Using the metadata-based App-PI ecosystem to assess the privacy impact of Health apps*

M. Mercedes Martínez-González[1 [0000−0002−3151−0842]], Alejandro Pérez-Fuente[1 [0009−0006−9717−0824]], Amador Aparicio[1 [0000−0003−2546−9246]], and Pablo A. Criado-Lozano[1,2 [0009−0002−7038−6378]]

[1] Privacy Engineering Research Group, University of Valladolid (Spain)
gi.ingpriv@uva.es
{mercedes,amador}@infor.uva.es
alejandro.perez.fuente@uva.es
[2] Universidad Europea Miguel de Cervantes (Valladolid, Spain)
pacriado@uemc.es

Abstract. Mobile applications (apps) facilitate the management of devices and sensors from mobile devices in IoE environments. However, their use carries risks for the privacy of their users: many of them manage personal data. The App-PI (App Privacy Impact) ecosystem analyzes the impact of apps on privacy, addressing the challenge of knowing, understanding and mitigating these risks.

In App-PI, a metadata warehouse, a set of analysis tools that calculate indicators, a visualization platform, and verification processes, collaborate. Data flows between these components to provide persons using the visualization platform with accurate, reliable, and understandable information. The warehouse hosts metadata related to the privacy and security of mobile apps. The data flow starts with the collection and integration of data hosted in the warehouse. The analysis tools use these data to calculate indicators that provide objective measures of the risk associated with each app. These values are the input for a verification process based on static analysis, which provides confidence. To make it easier for end users to understand these indicators, they are displayed on the visualization platform with easy-to-understand charts. The flows and usefulness of this ecosystem are shown for health and wellness apps, characteristic of IoE environments.

Keywords: Privacy · Metadata · Mobile Apps · Health Apps · IoE.

* This version of the contribution has been accepted for publication, after peer review (when applicable) but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: http://dx.doi.org/10.1007/978-3-031-77571-0. Use of this Accepted Version is subject to the publisher's Accepted Manuscript terms of use https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms.

1 Introduction

Mobile applications (apps) facilitate the management of devices and sensors from mobile devices in IoE (Internet of Everything) environments. Among mobile apps, health apps have become increasingly popular, providing users with accessible ways to manage their health and wellness. However, sensors provide personal data, that is, data whose access by non-desired third parties violates user privacy. Prevention of this issue is logical, especially in a world in which the amount of data breaches increases every day [11]. The tool that users have to self-protect their privacy when using mobile apps is their device settings. There are some analysis tools that help users to check app privacy impact. However, most of them use concepts that do not correspond to what users can handle, which hinders their ability to translate those results into effective self-protection. Also related to the ability of users to protect themselves is the issue of the readability of privacy policies. According to the General Data Protection Regulation (GDPR)[3], privacy policies should provide to end users clear and transparent information to know how to tune these Settings. Actually, the readability of privacy policies has not improved since GDPR got into force as much as pretended [19]. Therefore, end users need easy to understand tools that help them to make good decisions to protect their privacy.

One problem for Privacy Enhancing Technologies (PET) developers working for mobile environments is that it is difficult to find repositories with quality metadata that can be used as input data. There are few of them, and those that do exist often focus on security issues, which do not necessarily include privacy issues. In the App-PI (App Privacy Impact) ecosystem a set of tools and processes collaborate to offer a set of services that can be used by end users and/or developers. The impact of apps on privacy is evaluated using privacy impact metrics. Their results are offered in multiple formats and views, based on concepts accessible to any type of user. The data used for these analysis are read from the App-PIMD (App-PI MetaData) warehouse. In App-PIMD, metadata about the privacy and security of mobile applications is stored and can be accessed by means of an API (Application Program Interface). In order to ensure data quality, the results obtained by privacy indicators a set of static analysis processes are available, in which we verify metadata used to calculate indicators. To our knowledge, there is no similar ecosystem in which visualization tools, a metadata warehouse, indicators, and verification processes collaborate to ensure the provision of quality data to PET developers, while also having the quality of being easy to use.

