

The analysis also illustrated that there exist HTTP/S requests that take place without user's interaction, which include GET requests from https://graph.facebook.com and POST requests to https://notify.bugsnag.com.

5.4.2 The Amazon shopping app

During the analysis of the application, 3 risks of medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 3.

Moreover, this tool identified that this app also requires the `CALL_PHONE` permission, which is an additional high-risk permission compared to those found out by the previous tools.

Table 4 Security risks for the Facebook app

Risk	Classification	Severity
Weak hashing algorithm	M5 / CWE - 916	Medium

Table 5 Security risks for the Instagram app

Risk	Classification	Severity
Possible man-in-the-middle attack	M3 / CWE-297	High
Hardcoded sensitive data	M10 / CWE-200	Medium
External data storage	M2 / CWE-921	Medium
Enabled application backup	M2 / CWE-921	Medium
Weak encryption	M5 / CWE-327	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium
JS enabled in a webview	M10 / CWE-749	Medium

5.4.3 The Facebook app

During the analysis of the application, 1 risk of medium importance, that is generally included in the OWASP Mobile Top 10 Security Test list, has been identified; this is illustrated in Table 4.

Moreover, this tool identified that this app also requires the `CALL_PHONE` permission, which is an additional high-risk permission compared to those found out by the previous tools.

5.4.4 The Instagram app

During the analysis of the application, 7 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 5.

Moreover, this tool identified that this app also requires the `READ_CALENDAR` and the `USE_CREDENTIALS` permissions, which are additional high-risk permissions compared to those found out by the previous tools.

5.4.5 The GoogleMaps app

During the analysis of the application, 7 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 6.

Moreover, this tool identified that this app also requires the `USE_CREDENTIALS` and `MANAGE_ACCOUNTS` permissions, which are additional high-risk permission compared to those found out by the previous tools.

Table 6 Security risks for the Google Maps app

Risk	Classification	Severity
Cleartext SQLite Database	M3 / CWE-312	High
External data in SQL queries	M7 / CWE-89	Medium
Unencrypted http protocol	M3 / CWE-319	Medium
External data storage	M2 / CWE-921	Medium
Enabled application backup	M2 / CWE-921	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium
JS enabled in a webview	M10 / CWE-749	Medium

Table 7 Security risks for the Netflix app

Risk	Classification	Severity
Weak encryption	M5 / CWE-327	Medium
Weak hashing algorithms	M5 / CWE - 916	Medium
JS CORS enabled in a webview	M10 / CWE-749	Medium
JS enabled in a webview	M10 / CWE-749	Medium

5.4.6 The Netflix app

During the analysis of the application, 4 risks of medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 7.

5.4.7 The Nike training app

During the analysis of the application, 9 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 8.

Moreover, this tool identified that this app also requires the `CALL_PHONE` permission, which is an additional high-risk permission compared to those found out by the previous tools.

5.4.8 The Spotify app

During the analysis of the application, 6 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 9.

Moreover, this tool identified that this app also requires the `USE_CREDENTIALS` permission, which is an additional high-risk permission compared to those found out by the previous tools.

Table 8 Security risks for the Nike Training app

Risk	Classification	Severity
Cleartext SQLite Database	M3 / CWE-312	High
External data in SQL queries	M7 / CWE-89	High
Unencrypted http protocol	M3 / CWE-319	High
Exposure of potentially sensitive data	M2 / CWE-200	Medium
Hardcoded sensitive data	M10 / CWE-200	Medium
Weak encryption	M5 / CWE-327	Medium
External data storage	M2 / CWE-921	Medium
JS enabled in a webview	M10 / CWE-749	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium

Table 9 Security risks for the Spotify app

Risk	Classification	Severity
Cleartext SQLite Database	M3 / CWE-312	High
External data in SQL queries	M7 / CWE-89	High
Hardcoded sensitive data	M10 / CWE-200	Medium
External data storage	M2 / CWE-921	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium
JS enabled in a webview	M10 / CWE-749	Medium

Table 10 Security risks for the TikTok app

Risk	Classification	Severity
Hardcoded sensitive data	M10 / CWE-200	Medium
External data storage	M2 / CWE-921	Medium
JS enabled in a webview	M10 / CWE-749	Medium
JS CORS enabled in a webview	M10 / CWE-749	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium

5.4.9 The TikTok app

During the analysis of the application, 5 risks medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 10.

