

Krämer, Julia

Article

The death of privacy policies: How app stores shape GDPR compliance of apps

Internet Policy Review

Provided in Cooperation with:

Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Krämer, Julia (2024) : The death of privacy policies: How app stores shape GDPR compliance of apps, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 2, pp. 1-38,
<https://doi.org/10.14763/2024.2.1757>

This Version is available at:

<https://hdl.handle.net/10419/296497>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/3.0/de/legalcode>



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

The death of privacy policies: How app stores shape GDPR compliance of apps

Julia Krämer *Erasmus University Rotterdam*

DOI: <https://doi.org/10.14763/2024.2.1757>

Published: 2 April 2024

Received: 16 June 2023 Accepted: 1 December 2023

Funding: The author's PhD position is supported by the research initiative on Rebalancing Public & Private Interests and the Erasmus Center of Empirical Legal Studies of Erasmus School of Law, which is part of the sector plan of the Dutch Ministry of Education, Culture and Research.

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Krämer, J. (2024). The death of privacy policies: How app stores shape GDPR compliance of apps. *Internet Policy Review*, 13(2). <https://doi.org/10.14763/2024.2.1757>

Keywords: GDPR, App Store, Privacy labels, Transparency, Mobile apps

Abstract: The General Data Protection Regulation (GDPR) obliges data controllers to inform users about data processing practices. Long criticised for inefficiency, privacy policies face a substantive shift with the recent introduction of privacy labels by the Apple App Store and the Google Play Store. This paper illustrates how privacy disclosures of apps are governed by both the GDPR and the contractual obligations of app stores and is complemented by empirical insights into the privacy disclosures of 845,375 apps from the Apple App Store and 1,657,353 apps from the Google Play Store. While the GDPR allows for the use of privacy labels as a complementary tool next to privacy policies, the design of the privacy labels does not satisfy the standards set in Art. 5(1)(a) GDPR and Art. 12-14 GDPR. The app stores may consequently distort the compliance of apps with data protection laws. The empirical data highlight further problems with the privacy labels. The design of the labels favours disclosures of developers that offer a variety of apps that can process data across different services and contradictory disclosures do not get flagged nor verified by app stores. The paper contributes to the overall discussion of how app stores in their role as intermediaries govern privacy standards and the impact of private sector-led initiatives.

Introduction

The regulation of the processing of personal data has become increasingly important in the context of mobile software applications (henceforth: apps), which collect vast amounts of personal data from their users (Binns et al., 2018; Zimmeck et al., 2016). Mobile apps from around the world are distributed in a handful of app stores that serve as a marketplace, with Apple and Google being the primary provider of these platforms in the European Union (EU). Developers are responsible for ensuring compliance with data protection laws. In the EU, the General Data Protection Regulation (Regulation 2016/67, henceforth: GDPR) is applicable if apps process personal data of their users. Next to these requirements, to be allowed to publish their software in the app stores, developers have to comply with various contractual obligations of the Google Play Store or the Apple App Store.

A new feature in both app stores that influences compliance with transparency requirements are so-called privacy labels. These labels refer to a set of standardised icons that illustrate different types of collected data and data processing practices of apps. In general, privacy labels are a response to inefficient transparency rules in data protection law and aim to inform users in a clearer and faster manner than privacy policies can. Even though the GDPR has provisions concerning the use of standardised icons, the app stores acted in their own capacity and interest when introducing the privacy labels with a self-designed set of definitions and corresponding icons. Apple has required developers to disclose privacy labels since December 2020 and in April 2022 Google followed suit with a native set of labels. The launch marks the first time that privacy labels have become widely available to users.

The introduction of privacy labels by the app stores has received mixed feedback. Several media commentators have reacted positively to the app stores' decision by describing the labels as "a big win for consumer privacy" (Perez, 2020) and giving users "easy, glance-able breakdowns of the data that developers can collect and track" (Gartenberg, 2020). At the same time, the design of the privacy labels has been subject to sharp criticism by regulators, for instance by the UK Competition and Markets Authority (CMA), and academics for not capturing the source of privacy problems and exempting tracking practices (CMA, 2022, p. 231; Kollnig et al., 2022, p. 9). Additionally, regarding the understanding of the labels, a recent study demonstrated that users encountered problems comprehending entangled and overlapping definitions of different data categories inherent in the privacy labels of the Apple App Store (Zhang et al., 2022, p. 214). While these studies point to potential problems of the privacy labels, it has yet to be explored how the labels

align with existing provisions in EU data protection law that regulate transparency disclosures.

Transparency obligations in data protection laws have a long history of criticism for being ineffective (Solove, 2013; Waldman, 2021, p. 61 ff.). The new adoptions by app stores have the potential to unravel what years of regulatory efforts could not. Yet it remains to be investigated whether the privacy labels will fully realise this potential. To draw these conclusions, empirical evidence is necessary. Next to a legal analysis that explores whether the privacy labels meet the requirements in EU data protection law, this paper delivers insights into the adoption of app developers in both the Apple App Store and Google Play Store to map the scope of the problem. Ultimately, the goal of this paper is to answer the question of the extent to which app store policies impact app compliance with the transparency provisions of the GDPR. Against this background, this paper addresses the following questions:

- Do the privacy labels designed by the Apple App Store and Google Play Store comply with the GDPR?
- To what extent do mobile apps in the app stores comply with the transparency requirements of the GDPR?

This paper contributes to the overall discussion of how app stores in their role as intermediaries govern privacy standards. By looking into effects of this private-sector led initiative, the paper follows claims put forward by van Dijck et al. (2019, p. 12) that differentiated analyses of integrated platform ecosystems, especially app stores, are needed to show how power is embedded in platform infrastructures. This paper is, to my best knowledge, the first to provide a comprehensive legal analysis of the extent to which the current transparency requirements that the Google Play Store and Apple App Store force on developers comply with transparency provisions in the GDPR. Additionally, most empirical investigations have focused on the app landscape of the US and UK app store (see for instance Kollnig, 2022; Story, 2018; Zimmeck, 2016). This paper will contribute with insights into the EU app store landscape, on a total sample of 2,502,728 apps (German geolocation).¹ The following empirical contributions are made: Firstly, this paper maps the extent apps in both app stores provide privacy policy links and privacy labels to their users. Secondly, the dataset illustrates how the design of privacy labels tends to favour developers who offer a variety of apps that can process data across dif-

1. For robustness checks, also app data with a Dutch geolocation has been scraped (N=2,491,128). Since the data did not show significant differences to the German scrape, the results will only be displayed in the appendix.

ferent services. Thirdly, the results show the number of contradictory disclosures by apps, which highlights a problematic self-assessment by developers if they are not verified by the app stores, as is the current scenario.

Privacy disclosures in the mobile ecosystem

Key stakeholders in the mobile ecosystem

In the EU mobile ecosystem, several actors have abilities to influence data protection compliance of apps. Initially, developers play a crucial role as they build and design an app, and their choices have direct consequences for the privacy protection offered to users (ENISA, 2017, p. 16). Closely connected is the role of the app provider, the entity owning and providing an app to the end user. In instances where the app provider does not have the necessary expertise, they may choose to outsource app development to a developer team (Autoriteit Consument & Markt, 2019, p. 23). It is noteworthy that app providers and developers are in most cases the same entity. Therefore, for the remainder of the paper, the term “developer” is used to describe both the app provider and the app developer. Developers design apps either for Android or iOS operating systems, which are the dominant mobile operating systems in Europe (Statista, 2023a). The choice of the operating system will also have an impact on the app store in which the app will be distributed: while the Apple App Store is, as it currently stands, the only app store available for iOS devices, the prevalent app store for Android devices is the Google Play Store. Technically, Android users have the feasibility to download apps from alternative stores, such as F-Droid, but the Google Play Store remains the most popular app store in Europe (Statista, 2023c). App stores facilitate transactions between users and developers while upholding quality and security of offered apps, a role Fong (2017) coined as “app intermediaries” (p. 96). Article 29 Working Party (2013) recognises this role and holds app stores to have “an important responsibility” to ensure appropriate information and to incentivise developers to provide adequate information about their data processing practices. While developers benefit from the distribution of their app to a large and global user base, app stores reap substantial revenue from their intermediary function. In 2022, the Google Play Store generated 42.3 billion \$ and the Apple App Store 86.8 billion \$ in app and game revenue (Iqbal, 2024).