The flows, and the usefulness of this ecosystem, are shown in a health and wellness app, characteristic of IoE environments. We have chosen *Samsung Health*[4] to illustrate the data flow in the App-PI ecosystem. We have chosen it because it is one of the most popular health apps, and it also has good documentation

[3] Recital 58, The Principle of Transparency.
[4] Version 6.27.0.161.

about the way personal data is collected and treated[5]. However, its management of personal data is still be viewed with caution [25].

An introduction to the privacy issue in mobile apps is offered in section 2. In section 3, we present the App-PI ecosystem and how it works on a health app, *Samsung Health*. In section 4, the main conclusions are presented, while ideas for future work follow in section 5.

2 Privacy and health apps in IoE

Health apps have become increasingly popular, providing users with convenient and accessible ways to manage their health and wellness. The health app industry generated $3.43 billion in 2023, a 9.9% increase on the previous year, and were downloaded a total of 379 million times in 2023[6]. However, there are concerns about privacy and data protection. Sensors provide health data, which are collected and analyzed by health apps, which themselves exchange these data with servers, on which improved analytics of these health data can be obtained. Data sharing and security risks derived from data breaches that can compromise user data are two issues behind these concerns. In our opinion, users need tools easy to understand and to use, irrespective of whether or not they are so accurate as other tools can be. In this way, they can be active in their self-protection.

Health apps use data obtained from sensors, such as blood pressure, glucose level, etc. Access to these data, which are especially private, has been organized by Google since October 2023 (Android 14)s in a special permission group, HealthPermissions[7]. Access to these permissions is done through the HealthConnect on-device data store, which provides APIs for storing and sharing health and fitness data between Android apps.

2.1 Privacy assurance in mobile apps

User privacy when using apps has been a constant concern since they became popular [20, 17, 8, 3]. To help users, the most important markets for app downloading, Google Play and Apple App Store, have recently introduced information about data security. This information, which users can consult in the market itself, is based on statements that the developers provide voluntarily. Google has begun to promote these practices more recently than Apple, since 2021 [7].

Both markets offer information about the apps' possible access to a set of data categories. In Android, these categories relate to the logical groups of permissions that users can find in their device's Settings. Permissions are the mechanism that Android uses to control access to personal data handled by [18] applications. In fact, this is the only mechanism that Android offers users to empower themselves

[5] https://eu.community.samsung.com/t5/mobile-apps-services/samsung-health-permissions/td-p/3252751

[6] Source: `https://www.businessofapps.com/data/health-app-market/`.

[7] `https://developer.android.com/reference/android/health/connect/HealthPermissions`

in protecting their privacy. They have no further capacity for action, except for the decision of whether or not to install an app. The relationship (*personal data*, *permission*) has motivated various works that investigate whether it is possible to determine the level of risk for the security and/or privacy of users derived from mobile applications based on permissions. Among the proposals are measures to analyze the privacy impact of mobile applications [5, 14, 21, 2]. Shrivastava et al. offer in [22] a compendium of the research carried out between 2010 and 2020. In general, the greater the number of permissions an app requests, the greater its impact on the privacy of its users [10, 6].

2.2 Metadata for privacy analysis in mobile apps

There are a few mobile application repositories [9]. One of the most voluminous and most commonly used by the research community is AndroZoo [1, 16]. Since December 2023, metadata extraction from Google Play has been added, making it also available to those who use this warehouse. Priority has been given to the availability and durability of the APK (*Android Application Package*) and the information available in the official markets.

If we focus on privacy, the repositories where we can find data about the impact of mobile applications are limited. The larger sets of data can be found in Exodus Privacy[8] and Privacy Grade[9][12], though the latter is no longer active, so it is not possible to find updated data. Exodus Privacy provides a warehouse, including the list of permissions requested by apps and information related to trackers [15]. This information is useful for building metrics for end users and developers. However, as with AndroZoo, our experience in educational actifvities concerning mobile privacy with end users shows that these users need easy to understand indicators that they are able to match to something they can act upon, such as the Setting of their devices. Users do not manage permissions on their mobiles, therefore they are not able to translate this information into actions they can take to control their privacy. What they manage are permission groups. For example, Whatsapp requests 81 permissions; users do not have access to 81 permissions on their mobile settings.