Moreover, this tool identified that this app also requires the `GET_TASKS` as well as the `AUTHENTICATE_ACCOUNTS` permissions, which are additional high-risk permissions compared to those found out by the previous tools.

5.4.10 The Waze app

During the analysis of the application, 9 risks of major or medium importance, that are generally included in the OWASP Mobile Top 10 Security Test list, have been identified; this is illustrated in Table 11.

Moreover, this tool identified that this app also requires the `USE_CREDENTIALS`, the `MANAGE_ACCOUNTS` as well as the `AUTHENTICATE_ACCOUNTS` permissions, which are additional high-risk permissions compared to those found out by the previous tools.

5.4.11 Summary

Our analysis illustrates that the apps studied are not free of known software security issues. A question that naturally arises is which exactly are the practical security risks for the users, pertaining to these security issues. This question though has not a straightforward answer, taking into account the whole ecosystem of databases concerning weaknesses, vulnerabilities and their impacts. More precisely, MITRE produces a list of known vulnerabilities, being called the CVE (Common Vulnerabilities and Exposure) list, whereas each CVE is associated with one or more CWEs. Then, this CVE list is provided to another organisation, being called NVD (National Vulnerability Database), in order to compute the so-called CVSS (Common Vulnerability Scoring System) score, aiming to provide an overview of the severity of a vulnerability (which, as stated above, could depend on more than one weaknesses). This scoring system in turn incorporates, for each vulnerability, several factors including its impact and its easiness for exploitation by an attacker. Moreover, it is widely known that using only the CVSS score for security risk assessment is a wrong approach - see, e.g., [66].

Therefore, on the basis of the above, it is not easy to state that a specific weakness from the CWE list leads, per se, to a specific security attack with high probability. However, we may refer to a list being called *CWE Top* 25 *Most Dangerous Software Weaknesses* that MITRE issues on an annual basis. According to this list for the year 2023 [67], the CWE-89 software weakness, that has been identified by our analysis in the Google Map, Spotify and Waze apps, is being ranked as 3rd, illustrating that it is generally considered as of high impor-

Table 11 Security risks for the Waze app

Risk	Classification	Severity
Cleartext SQLite Database	M3 / CWE-312	High
External data in SQL queries	M7 / CWE-89	High
Unencrypted http protocol	M3 / CWE-319	High
Exposure of potentially sensitive data	M2 / CWE-200	Medium
External data storage	M2 / CWE-921	Medium
Enabled application backup	M2 / CWE-921	Medium
Weak hashing algorithm	M5 / CWE - 916	Medium
JS CORS enabled in a webview	M10 / CWE-749	Medium
JS enabled in a webview	M10 / CWE-749	Medium

tance (note that the ImmuniWeb also evaluates this weakness as of high severity).

6 Discussion

The above analysis illustrates that personalisation comes along with several data protection and security concerns. These can be summarised as follows (being presented in relation with the initial research questions Q1-Q5 formulated in Sect. 1.1):