When a user interacts with an app, personal data in the sense of Article 4(1) GDPR is generated. The data are either stored locally on the device or transferred off the device, for instance to a server owned by the developer. This happens, for instance, through the implementation of trackers within apps, which are pieces of software

that systematically gather data for various purposes, such as crash reporting or user profiling (Exodus Privacy, n.d.b). A substantial privacy risk is associated with third-party mobile tracking as it can trace connections from multiple apps to a single user that allows the creation of a detailed user profile (Binns et al., 2018). A data transfer to a third-party involves an entity separate from the app developer, whereas a first-party transfer refers to data shared within the same developer's ecosystem. Third-party tracking is often used for advertising purposes. This is due to the fact that next to one-time app fees or in-app purchases, monetising data for ad purposes is a main revenue source for developers (ENISA, 2017, p. 33). Monetising and processing personal data for ad purposes is problematic if it happens without the user's awareness and consent.

Finally, in the EU, national data protection authorities are equipped with enforcing data protection rules and provide guidance to firms that ensure a certain level of privacy protection within apps offered to users. In the following section, the entity that bears legal responsibility under the GDPR will be described.

Legal responsibility under the GDPR

Data controllers and processors as defined in Art. 4 (7) and (8) GDPR are the addressees of most legal obligations in EU data protection law. A controller determines the “purposes and means” of the data processing and the processor processes data on the controller's behalf (GDPR, Art. 4 (7), (8)). Next to these concepts, two or more parties can be held jointly responsible for compliance with GDPR provisions if they jointly determine the purposes and means of processing (GDPR, Art. 26). Developers are usually considered the data controller for the processing of user data, to the extent that they process user data for their own purposes (ENISA, 2017, p. 16). As a result, the legal responsibility for integrating data protection principles into apps remains with developers (Fong, 2017, p. 113). Next to assigning legal responsibility to controllers, the GDPR encourages the producers of products and services that are based on the processing of personal data to consider the right to data protection in order to enable controllers to meet their obligations under the GDPR (GDPR, Recital 78). Within the mobile ecosystem, this recital is particularly relevant for app stores considering their intermediary function (ENISA, 2017, p. 16). However, the sharing of this responsibility is not reflected in the current legal landscape, which primarily assigns GDPR-related responsibilities solely to developers. App stores, for instance, process personal data, such as information of the number of apps a user has downloaded and metadata on their usage. It has, however, not yet been recognised that app stores can influence the personal data processing in a third-party app. Judgments by the European Court of Justice (CJEU)

that adopt a broad interpretation of controllership, such as *Wirtschaftsakademie Schleswig-Holstein* (Case C-210/16) and *FashionID* (Case C-40/17) suggest that this could change in the future. Both cases concerned the concept of joint controllership, which is enshrined in Art. 26 GDPR. In *Wirtschaftsakademie Schleswig-Holstein*, the CJEU established that it is not necessary for a party to have access to personal data to be held jointly responsible for the obligations under the GDPR (Case C-210/16, para 38). In *FashionID*, the CJEU stressed that processing of personal data involves various operations, and that liability should be limited to a set of operations in which an entity “actually determines the purposes and means of the processing” (C-40/17, para 85). In essence, the allocation of processing responsibilities is not a binary “all or nothing” scenario but rather a nuanced determination based on the degree of engagement by each entity in question (Janssen et al., 2020, p. 366). As a result, if platforms actively participate in specific stages of individual data processing, they may share joint responsibility with their business users for certain processing practices (van Hoboken & Fathaigh, 2021, p. 6). It is noteworthy that this shared responsibility has not yet been officially acknowledged for app stores, for instance through a decision by a data protection authority or in a court judgement.

App store policies and data protection standards

App stores are not merely passive marketplaces that facilitate the distribution of apps to potential users. As has been pointed out by Poell et al. (2019, p. 7), both the Google Play Store and the Apple App Store are “highly centralised, heavily controlled and curated”, which allows them to set standards and definitions. This structure influences the power distribution between the actors in the mobile ecosystem. Van Hoboken and Fathaigh (2021) have been the first to categorise different forms of privacy governance functions of app stores. They refer to app stores as “de-facto privacy regulators” and differentiate the regulatory functions of app stores between technical standards, contractual standards, and policing behaviour through enforcement. A good example of the policing of behaviour through enforcement is described by Greene and Shilton (2017), who illustrate how different design decisions and rules influence the way in which developers adapt privacy-preserving technology in their apps. Since the Apple App Store has access requirements that include privacy standards, developers have internalised Apple’s definition of privacy which ultimately affects the level of privacy offered to users. The authors coin this behaviour “privacy by platform” and “privacy by permitted design”.

Contractual standards are another way of governing privacy. The terms and conditions of app stores usually include provisions concerning a limitation of liability in

favour of the app store, the design of an app, and information on pricing structure. To publish an app in the Apple App Store, developers must adhere to the Apple Developer Program License Agreement (Apple, n.d.b) and comply with the guidelines outlined in the Apple App Store Review Guidelines (Apple, 2024). By entering the Developer Program License Agreement, developers are granted a limited licence to distribute apps in the app store. The Apple App Store Review Guidelines introduce several other guidelines that have to be complied with, such as the guidelines on app privacy details that prescribe the use of privacy labels.

To access the Google Play Store, developers have to agree to the Google Play Developer Distribution Agreement and comply with the Google Developer Program Policies (Google 2024), a collection of various policies that govern technical standards and app content. The developer policy on “Privacy, Deception and Device Abuse” requires all apps to provide a link to a privacy policy and to insert privacy labels, with the developer being responsible for accurate information and keeping the privacy labels up to date. Furthermore, Google (n.d.d, Section “Privacy Policy”) requires developers to “comprehensively disclose how your app accesses, collects, uses and shares user data, not limited by the data disclosed in the privacy label”. Next to these platform-specific rules, both app stores require developers to comply with (data protection) laws in all jurisdictions an app is distributed in. Due to the lack of alternatives and little opportunity to negotiate over contract provisions it is difficult for developers to change these “rules of the game” set by app stores (CMA, 2022). Therefore, app stores have the power to impose the responsibility for privacy compliance on the developer, who is usually the weaker party vis-à-vis the app store.

The contractual provisions are enforced by the app stores via the removal of an app’s listing, the refusal of new updates, or the rejection of an app to the app store in the first place. In its enforcement policy, Google (n.d.a) also describes the option of the termination of developer accounts and the restriction of visibility or regions the app is displayed in. Consequently, app stores have various tools at their disposal to ensure that developers comply with their rules. While these rules aim to ensure safety and quality of the app ecosystem, they have also been referred to by developers as “kafkaesque” and “arbitrary” (CMA, 2022, p. 194). This wide discretion the app stores grant themselves can be problematic since their gatekeeping function as intermediaries plays an essential role in ensuring that privacy standards are met and access requirements of an app store may determine the level of data protection offered to its users (Fong, 2017). Yet the current EU data protection law framework leaves a lot of discretion to the privacy regulator role of app stores

because it does not have a platform specific provision, as opposed to other areas like competition law (van Hoboken & Fathaigh, 2021, p. 8). As an illustration, the German Competition Act (GWB) addresses firms operating in “multi-sided markets and networks” (GWB, 18(3a)), thereby encompassing intermediaries that connect various user groups, a classification which also captures app stores (Franck and Peitz, 2021, p. 515).

Transparency provisions, the GDPR, and privacy labels

To empower data subjects to make informed choices about who may process their personal data and under what conditions, controllers must adhere to the principle of transparency (GDPR, Art. 5(1)(a)). The principle of transparency requires all information, addressed to the public or to the data subject, to be provided in a “*concise, transparent, intelligible and easily accessible form, using clear and plain language*” and “*in writing, or by other means, including, where appropriate, by electronic means*” (GDPR, Art. 12(1)). Where appropriate, this information may also be provided in combination with standardised icons (GDPR, Art. 12(7)). In this way, data subjects should be informed about the risks, rules and safeguards and rights they are able to exercise in surrounding the processing of their data (GDPR, Recital 39). This becomes especially important in the context of user consent, which is one of the six legal bases for lawful processing. Valid consent is defined as “*any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*” (GDPR, Art. 4 (11)). Consent is the only possible legal basis when special categories of personal data are processed, which refers to the processing of personal data revealing “*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation*” (GDPR, Art. 9 (1)). This form of data processing is especially relevant to dating apps, prayer apps, and (mental) health apps, facilitated in part by the integration of smartwatches, which have the capability to reveal this kind of sensitive user data. To apply this in the context of the mobile ecosystem: if an app processes personal data a user must be informed about, among other elements, the identity of the developer, the purposes of the processing of the personal data, the legal basis the processing is based on, the different rights the data subject enjoys, and the storage period of the data (GDPR, Art. 13).