2.3 Studying privacy risks in health apps

With the rise of health apps, concerns about privacy and data protection have also grown [23, 13]. There have been studies about their impact on user privacy, most focused on the analysis of privacy policies from a legal perspective [24]. There are also technical studies in which data transfer, permissions, and other technical issues are examined [4]. The main types of data collected include contact information, user location, and several device identifiers (IMEI, MAC, and IMSI), which can be used by third parties to track users across networks and

[8] https://exodus-privacy.eu.org/
[9] https://android-network-tracing.herokuapp.com/privacygrade

applications. However, these studies are prior to the inclusion of the Health-Permission category in Android, which dates from October 2023 and manages health data obtained from body sensors.

3 Assessing a health app privacy in the App-PI ecosystem

In App-PI, a metadata warehouse, a set of analysis tools that calculate indicators and visualization tools that make it easy for people to understand them, collaborate (see Figure 1). Data flow between these components and the App-PIMD warehouse that hosts metadata (related to the privacy and security) of mobile apps. The data flow starts with the collection and integration of data stored in the warehouse. The analysis tools use these data to calculate indicators that provide objective measures of the risk associated with each app. These values are the input for a verification process based on static analysis, which provides confidence. To make it easier for end users to understand these indicators, they are displayed on the visualization platform by tools that represent them with easy-to-understand charts. In this article, we focus on the data flow starting with privacy metadata extraction, their storage, later use in privacy impact analysis, and the final verification that provides confidence concerning the results of the privacy indicators obtained.

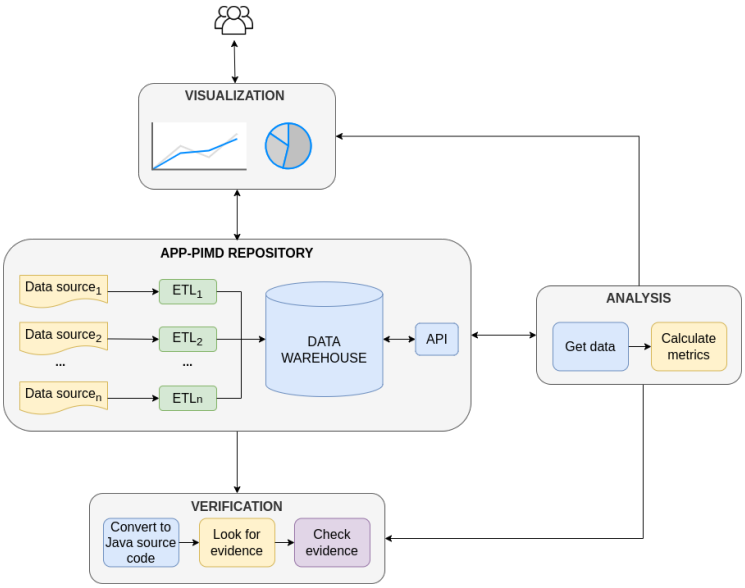

Fig. 1. Main components of App-PI.