- Some personalisation services, and especially (although not exclusively) those that are related with personalised advertising, seem to be by default enabled without requiring the user's consent (and possibly the users cannot even object, at a later stage, to this processing). Even if the privacy policy refers to the consent as the corresponding legal basis for this process (this is indeed the case for a few cases), it is not clear that such a consent can be, indeed, freely given. In other cases though, it is not even clear if some processes are by default enabled or not (see Q4).
- In several cases, the various purposes of the data processes are being described in a unified way, so as that it is not clear for the user which exactly personal data are needed for each purpose, as well as which is the legal basis for each purpose. More precisely, the provision of personalised services, as well as other purposes that are not related with personalisation, are being jointly described in the privacy policies and this clearly may confuse users. More generally, some privacy policies seem to be unclear and, thus, some of the findings obtained through our analysis with respect to the underlying personal data processes that take place cannot be justified easily (see Q1).
- In relation with the above, some data processes, as they are being implied by the permissions that the corresponding apps require, seem to be quite excessive or, at least, unjustifiable. In principle, there is not an explicit mapping between the Android app's permissions and the corresponding data processing purposes (see Q2); this is actually though an issue that is being found in all Android apps, not only in those providing personalised services—see, e.g, [16]. Although a permission, as also stated above, is associated with API calls and such API calls could possibly be in line with the data minimisation and purpose limitations principles, the fact that the privacy policy does not provide answers to questions of the form "why is this permission needed?" should be considered as problematic in terms (at least) of the requirement for transparency of the processes (see Q1).
- There is no sufficient information on the third parties that may get access to users' data for various purposes, whilst even the countries that personal data are being sent are not described (in most cases, we noticed that there are more than one destination countries, since data are being sent to several data processors) (see Q3).
- Some apps seem also to process data from individuals that do not use these apps; this is typically the case that a user allows such an access (e.g. through allowing the app getting access to her/his contacts). Moreover, one app—namely, the TikTok—seems to perform a process that could be considered as highly intrusive in terms of privacy, since it monitors user's data even if the user actually will not choose to transmit/upload these data through the app (see Q2).
- Interestingly enough, the majority of the apps examined is not free of security weaknesses; even if it is not straightforward to state that these weaknesses yield security risks with high probability and severity (since we have not examined, for the reasons explained in Sect. 5.4.11, whether these weaknesses correspond to specific vulnerabilities that could be practically exploited and, if yes, with which consequences), it is of interest to see that well-known (and, thus, easily manageable) weaknesses are present in such popular apps (see Q5).

Therefore, we get that—as a general observation—the providers of personalized services tend to assume that users are willing to allow the processing of their personal data without clearly informing them on the necessity and the risks of this process. Moreover, it is quite probable that some personal data that are being collected are quite excessive or, at least, with an ambiguous legal basis (which in turn contradicts the requirement for the transparency of the process). In principle, the apps providing personalised services seem somehow to inherit all the main data protection concerns spanning the entire Android ecosystem, which are further accentuated by the fact the providers of these services seem to assume that many processes are by default allowed by the user. In essence, the fulfilment of the transparency and data minimisation of the process seems to not be ensured, which in turn yields questions on the fulfilment of the data protection by design and by default principles; the overall security of the apps needs also further consideration.

During the process of writing this paper, the European Data Protection Board issued a binding decision [55] related with the personalised advertisements provided by the Facebook and Instagram (both under the Meta Company). Without getting into many details of this matter which go beyond the scope of the paper, the main outcome is that Meta is forced (through the competent Data Protection Supervisory Authority in Europe) to change the legal basis for this process, which was previously assumed to be the company's legitimate interests—and, thus, no user's consent was required for such a personalisation. In response to this, Meta has now proceeded in a so-called "Pay or Okay" model in Europe, which means that the users are being asked whether they provide their consent for personalised advertisements and, if not, then they need to pay a fee, on a monthly basis (between 9.99 and 12.99 Euro), in order to still use the corresponding applications/services, being free of personalised advertisements (and, thus, without being profiled for advertisement purposes). We believe that this is not the end of the story; it is still questionable whether this new practice can be considered as compliant with the requirement to protect fundamental rights such as personal data protection and, indeed, specific complaints on this matter have been also raised (see [68]). The above case though indicates how challenging is this field.