In addition to the transparency requirements in text form, Recital 60 GDPR highlights the conditions for the use of visualisations “*information may be provided in*

combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing". The responsibility for the development of standardised icons lies with the European Commission and the European Data Protection Board (Art. 29 WP, 2018, p. 26). Recital 166 GDPR further clarifies that delegated acts should be adopted to clarify the information to be presented by icons and procedures for such a provision. According to Polčák (2020), however, the European Commission has unofficially indicated that it is unlikely to adopt a delegated act on standardised symbols in the near future.

The idea of standardised icons to inform about data processing activities was first described in 2009, as a reaction to the lack of privacy policies to inform users properly about their privacy choices and was inspired by consumer law provisions concerning food packaging (Kelley et al., 2009). A study in the 2000s, before the use of apps became part of our daily life, calculated that the average time per year to read privacy policies amounts to more than 200 hours (McDonald & Cranor, 2008). Additionally, most people do not read lengthy legal documents (Bakos et al., 2014). Considering this empirical evidence, privacy labels can encourage users to quickly inform themselves about how their data is processed and simplify the comparison of data processing practices between different apps or services. Already in 2013, Article 29 Working Party suggested the use of icons for data processing information to app stores, emphasising their responsibility of ensuring "adequate" information (Art. 29 WP, 2013, p.12). In 2018, the International Consumer Protection and Enforcement Network (ICPEN) launched a call directed towards the Apple App Store and Google Play Store to improve the information provision about data processing practices on an app's installation page. The call was led by the Dutch competition authority (Autoriteit Consument & Markt) and involved 27 consumer authorities from all over the world (Autoriteit Consument & Markt, 2019).

In response to these calls, or driven by their own initiatives and interest, the Apple App Store introduced privacy labels in December 2020, followed by the Google Play Store in April 2022. While the app stores have developed their own design of privacy labels, various alternative designs for these labels have been proposed in the past. The labels of Ayres and Schwartz (2014), for instance, emphasise the most important terms in order to tackle the problem of information overload or of hiding unfavourable terms in a large chunk of text. Other proposals of privacy labels focus on compliance with GDPR provisions that show retention periods of data or third-country data transfers (Fox et al., 2018). The extent to which the designs of app stores comply with GDPR provisions will be analysed in the next sec-

tion.

Compliance of privacy labels with the GDPR

Both the Apple App Store and the Google Play Store mandate that developers have to inform about the data processing of their apps via privacy labels (Apple, n.d.a; Google, n.d.b). They have developed a set of standardised icons for different types of data, which help the user to identify what happens with the data, and a set of different categories of data, which help the user to understand which data is processed. They are accompanied by a description of the purpose of the data collection. Figure 1 and Figure 2 depict the privacy labels as shown in the app stores.

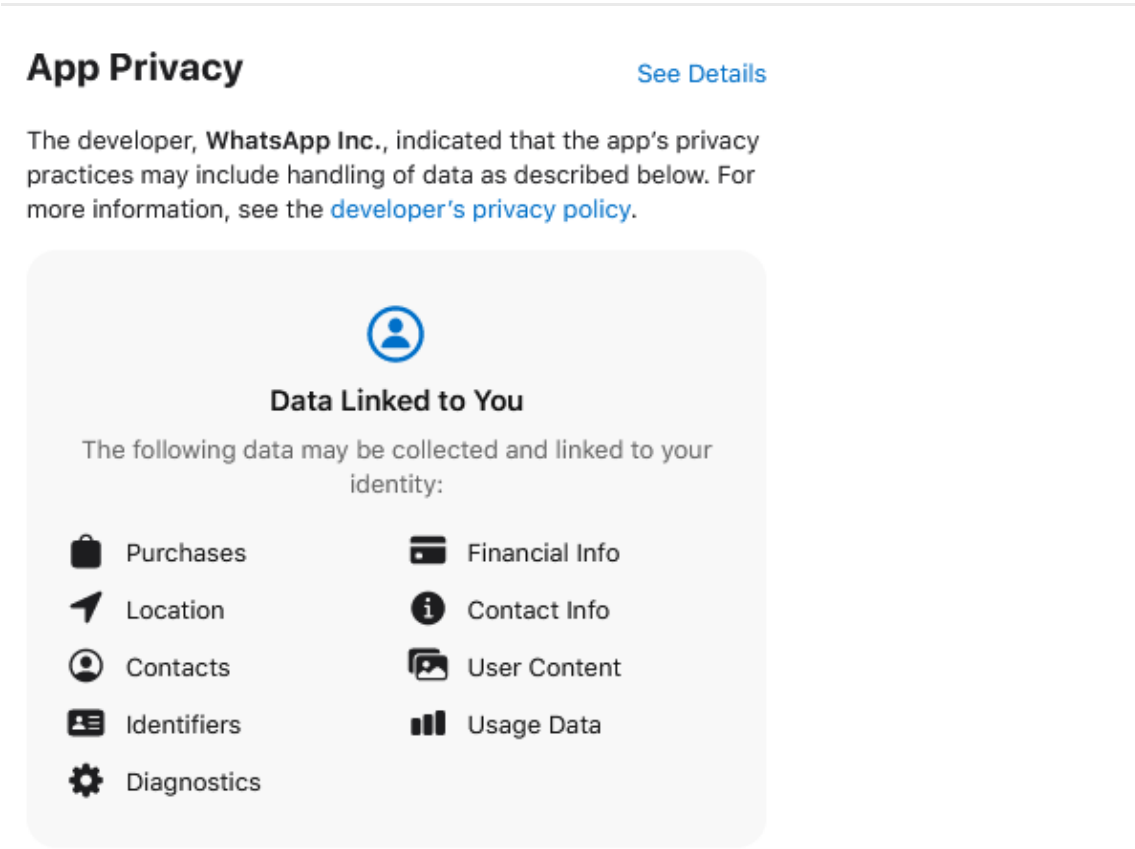


Figure 1: Example of privacy labels in the Apple App Store.



Data collected

Data this app may collect



Location

Approximate location



Personal info

Email address, User IDs, and Phone number



Financial info

User payment info and Purchase history



Contacts

Contacts

Figure 2: Example of privacy labels in the Google Play Store.

The labels introduced by Apple and Google follow different design choices. Apple categorises collected data in three types (“Data not Linked”, “Data Linked” and “Data Used to Track You”), 14 categories (for example location or contacts) and six purposes for which the data has been processed (for example third-party advertising or analytics). The data type “Data not linked” refers to data that cannot be linked back to the user’s identity, “Data Linked” means that the data can identify a user and “Data Used to Track” stands for data that is linked with third-party data or is shared with a data broker (Apple, n.d.a). The Google Play Store differentiates between two different types of data, “Data Collected”, when data is transmitted off a user’s device and “Data Shared”, that points to data transferred to a third-party. Google distinguishes between 14 different categories, but they are different compared to Apple’s. For instance, Google does not have a sensitive data category.

Transparency compliance through mobile apps has been explored in the past. A study of 61 prominent mental-health apps in both the Google Play Store and Apple App store identified severe shortcomings in relation to transparency require-

ments, with almost half of the apps not providing a privacy policy to their users. The authors suggest that app stores should incorporate stricter standards for privacy policies to assist users to understand privacy disclosures (Parker et al., 2019). The introduction of privacy labels, that can be seen as such a stricter standard, has likewise received scholarly attention. An empirical study by Xiao et al. (2022) examined 5,102 apps in the Apple App Store and determined that more than half of the privacy label disclosures of apps do not comply with actual data flows. An investigation into 1,687 apps from the German Apple App Store showed similar results (Koch et al., 2022). A large-scale analysis of the privacy labels of 1.4 million apps in the Apple App Store identified various challenges with privacy labels, such as a lack of incentives for inactive apps to provide information and for developers to update the labels continuously (Li et al., 2022). These findings draw attention to the fact that app stores do not check the veracity and completeness of privacy disclosures. Furthermore, the definitions the privacy labels are based upon have been subject to criticism. According to Kollnig et al. (2022), Apple's definitions do not capture the source of privacy problems, such as a distinction between first and third-party collection, and exempt Apple's native tracking practices. The CMA came to a similar conclusion: even though Apple is not referring to its own processing activities as "tracking", its activities are no less consistent with its own definition of "tracking" than that of third-parties (CMA, 2022).

Additionally, the labels have been analysed from a qualitative perspective to gain insight into how users perceive the new information provision. Recent studies showed that Apple's categorisation of data, such as the difference between "Data used to track you" and "Data linked to you" and certain data subcategories confused users (Zhang et al., 2022) and developers (Gardner et al., 2022). As a consequence, the findings suggest that the general objective of privacy labels, namely, to inform users effectively about data processing practices, is undermined by the several design decisions by the app stores. While these studies point to potential problems arising out of the implementation of privacy labels, it has to be analysed how they fit with existing provisions of EU data protection law that regulate privacy disclosures.