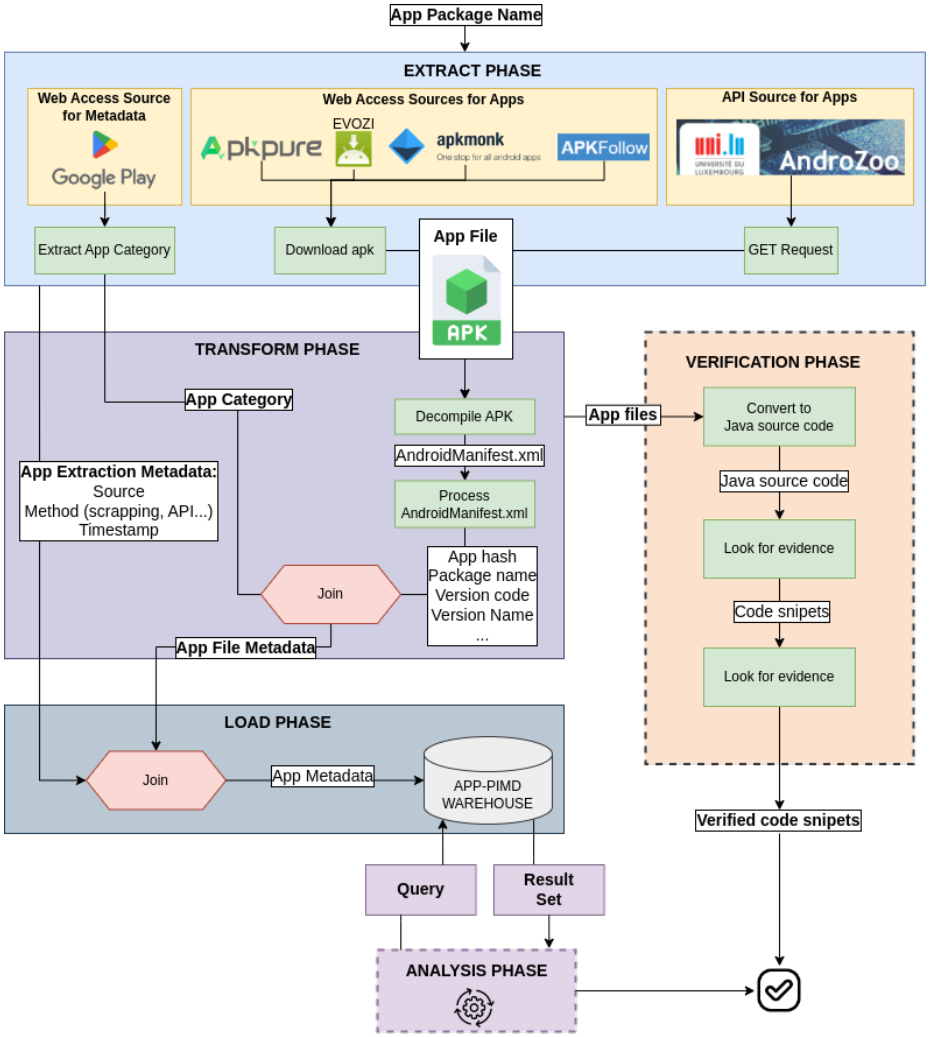

Fig. 2. Data flow in App-PI.

3.1 Assessing an app's privacy: The App-PI data flow

The data flow between the components in Figure 1 appears in Figure 2. The ETL processes that load app metadata into the warehouse provide the first set of data: app metadata. These metadata are used to compute the privacy impact indicators during the analysis phase. Evidence of the access to user data is provided using static analysis, confirming that the data used to obtain the indicators are trustworthy. This is done during the verification phase.

1. *Obtain and load app metadata into the App-PIMD warehouse.*
   (a) *Extract Phase: Obtaining the app file (*apk *file) and other app metadata.* The apps are downloaded from one of the various app sources in the *warehouse*: APKPure, Evozi, APKMonk, APKFollow, and AndroZoo are used for the apk file. Google Play is used to obtain the app category. Its API is used to obtain data from Androzoo. However, the other data sources have to be scrapped. These web scrapping processes have been mostly implemented with pattern searches using regular expressions on the links of each page, in such a way that it is independent of its visual interface. In addition to those extracted app metadata, other metadata about the extraction process for each app (source used, method, and timestamp) are also kept. In this way, each app can be traced.
   (b) *Transform Phase: App decompilation and Processing of the AndroidManifest.xml file.* This step receives the app category and the .apk file as input. It is decompiled to get access to the *AndroidManifest.xml* file and the rest of the app source code. As a result of this stage, we have the source code files that form the app. Metadata is extracted from the AndroidManifest.xml file: hash, package name, version code and name, permissions, etc.
   (c) *Load Phase: Join Metadata.* In this last phase of the ETL, the metadata extracted are put together with data about the extraction process and loaded into the warehouse.
2. *Analysis Phase.* Metadata in the warehouse are used to calculate privacy indicators using tools that analyze them. Metrics providing easy to understand, such as quantitative values, are preferred [2].
3. *Verification Phase.* A static analysis is performed and its results are aligned with privacy indicators. To confirm the metadata in App-PIMD used by indicators, the source code is analyzed. A search is carried out, for instance, for permissions activation calls. If the results of the static analysis confirm the metadata extracted from the AndroidManifest.xml file, it is guaranteed that the indicators are based on data that can be trusted.