7 Conclusions

Personalisation constitutes a main challenge from both legal as well as a technical perspective, being nicely described by the so-called personalisation-privacy paradox [39]. Our work indicates that, unfortunately (although one could say but not unexpectedly), in the smart app ecosystem the relevant privacy issues are further accentuated. Many providers seem to collect and further process several types of personal data with no clear information on the relevant purposes and their necessity, whereas it is pre-assumed that the users provide their consent for some of these processes; it is questionable though if the users would provide their consent for all such processes if they were fully aware of them.

Moreover, as stated previously, the smart apps providing personalised services seem to inherit all the main weaknesses, in terms of privacy and personal data protection, that inherently occur in the smart mobile ecosystem; for example, there are third-party trackers also collecting personal data, without the users being explicitly informed on this. In a similar manner, several high-risk permissions for accessing device are being required by the apps; if a users allows such permissions (which is typically the case since, otherwise, the app states that *it will not work properly*), then these permissions are also granted to third-party trackers.

It is interesting to point out that our work indicates that the various tools that we have used to monitor/examine the apps' behavior present some small discrepancies into their outcomes; this further illustrates the need for further research in this field. Of course, the inherent features of static and dynamic analysis indicate that one may see differences between these two approaches in terms of the results of the analyses; however, things are much more complicated than this. For instance, as indicated in [17], there is a number of publicly available API methods, as well as of protected API methods, that do not report the corresponding permission neither in the Android framework nor in the public documentation; hence, even the permissions analysis do not reveal the whole picture of the underlying personal data processes. In light of the above, we may point out that the lack of open standardised tools to effectively monitor what apps do in real time constitutes a significant impeding factor, which in turns poses limitations to our research.

Although this paper studied only ten apps, the fact that these apps—which are of high popularity—seem to share somehow the same privacy concerns/issues (of course, up to different extents), leads to the conclusion that the results obtained do reflect the generic problem. In any case though, it is of importance to further examine more apps, possibly with also different tools, so as to enrich the outcomes and our conclusions. To this end, the methodology adopted in this work (see Fig. 1) can be the basis for any subsequent analysis, having as input any possible app and using any tools for static/dynamic analyses considered as appropriate. Future research steps could also focus on a wider set of apps providing personalised services, not only in Android but also in iOS platforms. In addition, it would be of high value to further focusing on performing dynamic analysis of the apps, capturing exactly what they are doing in real time for specific conditions (i.e., to see exactly which personal data they collect). Of course, the issue of what constitutes a valid consent

is also of high importance—taking into account the discussion that has recently started in Europe based on the case of Meta.

Concluding, we get that the current legal framework, in conjunction with the practical guidance, cannot be considered as sufficient since it may leave some room for manoeuvre for the apps providers to rely on the the provision of personalised services in order to collect more personal data than they actually need. Hence, pre-assuming that the user agrees with a process, without even giving her/him the option to object to the process at a later stage, is a rather problematic situation that is, unfortunately, widely adopted. Therefore, the important notions of data protection by design and by default need to be further materialised so as to avoid any ambiguities. In the same manner, appropriate data protection engineering techniques should be further promoted, in order to provide the means for the apps providers to comply with the legal requirements; for example, the access to user's personal data by third parties can be fully under the control of the user, having full transparency for each step of the overall process. To this end, the existing Android model that allows third-party libraries to inherit the privileges that the host app has needs to be thoroughly re-considered. The role of all stakeholders (apps providers, apps developers, operating system/platform providers, data protection authorities etc.) is very important; the aforementioned recent example of the binding decision that EDPB issued concerning the Meta company and the legal basis of the personalised advertisements shows exactly this, illustrating that we are still in a highly evolving environment.

Acknowledgements The authors would like to thank the anonymous reviewers for their thorough study and their very constructive comments and suggestions, which helped to greatly improve the manuscript.

Declarations

Conflict of interest The authors declare that they have no Conflict of interest.

Ethics approval This article does not contain any studies with human participants or animals performed by any of the authors.

Data availability All data generated or analyzed during this study are included in this published article. The software tools that have been used for the analysis are available in public.