The data types and data categories chosen by the app stores deviate from the distinctions of data types recognised in the GDPR. According to Art. 4(1) GDPR, any information relating to an identified or identifiable person is considered personal data, no matter how and by whom that data has been collected. Guidance to distinguish data that are not personal, which are often termed 'anonymous data' in data protection discourse (Bygrave and Tosoni, 2020, p. 105), and personal data is

delivered in Recital 26 GDPR. Here, the GDPR specifies that “*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*” (Recital 26). Nevertheless, difficulties concerning the demarcation between both categories remain. The advancement of big data poses a challenge to this legal test, as apparent anonymised data in combination with additional data may be used to re-identify a data subject (Finck and Pallas, 2020, p. 20). These findings raise concerns in light of Apple’s definition of “Data not linked” to the user, emphasising data that, according to Apple (n.d.a), are not linked back to a user’s identity. This becomes especially relevant when an app collects various categories of “Data not linked”.

Tracking is referred to by Apple (n.d.a, Section “Tracking”) as “*linking data collected from your app about a particular end user or device [...] with Third-Party data for targeted advertising or advertising measurement purposes, or sharing data collected from your app about a particular end-user or device with a data broker*”. In contrast to the guidance in Recital 24 GDPR which emphasises the *result* of the concept by describing it as “taking decisions of a data subject to analyse or predict a certain behaviour”, Apple’s definition highlights the *actor* involved by differentiating between first and third-parties. This choice on the side of Apple is problematic since the distinction between third-party data and first-party data does not capture the source of privacy risks and exempts Apple’s own advertising techniques (Kollnig et al., 2022, p. 9). The same can be said about the “Data sharing” and “Data collected” category of Google that differentiates between first and third-parties. While both categories refer to the transfer of data from the user’s device, the difference lies in the transfer to a third-party. Furthermore, previous research pointed out that this categorisation in different data types confused consumers and developers alike (Gardner et al., 2022; Zhang et al., 2022). It is therefore questionable if the design of both labels would meet the general standard of being intelligible (GDPR, Art. 12(1)).

Both Apple and Google introduce exceptions which make the disclosure of data processing via privacy labels optional for developers. In the Apple App Store, several cumulative criteria have to be fulfilled for an optional disclosure. This may involve instances where data collection is infrequent, the data is not used for tracking purposes, and if the data collection is provided in the app’s interface in a way that “it is clear to the user what data is collected” (Apple, n.d.a). Google exempts mandatory disclosures when it is reasonable for the user to expect the data to be shared, the data is anonymised, or the data is transferred to a service provider who

processes it on behalf of the developer (Google, n.d.c). Consequently, both app stores present a variety of exceptions that have the potential to confuse users, since their personal data may still be processed even when not disclosed by the developer. Most of these exceptions are not compatible with the GDPR since not disclosing personal data processing practices would undermine the whole purpose of transparency requirements which is to make users aware of risks, rules, and safeguards of data processing (GDPR, Recital 39).

While the design of the privacy labels allows for optional disclosures, data processing practices of an app could still accurately be described in the privacy policy of an app. An example is a data transfer within an Android app to a third-party where a user could “reasonably expect the data to be shared” which falls under the optional disclosure regime of the Google Play Store (Google, n.d.c). While this kind of data processing does not have to be disclosed in the privacy label section, the developer could still correctly inform about it in an app’s privacy policy. However, as previous empirical studies have shown, people do not tend to read long legal documents online (Bakos et al., 2014). Therefore, it is questionable if users that inform themselves via privacy labels would cross-verify the entries with the privacy policy of that app.

Implications for users and developers

The deviations of the app store privacy labels from the GDPR are problematic for several reasons. Firstly, introducing data categories that do not reflect privacy risks and allowing for optional disclosures does not provide users with accuracy and completeness of information. Complete and accurate information, however, is crucial to the principle of transparency of the GDPR and for obtaining valid consent (Zanfir-Fortuna, 2020, p. 415). Consequently, by relying on incomplete disclosures of privacy labels rather than experiencing enhanced transparency, users might inadvertently develop a false sense of protection. If the privacy labels would be GDPR compliant, on the other hand, optional disclosures would not be possible for developers. Secondly, developers could be held accountable for violating Art. 12-14 GDPR for disclosing misleading information on an app’s installation page by simply adhering to the privacy label design dictated by Google and Apple. Since disclosing privacy information via the labels has become mandatory under both the Google Developer Program Policies (Google, 2024) and the Apple App Store Review Guidelines (Apple, 2024), developers have no choice but to adhere to the policy if they do not want to risk being delisted from the app stores. Thirdly, app stores are not considered data controllers under the GDPR for data processing within third-party apps. The GDPR cannot restrict app stores in imposing a non-

compliant GDPR privacy label design on developers. In other words, developers are responsible for displaying privacy labels that do not meet the requirements of the GDPR, but app stores who require the labels cannot be held responsible. A heavy responsibility is thus placed on developers, who have limited negotiating power to change contractual provisions of powerful platforms.

The question arises as to whether privacy labels hinder developers from adhering to transparency requirements since previous empirical studies have shown that apps often do not have a privacy policy in the first place, as described in the previous section. Thus, an alternative perspective on the app stores' actions suggests that the introduction of privacy labels represents an improvement compared to a scenario where neglect of privacy compliance is widespread. However, creating GDPR-compliant labels that eliminate data categories that do not reflect privacy risks and avoid optional disclosures would not impose a significant financial burden on the app stores. This effort would align with the acknowledgment of responsibilities inherent in the intermediary function of app stores, as emphasised by numerous organisations and academics (e.g., Art. 29 WP, 2013; Cows et al., 2023; ENISA, 2017; Fong, 2017).

Consequently, by forcing the labels upon developers, app stores may not support but distort the compliance of apps with the GDPR's transparency requirements. To map the impact of the requirements imposed by Apple and Google, the next section will provide insights into how many apps have adopted the privacy labels.

Extent of compliance

Dataset and methodology

The data to perform the empirical analysis has been collected with a web scraper that is based on the scrapy python package. Scraping information about mobile apps is a common approach to assessing whether apps meet transparency requirements (Egele et al., 2011; Story et al., 2018; Viennot et al., 2014; Zimmeck et al., 2016). With the help of so-called crawl spiders, that follow links on a page based on certain requirements, I was able to collect the data of apps in the Google Play Store and the Apple App Store in Germany and the Netherlands.² Germany was selected due to its considerable size in reaching users and the Netherlands to control for country-specific deviations.³ The dataset of the German app store includes

2. The geolocation has an impact on the scraped data since certain information differs, such as the links to privacy policies, reviews, ratings, and descriptions of an app.

3. Because the Dutch scrape did not show significant differences to the German geolocation scrape,

1,657,353 apps in the Play Store and 845,375 the Apple App Store and was scraped during the month of December 2022.⁴ In 2022, the Apple App Store listed 1,783,232 apps (Apple, 2023) and the Google Play Store 2,694,114 apps (Statista, 2023b).

Next to the scrape, I collected information about embedded trackers and permissions of several apps via the Exodus Privacy Project (Exodus Privacy, n.d.a) and TrackerControl for iOS (TrackerControl, n.d.).⁵ These findings help in verifying the privacy label information, but since they have to be retrieved manually data could only be collected on a subset of the apps in the dataset.

Empirical results

Problematic level of compliance

The characteristics of the dataset are reported in Table 1. The GDPR stipulates that the controller shall inform data subjects “at the time when personal data are obtained” (GDPR, Art. 13(1)), which means that a user has to be informed about the data processing before the data collection starts (Art. 29 WP, 2018). Accordingly, there should be a clear link to the privacy policy on the installation page of an app in order for the user to have access to the information prior to the installation of an app. More than 80% of apps in both app stores have a privacy policy link on their app store page, as illustrated by Figure 3. The graph includes the percentage of privacy policy links that are the same as the link to the developer’s homepage. Since a privacy policy should be “clearly differentiated from non-privacy related information” (Art. 29 WP, 2018), it is unlikely that in these instances the link refers to a privacy policy.

Since October 2018, developers are not able to publish or update an app in the Apple App Store without providing a privacy policy link (Apple, 2018). At the Google Play Store, a similar obligation is applicable to apps that process sensitive data since July 2016 and for all apps in the Play Store starting in the second quarter of 2022 (Frey, 2021). Across all app stores and geolocations, the average rating and average number of ratings indicating an app’s popularity are lowest for apps without a privacy link, which suggests that popular apps have a better compliance with transparency obligations. Figure 3 suggests that some developers tried to cir-

the results will only be displayed in the appendix.