3.2 Case study: the Samsung Health app

To show this flow on an example, one of the most popular health apps, has been chosen: Samsung Health. Version 6.27.0.161 of Samsung Health has been analyzed[10].

1. Obtain and load Samsung Health metadata into the App-PIMD warehouse. This app is available on Google Play[11]. From its *AndroidManifest.xml* file, we obtained information such as the list of permissions declared by this app. Table 1 shows the number of permissions, classified by permission

[10] Version 6.27.0.161 is available in the APP-PIMD warehouse.

[11] `https://play.google.com/store/apps/details?id=com.sec.android.app.shealth`

type (*Dangerous, Normal, Signature*). From the total number of 75 permissions this app requests, 50 of them are *Dangerous*, that is, permissions the users can control on their devices. Health permissions are included in the *Dangerous* category. However, users have no possibility of controlling the other 26 permissions. All these data, including the information about each permission, are stored in the App-PIMD warehouse. Figure 3 shows a query that returns this list.

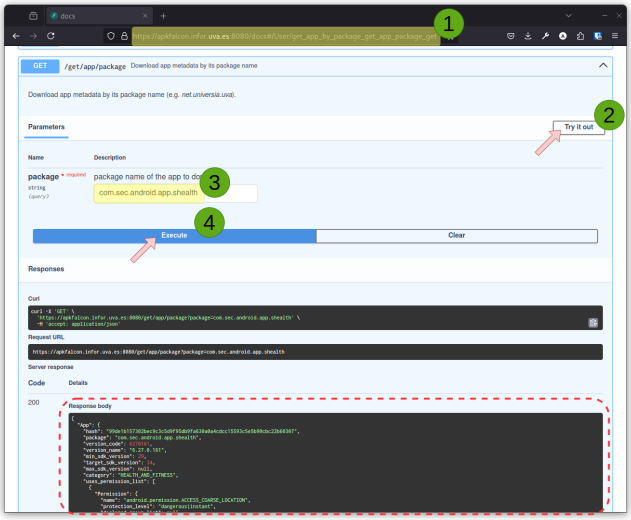

Fig. 3. Using App-PIMD to get the list of permissions of Samsung Health.

2. Obtain Privacy Indicators for Samsung Health. The privacy impact indicator uses the information about *Dangerous* permissions. The value calculated for this app points to a percentage risk of 33.60% (0.336031). The the risk created by an app that asks permission to access every resource of the device on which it is installed would be 100%. This indicates that the app does not seem to be very intrusive. Something which seems surprising, if we consider that many of them are used to get access to health data.

Table 2 summarizes the privacy risk calculated by the privacy impact metric for each permission group. The quantitative and percentage values are shown for each of them. The percentage indicates the rank of each permission group with respect to the final score of the app. The permission groups that contribute most to this value are *Phone* and *Contacts*, with a relative impact of 37.75% and 30.96%, respectively. *Health* permissions follow them with a relative impact of 24.27%. Again, it seems surprising that health permissions are not the most significant ones. The explanation comes from the manner in which our metric operates: the *riskness* of each permission is assigned considering how it has been

exploited by malware, so that permissions not exploited by malware are considered less risky than those already exploited. To our knowledge, there is no malware ranking in which health permissions have been included.