References

1. Hajjaji, Y., Boulila, W., Farah, I.R., Romdhani, I., Hussain, A.: Big data and IoT-based applications in smart environments: a systematic review. Comput. Sci. Rev. **39**, 100318 (2021). https://doi.org/10.1016/j.cosrev.2020.100318
2. OECD: E-commerce in the time of COVID-19 (2020). Available in https://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/ https://www.forbes.com/sites/blakemorgan/2020/02/18/50-stats-showing-the-power-of-personalization/?sh=7ce8a77a2a94
3. Nandy, M., Lodh, S., Tang, A.: Lessons from Covid-19 and a resilience model for higher education. Ind. High. Educ. **35**(1), 3–9 (2021). https://doi.org/10.1177/0950422220962696
4. Xiao, Y., Becerik-Gerber, B.D., Lucas, G., Roll, S.C.: Impacts of working from home during COVID-19 pandemic on physical and mental well-being of office workstation users. J. Occup. Environ. Med. **63**(3), 181–190 (2021). https://doi.org/10.1097/JOM.0000000000002097
5. McKinsey & Company: How COVID-19 has pushed companies over the technology tipping point-and transformed business forever, (2020). Available in https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
6. Morgan, B.: 50 Stats showing The Power Of Personalization (2020). Available in https://www.forbes.com/sites/blakemorgan/2020/02/18/50-stats-showing-the-power-of-personalization/?sh=7ce8a77a2a94 (Accessed on May 14th, 2024)
7. Tay, S.W., Teh, P.S., Payne, S.J.: Reasoning about privacy in mobile application install decisions: risk perception and framing. Int. J. Hum Comput Stud. **145**, 102517 (2021). https://doi.org/10.1016/j.ijhcs.2020.102517
8. European Union Agency for Cybersecurity: Privacy and Data Protection in Mobile Applications—A Study on the App Development Ecosystem and the Technical Implementation of GDPR (2017). Available in https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications. (Accessed on May 14th, 2024)
9. Michael, J., Kuhn, R., Voas, J.: Security or privacy: can you have both? Computer **53**, 20–30 (2020). https://doi.org/10.1109/MC.2020.3004606
10. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation). Off. J. L. 119(1) (2016)
11. Kaminski, M.: A recent renaissance in privacy law. Commun. ACM **63**(9), 24–27 (2020). https://doi.org/10.1145/3411049
12. Alshammari, M., Simpson, A.: Towards a Principled Approach for Engineering Privacy by Design. In: Schweighofer, E., Leitold, H., Mitrakas, A., Rannenberg, K. (eds.) Privacy Technologies and Policy - APF 2017 10518, pp. 161–177. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-67280-9_9
13. European union agency for cybersecurity: recommendations on shaping technology according to GDPR provisions—Exploring the notion of data protection by default (2019). Available in https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2
14. European Data Protection Board: Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (2023). Available in https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en (Accessed on May 14th, 2024)
15. Statcounter: Mobile Operating System Market Share Worldwide (2023). Available in https://gs.statcounter.com/os-market-share/mobile/worldwide (Accessed on May 14th, 2024)
16. Achilleos, G., Limniotis, K.: Exploring personal data processing in video conferencing apps. Electronics **12**(5), 1247 (2023). https://doi.org/10.3390/electronics12051247
17. Lyvas, C., Lambrinoudakis, C., Geneiatakis, D.: Dypermin: dynamic permission mining framework for android platform. Comput. Secur. **77**, 472–487 (2018). https://doi.org/10.1016/j.cose.2018.05.007