4. For a pseudonymised version of the dataset, see Krämer (2024).

5. The Exodus Privacy Project retrieves tracker information of apps by performing a static analysis, for more information see Exodus Privacy (2018).

cumvent the obligation to disclose a privacy policy by putting the same link as to their developer homepage. Even though the GDPR is already in force since 2018, a lot of apps still do not comply with the basic requirement of informing users about data processing practices, as highlighted by the number of apps with a missing privacy policy link.

TABLE 1: Sample characteristics

Notes: The sample size and app characteristics of the dataset, including total observations, average price, average rating and the average number of ratings. Observations are from December 2022 (German geolocation).

| | OBS. | PRICE | RATING | NUMBER OF RATINGS |
|------------------------|--------|----------|------------|-------------------|
| APPLE APP STORE | | | | |
| All | 845375 | 0.53 EUR | 3.88 stars | 477 |
| Free | 771766 | 0 EUR | 3.9 stars | 531 |
| Paid | 70448 | 6.32 EUR | 3.76 stars | 74 |
| Offering IAP | 146735 | 0.34 EUR | 3.98 stars | 683 |
| Privacy Policy link | 752833 | 0.55 EUR | 3.97 stars | 555 |
| No privacy policy link | 92542 | 0.39 EUR | 3.38 stars | 19 |

| | OBS. | PRICE | RATING | NUMBER OF RATINGS |
|---------------------------|---------|----------|------------|-------------------|
| Privacy label information | 510770 | 0.52 EUR | 4.05 stars | 768 |
| GOOGLE PLAY STORE | | | | |
| All | 1657353 | 0.21 EUR | 3.91 stars | 17308 |
| Free | 1594217 | 0 EUR | 3.9 stars | 17958 |
| Paid | 57349 | 6.01 EUR | 4.12 stars | 3172 |
| Offering IAP | 821248 | 0.05 EUR | 3.93 stars | 20746 |
| Privacy policy link | 1432218 | 0.18 EUR | 3.91 stars | 18463 |
| No privacy policy link | 225135 | 0.36 EUR | 3.9 stars | 2723 |
| Privacy label information | 703136 | 0.21 EUR | 3.96 stars | 23918 |

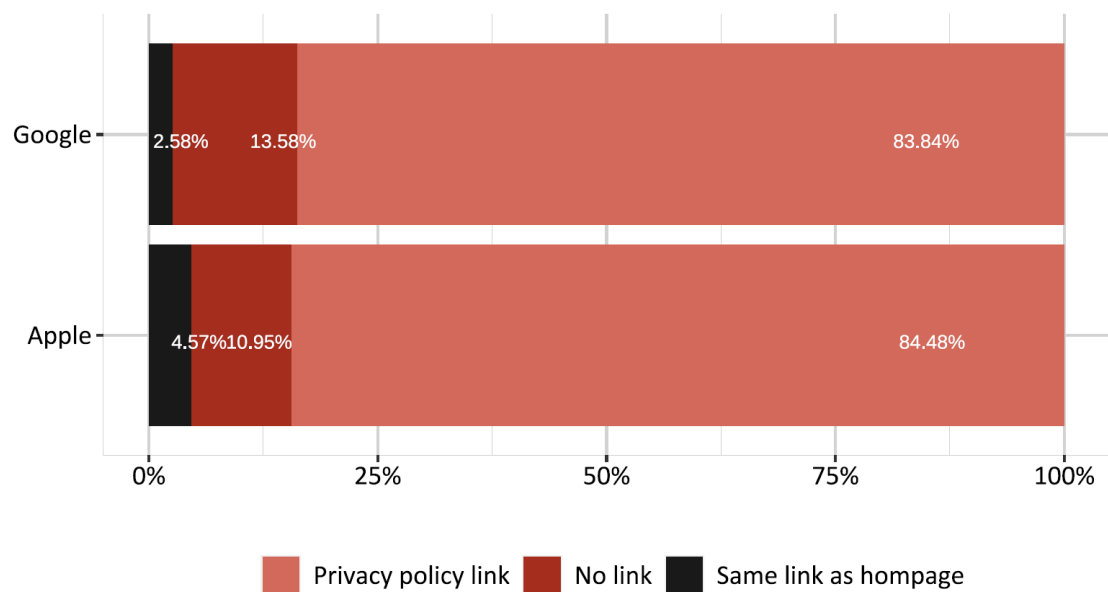


Figure 3: Apps with privacy policies. The figure presents the percentage of apps with a privacy policy link in the Apple App Store (N=845.375) and the Google Play Store (N=1.657.353). Observations are from December 2022 (German geolocation).

Privacy labels have become mandatory in both app stores due to provisions in the Google Developer Program Policies (Google, 2024) and the Apple App Store Review Guidelines. As illustrated by Figure 4, 60.5% of the apps in the Apple App Store have privacy labels, of which 25.2% state that they do not collect any data. In the Google Play Store, 42.4% adopted privacy labels, of which 19.6% disclose that they do not process any data. Nevertheless, in the Apple App Store 39.6% and in the Play Store 57.6% of the apps in the sample do not yet comply with the privacy label obligation.⁶

6. The difference could be due to the different time periods the privacy label policy is in place. Apple already introduced the obligation in December 2020, Google followed suit in April 2022.

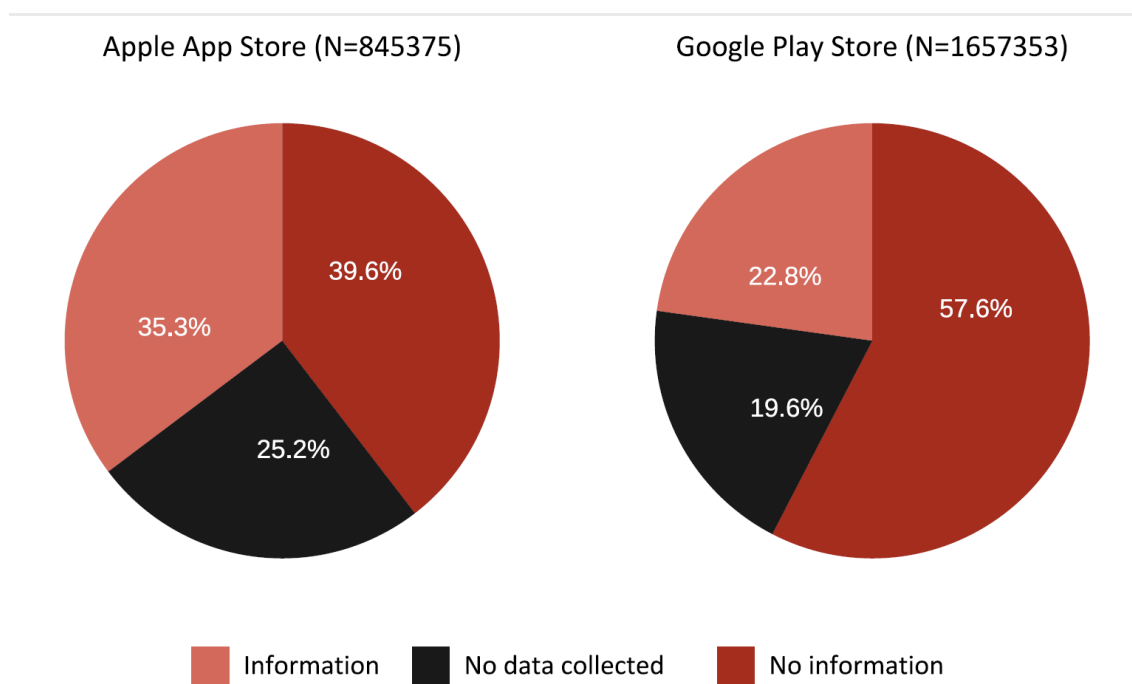


Figure 4: Percentage of apps with privacy labels. The figure depicts the percentage of apps that have privacy label information, disclose that they do not collect any data, or do not have privacy information yet. Observations are from December 2022 (German geolocation).

Problematic sense of protection

Figure 5 plots the privacy label disclosures of apps in the Apple App Store and depicts the number of data categories collected for the entire store (N=845,375) and Apple-owned apps (N=80), differentiated by three data types. Surprisingly, Apple-owned apps do not disclose any data they are processing as tracking. A similar observation is made in the Google Play Store when comparing Google-owned apps (N=140) with the rest of the sample (N=1,657,353). Figure 6 shows that only eight Google-owned apps disclose data processing that falls into the “Data Shared” category.