Table 1. Number of permissions by protection level

Permission Type	**Number**
Dangerous permissions	50
Normal permissions	21
Signature permissions	4
Total	75

Table 2. Privacy impact of each permission group in the *Samsung Health* app

Permission group	**Impact**	**Impact (%)**
PHONE	0.496785	37.75%
CONTACTS	0.407408	30.96%
HEALTH	0.319328	24.27%
STORAGE	0.016807	1.28%
LOCATION	0.016807	1.28%
NEARBY_DEVICES	0.016807	1.28%
READ_MEDIA_VISUAL	0.008403	0.64%
MICROPHONE	0.008403	0.64%
ACTIVITY_RECOGNITION	0.008403	0.64%
CAMERA	0.008403	0.64%
NOTIFICATIONS	0.008403	0.64%

3. Static analysis and alignment with results of privacy indicators. Table 3 provides a detailed breakdown of some permissions declared in the app which were found with a static analysis. Some are *Health* permissions included in Android from API level 34, which is something expected in a health app. They can be easily recognized because their name starts with *android.permission.health*:*READ_HEART_RATE*, etc. Figure 4 shows the evidence of the use of one of them, *android.permission.health*:*READ_BLOOD_GLUCOSE*.

Table 3. Selection of permissions declared in *Samsung Health*.

Permission	**Description**
READ_HEART_RATE	Read the user's heart rate data.
READ_BLOOD_GLUCOSE	Read the user's blood glucose data.

4 Conclusions

The App-PI privacy impact ecosystem is designed to deal with information about Android apps that can be used to evaluate their potential impact on user pri-

```
package p000;

import java.util.Map;
import kotlin.Pair;

/* renamed from: ic7 */
/* loaded from: classes.dex */
public abstract class ic7 {

    /* renamed from: a */
    public static final Map f44768a = q60.m11192N2(new Pair(moe.m14498a(C3055gf.class), caj.m3390
    new Pair(moe.m14498a(ov0.class), caj.m33909I1("android.permission.health.READ_BLOOD_GLUCOSE"),
    new Pair(moe.m14498a(ow0.class), caj.m33909I1("android.permission.health.READ_BLOOD_PRESSURE"),
    new Pair(moe.m14498a(fy0.class), caj.m33909I1("android.permission.health.READ_BODY_TEMPERATURE
}
```

Fig. 4. Evidence of the use of READ_BLOOD_GLUCOSE permission.

vacy. Data flows from the data sources where the information is extracted to calculators that use them to obtain privacy impact indicators, and processes that verify the accuracy of these indicators. When applied to health apps, we have found that the potential risk of these apps does not seem to be as high as we could expect. There are two possible explanations for this surprising finding. First, these health permissions, which were introduced in Android in October 2023, are used under a model which is less vulnerable to malware. The second is related to the recent introduction of these permissions: there are as yet no malware rankings that include health permissions as being among those exploited by malware. Time will tell which explanation is more realistic.

5 Future Work

The evolution of the Android permission model requires constant revisions of the information stored in the warehouse. In the first phase of the ETL flow, the *Extract* is constantly revised so as to update the data sources, and reflect changes in the Android permission model. In a similar manner, malware rankings are revised to update the information used with the most recent knowledge about privacy threats. In the case of health apps, this is particularly interesting, because there are as yet no malware rankings that include these permissions. In case they are found, new ETLs will be prepared to include this information in the App-PIMD warehouse. In addition, summaries in natural language will be integrated to improve user readability and comprehension.

Acknowledgements This work is included in the activities of the strategic Cybersecurity project "App-PI (*App Privacy Impact*): An ecosystem for the evaluation of the impact of apps for mobile devices on the privacy and security of their users", which is carried out under a collaboration agreement between the University of Valladolid and the Spanish National Institute of Cybersecurity (INCIBE) for the promotion of strategic Cybersecurity projects in Spain, within the framework of the funds of the Recovery, Transformation and Resilience Plan, financed by the European Union (*Next Generation*).