18. Kurtz, A., Gascon, H., Becker, T., Rieck, K. and Freiling. F.: Fingerprinting mobile devices using personalized configurations. In: Proceedings on privacy enhancing technologies, pp. 4–19 (2016). https://doi.org/10.1515/popets-2015-0027
19. Bilgihan, A., Kandampully, J., Zhang, T.: Towards a unified customer experience in online shopping environments: antecedents and outcomes. Int. J. Qual. Serv. Sci. **8**(1), 102–119 (2016). https://doi.org/10.1108/IJQSS-07-2015-0054
20. Levenson, H.: Mobile App Personalization: How To Do It Right (2018). Available in https://usabilitygeek.com/mobile-app-personalization-how-to/ (Accessed on May 14th, 2024)
21. Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., Shadbolt, N.: Third Party Tracking in the Mobile Ecosystem. arXiv:1804.03603v3 [cs.CY] (2018). Available in https://arxiv.org/pdf/1804.03603.pdf (Accessed on May 14th, 2024)
22. Okoyomon, E., Samarin, N., Wijesekera, P., Elazari, A., Vallina-Rodriguez, N., Reyes, I., Feal, A., Egelman, S.: On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies. In: The workshop on technology and consumer protection (ConPro '19) (2019)
23. Bracamonte, V., Pape, S., Löbner, S.: "All apps do this": Comparing Privacy Concerns Towards Privacy Tools and Non-Privacy Tools for Social Media Content. Proc. Priv. Enhancing Technol., pp. 57–78 (2022). https://doi.org/10.56553/popets-2022-0062
24. Monogios, S., Magos, K., Limniotis, K., Kolokotronis, N., Shiaeles, S.: Privacy issues in android applications: the cases of GPS navigators and fitness trackers. Int. J. Electron. Gov. (IJEG) **14**, 83–111 (2022). https://doi.org/10.1504/IJEG.2022.123245
25. Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C.: Security and privacy analysis of mobile health applications: the alarming state of practice. IEEE Access **6**, 9390–9403 (2018). https://doi.org/10.1109/ACCESS.2018.2799522
26. Son, S., Kim, D. and Shmatikov, V.: What mobile ads know about mobile users. In: Network and distributed system security symposium (2016). 0.14722/ndss.2016.23407
27. Taylor, V. F., Beresford, A. R., Martinovic, I.: Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones. arXiv:1708.03520v1 [cs.CR] (2017). https://doi.org/10.48550/arXiv.1708.03520
28. Reyes, I., Wijesekera, P., Razaghpanah, A., Reardon, J., VallinaRodriguez, N., Egelman, S., Kreibich, C.: Is Our Children's Apps Learning? Automatically detecting COPPA violations, IEEE Workshop on Technology and Consumer Protection (ConPro) (2017)
29. Chatzistefanou, V., Limniotis, K.: Anonymity in social networks: the case of anonymous social media. Int. J. Electron. Gov. **11**, 361–385 (2019). https://doi.org/10.1504/IJEG.2019.103720
30. Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., Gill, P.: Apps, trackers, privacy, and regulators: a global study of the mobile tracking ecosystem. In: Network and distributed system security symposium (2018). https://doi.org/10.14722/ndss.2018.23353
31. de Mattos, E.P., Domingues, A.C.S.A., Santos, B.P., Ramos, H.S., Loureiro, A.A.F.: The impact of mobility on location privacy: a perspective on smart mobility. IEEE Syst. J. **16**(4), 5509–5520 (2022). https://doi.org/10.1109/JSYST.2022.3147808
32. Kollnig, K., Binns, R., Dewitte, P., Van Kleek, M., Wang, G., Omeiza, D., Webb, H., Shadbolt, N.: A fait accompli? An empirical study into the absence of consent to third-party tracking in android apps. In: Proceedings of the 17th symposium on usable privacy and security (2021). Available in https://www.usenix.org/system/files/soups2021-kollnig.pdf (Accessed on May 14th, 2024)
33. Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., Shadbolt, N.: Are iPhones really better for privacy? A comparative study of iOS and android apps. Proc. Priv. Enhancing Technol. (POPETS), pp. 6–24 (2022). https://doi.org/10.2478/popets-2022-0033
34. Riegger, A., Klein, J.F., Merfeld, K., Henkel, S.: Technology-enabled personalization in retail stores: understanding drivers and barriers. J. Bus. Res. **123**, 140–155 (2021). https://doi.org/10.1016/j.jbusres.2020.09.039
35. Ullah, I., Boreli, R., Kanhere, S.S.: Privacy in targeted advertising on mobile devices: a survey. Int. J. Inf. Secur. **22**, 647–678 (2023). https://doi.org/10.1007/s10207-022-00655-x
36. Ameen, N., Hosany, S., Paul, J.: The personalisation-privacy paradox: consumer interaction with smart technologies and shopping mall loyalty. Comput. Hum. Behav. **126**, 106976 (2022). https://doi.org/10.1016/j.chb.2021.106976
37. Pérez-Troncoso, D., Epstein, D.M., Castañeda-García, J.A.: Consumers' preferences and willingness to pay for personalised nutrition. Appl. Health Econ. Health Policy **19**(5), 757–767 (2021). https://doi.org/10.1007/s40258-021-00647-3
38. Volchek, K., Yu, J., Neuhofer, B., Egger, R., Rainoldi, M.: Co-creating personalised experiences in the context of the personalisation-privacy paradox. Inform. Commun. Technol. Tour (2021). https://doi.org/10.1007/978-3-030-65785-7_8
39. Kokolakis, S.: Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Sec. **64**, 122–134 (2017). https://doi.org/10.1016/j.cose.2015.07.002
40. Au, K. W. Y., Zhou, Y. F., Huang, Z. and Lie, D.: PScout: Analyzing the android permission specification. In: Proceedings of the 19th ACM conference on computer and communications security (CCS), Oct (2012). https://doi.org/10.1145/2382196.2382222
41. Zhao, Z., Osono, F. C. C.: TrustDroid: Preventing the use of smartphones for information leaking in corporate networks through the used of static analysis taint tracking. In: 7th International conference on malicious and unwanted software, Fajardo, PR, USA, pp. 135–143 (2012). https://doi.org/10.1109/MALWARE.2012.6461017
42. Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., Traon, Y.L., Octeau, D., McDaniel, P.: FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. ACM SIGPLAN Not. **49**, 259–269 (2014). https://doi.org/10.1145/2666356.2594299
43. Backes, M. Bugiel, S., ,Derr, E., McDaniel, P., Octeau, D., Weisgerber, S.: On demystifying the Android application framework: re-visiting android permission specification analysis. In: Proceedings of the 25th USENIX security symposium (USENIX Security), Austin, TX., USENIX Association, pp. 1101–1118 (2016). Available in https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_backes-android.pdf (Accessed on May 14th, 2024)
44. Lee, S. Hwang, S., Ryu, S.: All about activity injection: threats, semantics, and detection. In: 32nd IEEE/ACM international conference on automated software engineering (ASE), IEEE, pp. 252-262 (2017). https://doi.org/10.1109/ASE.2017.8115638
45. Spreitzer, R., Palfinger, G., Mangard, S.: SCAnDroid: Automated side-channel analysis of android APIs. In: Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks (WiSec), pp. 224–235 (2018). https://doi.org/10.1145/3212480.3212506
46. Carlsson, A., Pedersen, C., Persson, F. and Söderlund, G.: KAUDroid—a tool that will spy on applications and how they spy on their users. Working paper, 2018. Available in https://www.diva-portal.org/smash/get/diva2:1179950/FULLTEXT01.pdf (Accessed on May 14th, 2024)
47. Burguera, I., Zurutuza, U., Nadjm-Tehrani, S.: Crowdroid: Behavior-based malware detection system for Android. In: Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices (SPSM), pp. 15–26 (2011). https://doi.org/10.1145/2046614.2046619