However, compared to the collected data from the Exodus and TrackerControl project, as indicated by Table 2, at least 15 (of 24 analysed) apps from Apple embed trackers. Moreover, at least 63 out of 116 analysed apps from Google demonstrate a similar trend.⁷ These observations suggest that the design of the privacy labels tend to benefit developers offering a range of services that involve data processing across apps, primarily due to the distinction between first and third-party tracking inherent to the privacy label definitions. Given that both Google and Apple provide an array of services within their individual ecosystems, the transfer of personal da-

7. The number is most likely higher since the analysis did not succeed for every app. A detailed table of the results can be found in the appendix, table A2.

ta may occur internally among their own apps. Consequently, there may be no necessity for the data to be transmitted to third parties to have the ability to construct a comprehensive user profile.⁸ To illustrate, data collected within Apple-owned apps like Shazam, Apple music, and Apple TV can be processed to create a detailed user profile without this practice falling into the “Data used to track” category of the Apple App Store. The same can be said about Google-owned services: if data from YouTube, Google Maps or Gmail are combined this does not have to be disclosed in the “Data Shared” category of the Google Play Store. This suggests that the design of the privacy labels in the app stores exempt own data tracking practices, which ultimately leads to a false sense of protection of users and has the potential to place apps of other developers in a less favourable position.

8. Insights into apps of other developers that are likewise offering a number of different apps and services, such as Meta or Microsoft, that show a similar pattern can be found in the appendix (Table A1)

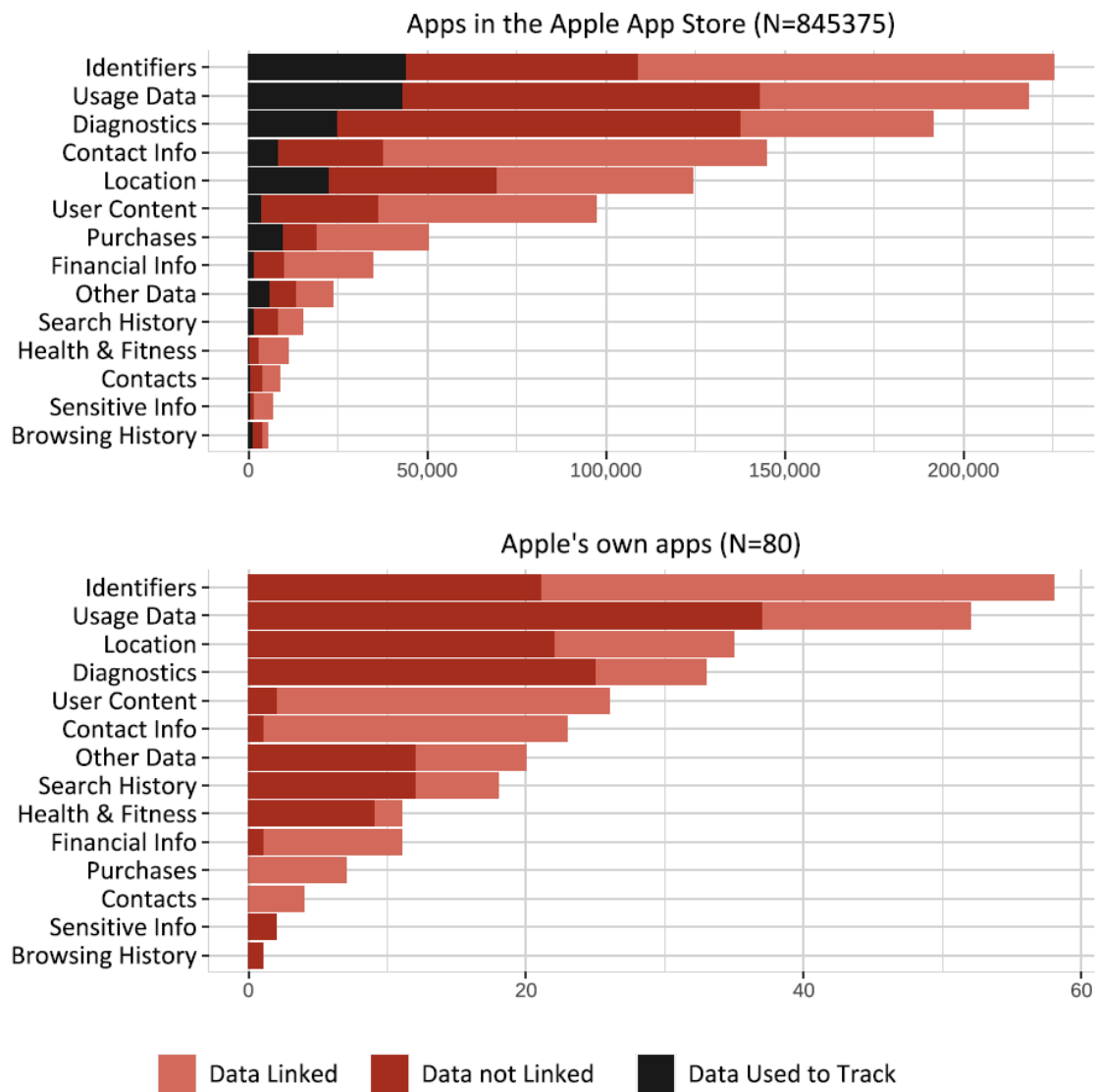


Figure 5: Observations by data category (Apple App Store). The figure depicts data categories and data types of apps in the Apple App Store and Apple-owned apps. Observations are from December 2022 (German geolocation).

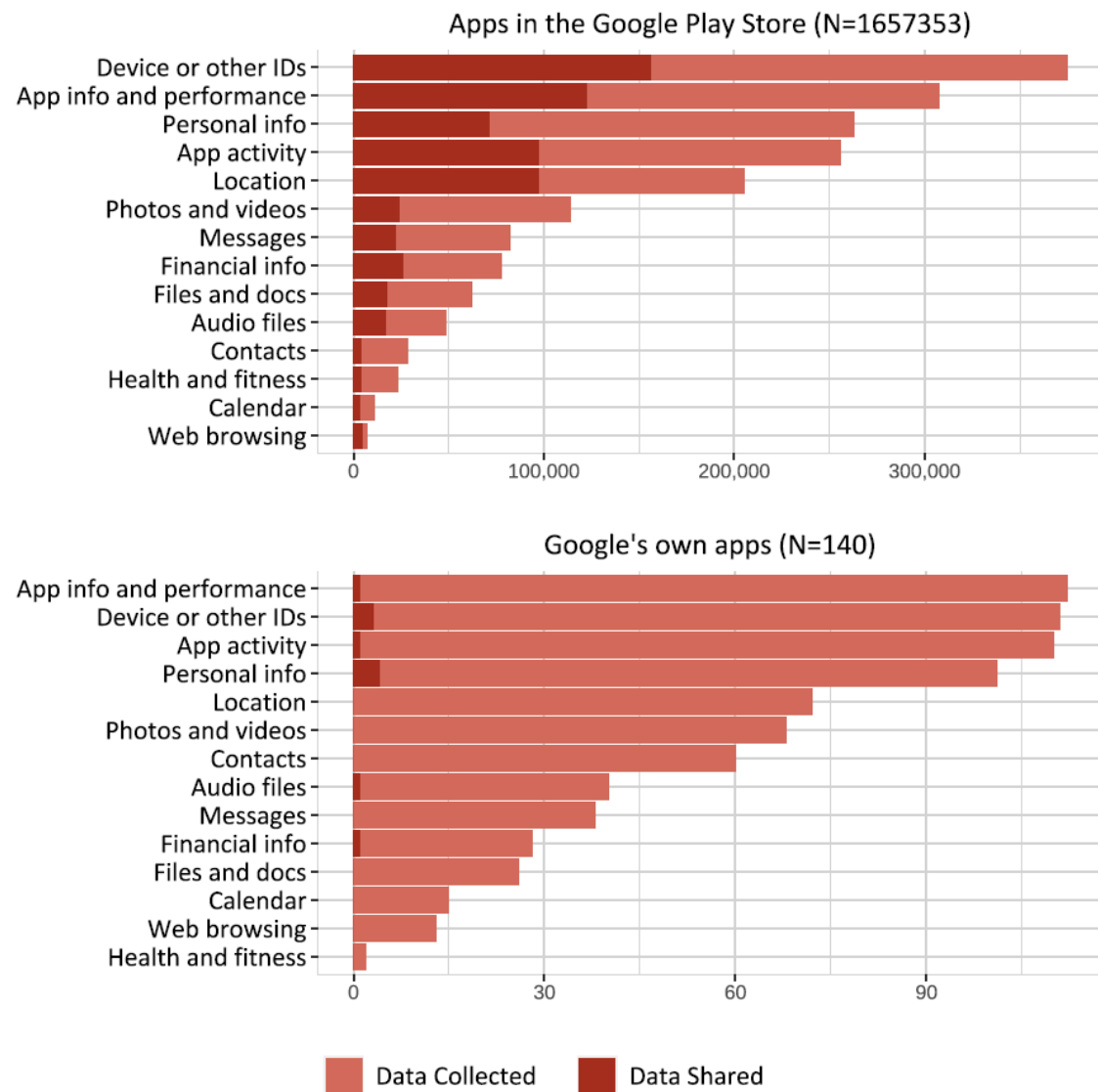


Figure 6: Observations by data category (Google Play Store). The figure depicts data categories and data types of apps in the Google Play Store and Google-owned apps. Observations are from December 2022 (German geolocation).