References

1. Allix, K., Bissyandé, T.F., Klein, J., Le Traon, Y.: AndroZoo: Collecting Millions of Android Apps for the Research Community. In: Proceedings of the 13th International Conference on Mining Software Repositories. pp. 468–471 (2016)
2. Aparicio, A., Martínez-González, M.M., Cardeñoso, V.: Métrica basada en grupos de permisos para entender el impacto de las aplicaciones Android sobre la privacidad. In: 2022 17th Iberian Conference on Information Systems and Technologies (CISTI). pp. 1–5 (2022). https://doi.org/10.23919/CISTI54924.2022.9820147
3. Arbanas, J., Silverglate, P.H., Hupfer, S., Loucks, J., Raman, P., Steinhart, M.: Data privacy and security worries are on the rise, while trust is down. deloitte's connected consumer survey 2023. Tech. rep., Deloitte Center for Technology, Media & Telecommunications (2023), https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html
4. Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., Carrasco, A.: Privacy assessment in mobile health apps: Scoping review. JMIR Mhealth Unhealth **8**(7) (2020). https://doi.org/10.2196/18868
5. Chang, K.C., Zaeem, R.N., Barber, K.S.: A framework for estimating privacy risk scores of mobile apps. In: Susilo, W., Deng, R.H., Guo, F., Li, Y., Intan, R. (eds.) Information Security - 23rd International Conference, ISC 2020, Bali, Indonesia, December 16-18, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12472, pp. 217–233. Springer (2020). https://doi.org/10.1007/978-3-030-62974-8_13, https://doi.org/10.1007/978-3-030-62974-8_13
6. Degirmenci, K.: Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management **50**, 261 – 272 (2020). https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.05.010, http://www.sciencedirect.com/science/article/pii/S0268401218307965
7. Developers, A.: Android Developers. Security guidelines. https://developer.android.com/training/articles/security-tips?hl=es-419#UserData
8. Gashi, E., Tafa, Z.: Permission-based privacy analysis for android applications. International Journal of Business and Technology **6**(3) (2018). https://doi.org/0.33107/ijbte.2018.6.3.02, https://knowledgecenter.ubt-uni.net/ijbte/vol6/iss3/2
9. Geiger, F.X., Malavolta, I.: Datasets of Android Applications: a Literature Review. ArXiv **abs/1809.10069** (2018), https://api.semanticscholar.org/CorpusID:52845379
10. Hudson, S., Liu, Y.: Mobile app users' privacy concerns: different heuristics for privacy assurance statements in the EU and china. Inf. Technol. People **36**(1), 245–262 (2023). https://doi.org/10.1108/ITP-06-2021-0478, https://doi.org/10.1108/ITP-06-2021-0478
11. Hylender, C.D., Langlois, P., Pinto, A., Widup, S.: Data Breach Investigations Report. Tech. rep., Verizon (2024)
12. Jin, H., Liu, M., Dodhia, K., Li, Y., Srivastava, G., Fredrikson, M., Agarwal, Y., Hong, J.I.: Why are they collecting my data?: Inferring the purposes of network traffic in mobile apps. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **2**(4), 173:1–173:27 (2018). https://doi.org/10.1145/3287051, https://doi.org/10.1145/3287051
13. Kitkowska, A., Karegar, F., Wästlund, E.: Share or protect: Understanding the interplay of trust, privacy concerns, and data sharing purposes in health and wellbeing apps. In: Gena, C., Russis, L.D., Spano, L.D., Lanzilotti, R., Mascio, T.D.,

Prandi, C., Andolina, S. (eds.) Proceedings of the 15th Biannual Conference of the Italian SIGCHI Chapter, CHItaly 2023, Torino, Italy, September 20-22, 2023. pp. 15:1–15:14. ACM (2023). https://doi.org/10.1145/3605390.3605417, https://doi.org/10.1145/3605390.3605417