48. Shabtai, A., Kanonov, U., Elovici, Y., Weiss, Y.: Andromaly: a behavioral malware detection framework for android devices. J. Intell. Inf. Syst. **38**, 161–190 (2012). https://doi.org/10.1007/s10844-010-0148-x
49. Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P. D., Sheth, A, N.: TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. ACM Trans. Comput. Syst. **32**, 1–29 (2014). https://doi.org/10.1145/2619091
50. Tam, K., Khan, S. J., Fattori, A., and Cavallaro, L.: CopperDroid: automatic reconstruction of Android malware behaviors. NDSS '15, 8–11 Feb 2015, San Diego, CA, USA (2015). https://doi.org/10.14722/ndss.2015.23145
51. Lyvas, C., Lambrinoudakis, C., Geneiatakis, D.: On Android's activity hijacking prevention. Comput. Secur. **111**, 102468 (2021). https://doi.org/10.1016/j.cose.2021.102468
52. Titze, D., Stephanow, P., Schuette, J.: App-Ray: user-driven and fully automated android app security assessment report. Available in https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/2014_03 (2013)
53. Liu, J., Wu, D., Xue, J.: Tdroid: Exposing app switching attacks in android with control flow specialization. In: Proceedings of the 33rd ACM/IEEE international conference on automated software engineering, pp. 236–247 (2018). https://doi.org/10.1145/3238147.3238188
54. Gajrani, J., Agarwal, U., Laxmi, V., Bezawada, B., Gaur, M.S., Tripathi, M., Zemmari, A.: EspyDroid+: precise reflection analysis of android apps. Comput. Sec. **90**, 101688 (2020). https://doi.org/10.1016/j.cose.2019.101688
55. European data protection board: urgent binding decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) (2023). Available in: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf (Accessed on May 14th, 2024)
56. Exodus Privacy. https://exodus-privacy.eu.org/en/ (Accessed on May 14th, 2024)
57. Tracker Control for Android. https://trackercontrol.org/ (Accessed on May 14th, 2024)
58. ImmuniWeb for Mobile App Security. https://www.immuniweb.com/mobile/ (Accessed on May 14th, 2024)
59. Naeem, A.: Apps that Americans can't live without (2023). Available in https://www.digitalinformationworld.com/2023/10/apps-that-americans-cant-live-without.html. (Accessed on May 14th, 2024)
60. Du, T.: Ranked: The World's Most Popular Apps by Downloads (2023). Available in https://www.visualcapitalist.com/cp/most-popular-apps-by-downloads/#google_vignette (Accessed on May 14th, 2024)
61. Leo, K.: Manage External Storage Permission -Android Studio - Java (2023). https://medium.com/@kezzieleo/manage-external-storage-permission-android-studio-java-9c3554cf79a7 (Accessed on May 14th, 2024)
62. Li, L., Bissyandé, T.F., Papadakis, M., Rasthofer, S., Bartel, A., Octeau, D., Klein, J., Le Traon, Y.: Static analysis of android apps: a systematic literature review. Inf. Softw. Technol. **88**, 67–95 (2017). https://doi.org/10.1016/j.infsof.2017.04.001
63. Hatamian, M., Wairimu, S., Momen, N., Fritsch, L.: A privacy and security analysis of early-deployed COVID-19 contact tracing android apps. Empir Softw. Eng **26**, 36 (2021). https://doi.org/10.1007/s10664-020-09934-4
64. OWASP: Mobile Top 10 (2023). https://owasp.org/www-project-mobile-top-10/ (Accessed on May 14th, 2024)
65. MITRE: CWE List Version 4.13. https://cwe.mitre.org/data/index.html (Accessed on May 14th, 2024)
66. Campagna, R.: 5 Reasons to Stop Using CVSS Scores to Measure Risk. https://www.balbix.com/blog/5-reasons-to-stop-using-cvss-scores-to-measure-risk/ (Accessed on May 9th, 2024)
67. MITRE: 2023 CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html (Accessed on May 9th, 2024)
68. NOYB: NOYB files GDPR complaint against Meta over "Pay or Okay". https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay. (Accessed on May 9th, 2024)