TABLE 2:Tracker in Apple's and Google's own apps

Notes: Information about Apple's own apps in the Apple App Store and Google's own apps in the Play Store. The data about embedded trackers has been collected via the iOS Trackercontrol project (n.d.) and the Exodus privacy project (n.d.a). The "Tracker" column denotes the number of apps with trackers present.

| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA NOT LINKED | DATA LINKED | DATA USED TO TRACK | TRACKER |
|--------------------|------|---------------|-------------------|-----------------|-------------|--------------------|---------|
| IOS TRACKERCONTROL | | | | | | | |
| Apple's apps | 80 | 68 | 9 | 45 | 38 | 0 | 15 |
| Analysed Apps | 24 | 23 | 1 | 17 | 16 | 0 | 15 |
| Non-analysed Apps | 56 | 45 | 8 | 28 | 22 | 0 | NA |
| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA COLLECTED | DATA SHARED | | TRACKER |
| EXODUS PRIVACY | | | | | | | |
| Google's own apps | 140 | 137 | 3 | 112 | 8 | | 63 |
| Analysed apps | 115 | 112 | 3 | 99 | 8 | | 63 |
| Non-analysed apps | 26 | 26 | 0 | 13 | 0 | | NA |

Problematic self-disclosures by developers

The results highlight the issue of privacy information based on the developers' self-assessment. In contrast to the Play Store, in the Apple App Store developers can offer information about the processing of non-personal data, denoted by the data type "Data not linked". Figure 7 illustrates that of the 298,117 apps in the Apple App Store that have a privacy label, 36,856 indicate that a data category is both "Data not Linked" and "Data used to Track you" or "Data Linked". The statement that data is not linked to a person but is nevertheless used to track that same person, however, is inherently contradictory (Bundeskartellamt, 2021, p. 109). These contradictory disclosures amount to 12.3% of all the privacy label disclosures within the sample of the Apple App Store.

Another example of contradictory disclosures is the categorisation of developers concerning contact info, online identifiers, contacts, and location data. In the Apple App Store, 29,420 apps marked contact info, 64,966 identifiers, 46,684 location data, and 3,502 contact data as not linkable to a user. Apple's guidelines specify that data falling into this category must be either 'de-identified' or 'anonymised', for instance by 'manipulating data to break the linkage and prevent re-linkage to world identities' (Apple, n.d.a). Article 4(1) GDPR, however, states that location data has

to be regarded as personal data. Recital 30 GDPR provides guidance that online identifiers provided by devices may also count as personal data as they can allow for the identification of users. Contacts and contact info usually involve the name, phone number, addresses or the birthday of an individual. Consequently, it is unlikely that these categories do not represent personal data as indicated by the label “Data not Linked”. In total, 142,086 apps disclosed one or more of these categories as “Data not linked”, which amounts to 16.81% of the whole sample.

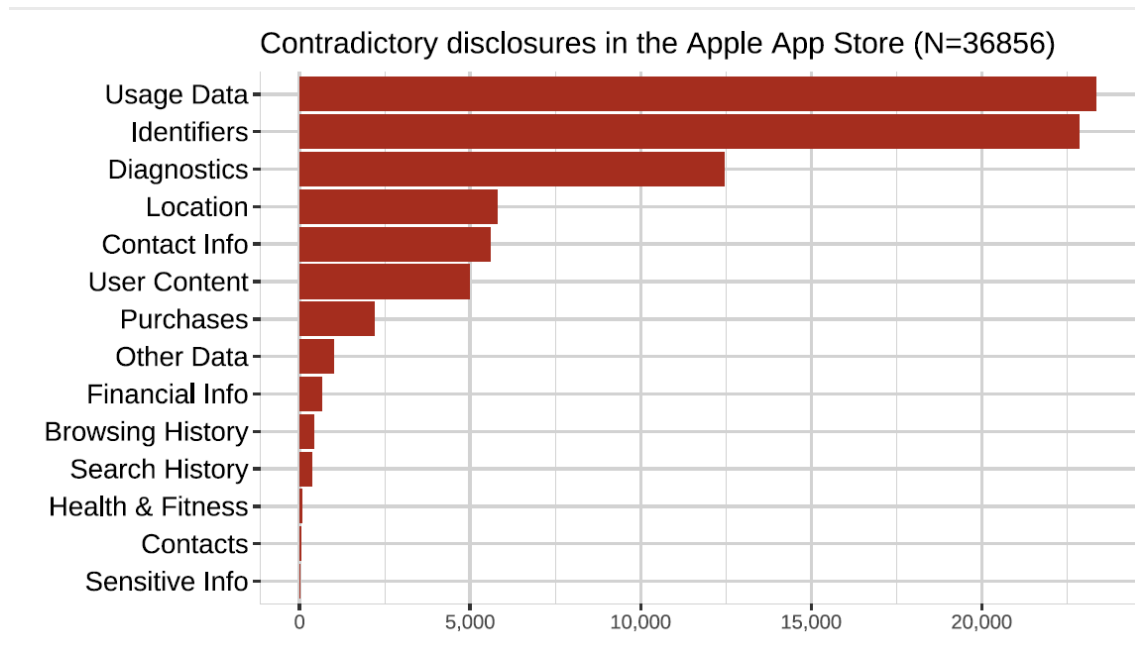


Figure 7: Contradictory disclosures (Apple App Store). The figure presents the data categories of apps in the Apple App Store with 36.856 apps disclosing the same data categories in both data types “Data not Linked” and “Data used to Track you” or “Data Linked to you”, observations from December 2022 (German geolocation).

Discussion and limitations

Discussion

The privacy labels enforced by app stores partly do not comply with the requirements of the GDPR. The different definitions are problematic in this sense, in particular because the types of data upon which the labels are based do not reflect privacy risks. In addition, the labels are accompanied by several optional disclosures which undermines the purpose of the principle of transparency. These obligations can be seen as examples of app stores setting standards that affect data protection compliance when they act as intermediaries between users and developers, taking advantage of a lack of legal restrictions. This case further demonstrates how the design of platforms supports only certain ways of doing privacy, a

phenomenon that Greene and Shilton (2017) refer to as “privacy by permitted design” or “privacy by platform” (p. 1655).

The results illustrate that app stores have wide discretion in setting standards for required information outside the data controller framework. As Waldman (2021) has noted, “industry may say that it wants to ‘do better’ when it comes to privacy, but only if ‘privacy’ means what industry wants it means” (p.47). This statement is reflected in the findings of this paper: the app stores promote a privacy-friendly discourse by introducing privacy labels but, as the results have shown, the standards set by Apple and Google preclude their own tracking activities. Even though a considerable part of their apps embed tracker libraries, they do not fall within the categories “Data used to Track you” by Apple or “Data Shared” by Google. This is because the design of the labels does not capture data sharing with first-party but third-party services, which has, however, the potential to mislead consumers who gain a false sense of protection of their privacy and can negatively impact apps by other developers. While it is accurate to acknowledge the high privacy risk associated with third-party tracking given its capability to trace connections from multiple apps to a single user (Binns et al., 2018), a similar concern arises with first-party tracking across multiple apps. This concern becomes pronounced when the first party owns a variety of services that also facilitate the creation of detailed profiles of users.

The empirical results support statements made by Kollnig et al. (2022, p. 9) and the CMA (CMA, 2022) in relation to the definitions of the privacy labels that suggest the definitions benefit Apple’s own tracking practices over that of third-parties. The results contribute to the discussion on how to address platforms that act as privacy regulators outside the scope of data protection law. Van Hoboken and Fathaigh (2021) propose an official disclosure regime that obliges app stores to be more transparent about the impact of their regulatory function. While this proposal could help provide an overall picture of the number of apps removed from app stores for failing to comply with Google and Apple’s transparency obligations, it would likely not address the flawed design of the imposed definitions.