14. Kuan-Lin, C., Chung-Huang, Y.: Design and implementation of privacy impact assessment for android mobile devices. ZTE Communications **14**(S0), 37 (2016). https://doi.org/http://zte.magtechjournal.com/EN/10.3969/j.issn.1673-5188.2016.S0.003
15. Laperdrix, P., Mehanna, N., Durey, A., Rudametkin, W.: The price to play: A privacy analysis of free and paid games in the android ecosystem. In: Laforest, F., Troncy, R., Simperl, E., Agarwal, D., Gionis, A., Herman, I., Médini, L. (eds.) WWW '22: The ACM Web Conference 2022, Virtual Event, Lyon, France, April 25 - 29, 2022. pp. 3440–3449. ACM (2022). https://doi.org/10.1145/3485447.3512279, https://doi.org/10.1145/3485447.3512279
16. Li, L., Gao, J., Hurier, M., Kong, P., Bissyandé, T.F., Bartel, A., Klein, J., Le Traon, Y.: AndroZoo++: Collecting Millions of Android Apps and Their Metadata for the Research Community. arXiv e-prints arXiv:1709.05281 (Sep 2017)
17. Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Zhang, S., Sadeh, N.M., Agarwal, Y., Acquisti, A.: Follow my recommendations: A personalized privacy assistant for mobile app permissions. In: Twelfth Symposium on Usable Privacy and Security, SOUPS 2016, Denver, CO, USA, June 22-24, 2016. pp. 27–41. USENIX Association (2016), https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu
18. Mayrhofer, R., Stoep, J.V., Brubaker, C., Kralevich, N.: The android platform security model. ACM Trans. Priv. Secur. **24**(3) (apr 2021). https://doi.org/10.1145/3448609, https://doi.org/10.1145/3448609
19. Momen, N., Hatamian, M., Fritsch, L.: Did app privacy improve after the gdpr? IEEE Secur. Priv. **17**(6), 10–20 (2019). https://doi.org/10.1109/MSEC.2019.2938445, https://doi.org/10.1109/MSEC.2019.2938445
20. de Montjoye, Y.A., Gambs, S., Blondel, V.D., Canright, G.S.J., de Cordes, N., Deletaille, S., Engø-Monsen, K., García-Herranz, M., Kendall, J., Kerry, C.F., Krings, G., Letouzé, E., Luengo-Oroz, M.A., Oliver, N., Rocher, L., Rutherford, A., Smoreda, Z., Steele, J.E., Wetter, E., Pentland, A.S., Bengtsson, L.: On the privacy-conscientious use of mobile phone data. Scientific Data **5** (2018), https://api.semanticscholar.org/CorpusID:54472286
21. Orjiude, K.E., Yinka-Banjo, C.O.: A multilateral privacy impact analysis method for android applications. Annals of Science and Technology **7**(2), 1–20 (2022). https://doi.org/doi:10.2478/ast-2022-0005, https://doi.org/10.2478/ast-2022-0005
22. Shrivastava, G., Kumar, P., Gupta, D., Rodrigues, J.J.P.C.: Privacy issues of android application permissions: A literature review. Trans. Emerg. Telecommun. Technol. **31**(12) (2020). https://doi.org/10.1002/ett.3773, https://doi.org/10.1002/ett.3773
23. Stach, C.: Big brother is smart watching you - privacy concerns about health and fitness applications. In: Mori, P., Furnell, S., Camp, O. (eds.) Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira - Portugal, January 22-24, 2018. pp. 13–23. SciTePress (2018). https://doi.org/10.5220/0006537000130023, https://doi.org/10.5220/0006537000130023

24. Tangari, G., Ikram, M., Ijaz, K., Kaafar, M.A., Berkovsky, S.: Mobile health and privacy: cross sectional study. BMJ (jun 2021). https://doi.org/10.1136/bmj.n1248
25. Veltman, A.: Samsung health: How self-tracking trivialises our ethical concerns. diggit magazine (2023), https://www.diggitmagazine.com/articles/samsung-health-ethical-concerns