This paper has highlighted contradictions in self-disclosures by developers, which suggests that disclosures are neither flagged nor verified by the app stores. These findings support previous studies which showed problematic self-disclosures that did not match actual data flows within the Apple App Store (Koch et al., 2022; Xiao et al., 2022). As a possible response to this, Cranor (2022, p. 28) suggests that app stores should implement techniques to automatically verify privacy labels. Building upon this suggestion, introducing tools within an app publishing process

that preclude contradictory disclosures and notify developers thereof should be a feasible improvement of the current disclosure regime. This should be a necessary step, bearing in mind the responsibilities that come with the intermediary function of app stores.

Limitations

Since there is no official list nor number of apps in the app stores, the collection of app data for this paper depends on the recommendation algorithm of the respective app store and does not scrape all available apps in both stores. Because Apple and Google have an incentive to favour their own apps and apps that use Apple's or Google's in-app payment system based on a direct monetary profit, there may be a risk that users will not receive apps that are recommended based on objective factors (CMA, 2022, p. 209). Neither app store discloses the factors underlying their app ranking and recommendation system, so there is a possibility of bias in the data sample. Furthermore, there exists no official account of the number of apps in the Google Play Store, and the number of apps in the Apple App Store are only reported annually in the App Store Transparency Report (Apple, 2023). Consequently, it is difficult to evaluate if the number of apps in the dataset includes the total number of apps in the app stores.

Conclusion

This paper sought to illustrate how self-regulatory practices by app stores affect apps in their compliance with transparency obligations with the GDPR. Firstly, the analysis of the recently introduced privacy labels of Apple and Google reveals some profound differences in the distinction between the different data types and data categories than is recognized in the GDPR. Furthermore, some characteristics of the privacy labels do not comply with the transparency requirements of the GDPR. Especially problematic are the different data categories that do not reflect privacy risks and optional disclosures of certain data processing practices. Secondly, the design of these labels appears to favour developers offering a diverse range of apps capable of processing data across various services, such as apps of Apple and Google, placing them in more favourable label categories compared to apps from other providers. This can lead to users having a false sense of protection when it comes to the processing of their data and puts other apps in a less favourable position, as users might be inclined to think that their data is better protected by these developers. Thirdly, this paper highlighted the problem of self-assessments of developers by showing the extent of contradictory disclosures of apps. Since the privacy label disclosures are not verified by the app stores, contra-

dictory information is not flagged which has the potential of confusing users.

Privacy labels have the potential to inform users in an easy and effective manner about data processing practices. Nevertheless, enforcement to ensure correct privacy disclosures does not only have to stem from app stores but from regulators as well. Examining whether developers are forced to employ inaccurate labels, due to their design, through a comparison of an app's privacy policy could be a valuable avenue for future research. Additionally, further investigations may explore how emerging legislation, such as the Digital Services Act, could potentially address the issues emphasised in this paper.

ACKNOWLEDGEMENTS

The author would like to thank the participants and reviewers of the CPDP 2023 conference, the managing editor Frédéric Dubois, the academic editor David Dueñas-Cid and both reviewers for their valuable comments and suggestions.

References

- Apple. (n.d.a). *App privacy details on the App Store*. Apple Developer. <https://developer.apple.com/app-store/app-privacy-details/>
- Apple. (n.d.b). *Apple developer license agreement*. Apple Developer. <https://developer.apple.com/support/terms/apple-developer-program-license-agreement/>
- Apple. (2018, August 31). *Privacy policy reminder*. Apple News. <https://developer.apple.com/news/?id=08312018a>
- Apple. (2023). *App Store transparency report* [Report]. <https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf>
- Apple. (2024, March 5). *App review guidelines*. Apple Developer. <https://developer.apple.com/app-store/review/guidelines/>
- Article 29 Data Protection Working Party (Art.29 WP). (2013). *Opinion 02/2013 on apps on smart devices* (Opinion 00461/13/EN WP 202). European Union. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
- Article 29 Data Protection Working Party (Art.29 WP). (2018). *Guidelines on transparency under Regulation 2019/679* (Guidelines 17/EN WP260 rev.01). European Union. <https://ec.europa.eu/newsroom/article29/items/622227>
- Autoriteit Consument & Markt. (2019). *Market study into mobile app stores* (Report ACM/18/032693). <https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf>

Autoriteit Consument & Markt. (2021). *Google to require providers to add information about data use to apps in its app store* [Press release]. <https://www.acm.nl/en/publications/google-require-provider-s-add-information-about-data-use-apps-its-app-store>

Ayres, I., & Schwartz, A. (2014). The no-reading problem in consumer contract law. *Stanford Law Review*, 66(3), 545–610. <https://www.jstor.org/stable/24246723>

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies*, 43(1), 1–35. <https://doi.org/10.1086/674424>

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. *Proceedings of the 10th ACM Conference on Web Science*, 23–31. <https://doi.org/10.1145/3201064.3201089>

Bundeskartellamt (last). (2021). *Sektoruntersuchung Mobile Apps* [Sector investigation into mobile apps] (Report Az. V-35/20). Bundeskartellamt. https://www.bundeskartellamt.de/SharedDocs/Publication/DE/Sektoruntersuchungen/Sektoruntersuchung_Mobile_Apps.pdf?__blob=publicationFile&v=4

Bygrave, L. A., & Tosoni, L. (2020). Article 4(1) Personal data. In C. Kuner, L. A. Bygrave, C. Docksey, & L. Drechsler (Eds.), *The EU General Data Protection Regulation (GDPR). A commentary* (pp. 103–115). Oxford University Press New York. <https://doi.org/10.1093/oso/9780198826491.003.0007>

Case C-40/17. (2019). *Judgment of the Court (Second Chamber) of 29 July 2019: FashionID GmbH and Co. KG v. Verbraucherzentrale NRW e.V.* The Court of Justice of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0040&qid=1702977836463>

Case C-210/16. (2018). *Judgment of the Court (Grand Chamber) of 5 June 2018: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* [Judgment of the Court (Grand Chamber) of 5 June 2018: Independent Centre for Data Protection Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH]. The Court of Justice of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210&qid=1702977705002>

Competition and Markets Authority (CMA). (2022). *Mobile ecosystems: Market study final report* [Report]. UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL_.pdf

Cowls, J., Morley, J., & Floridi, L. (2023). App store governance: Implications, limitations, and regulatory responses. *Telecommunications Policy*, 47(1), Article 102460. <https://doi.org/10.1016/j.telpol.2022.102460>

Cranor, L. F. (2022). Mobile-app privacy nutrition labels missing key ingredients for success. *Communications of the ACM*, 65(11), 26–28. <https://doi.org/10.1145/3563967>

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS: Detecting privacy leaks in iOS applications. *Proceedings of the Network and Distributed System Security Symposium*. NDSS 2011, 18th Annual Network and Distributed System Security Symposium, San Diego, California. <https://sites.cs.ucsb.edu/~chris/research/doc/ndss11-pios.pdf>

European Union Agency for Cybersecurity (ENISA). (2017). *Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of the GDPR*. European Network and Information Security Agency. <https://doi.org/10.2824/114584>

Exodus Privacy. (n.d.a). *Exodus privacy project*. <https://exodus-privacy.eu.org/en/>

- Exodus Privacy. (n.d.b). *Trackers*. <https://reports.exodus-privacy.eu.org/en/info/trackers/>
- Exodus Privacy. (2018, August 17). *Exodus static analysis*. https://exodus-privacy.eu.org/en/post/exodus_static_analysis/
- Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11–36. <https://doi.org/10.1093/idpl/ipz026>
- Fong, A. (2017). The role of app intermediaries in protecting data privacy. *International Journal of Law and Information Technology*, 25(2), 85–114. <https://doi.org/10.1093/ijlit/eax002>
- Fox, G., Tonge, C., Lynn, T. G., & Mooney, J. (2018). Communicating compliance: Developing a GDPR privacy label. *AMCIS 2018 Proceedings*. Twenty-fourth Americas Conference on Information Systems. <https://aisel.aisnet.org/amcis2018/Security/Presentations/30>
- Franck, J.-U., & Peitz, M. (2021). Digital platforms and the new 19a tool in the German Competition Act. *Journal of European Competition Law & Practice*, 12(7), 513–528. <https://doi.org/10.1093/jeclap/lpab055>
- Frey, S. (2021, May 6). New safety section in Google Play will give transparency into how apps use data. *Android Developers Blog*. <https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html>
- Gardner, J., Feng, Y., Reiman, K., Lin, Z., Jain, A., & Sadeh, N. (2022). *Helping mobile application developers create accurate privacy labels*. 212–230. <https://doi.org/10.1109/EuroSPW55150.2022.00028>
- Gartenberg, C. (2020, December 9). Apple's privacy labels are coming to all apps, including its own. *The Verge*. <https://www.theverge.com/2020/12/9/22165959/apple-privacy-nutrition-labels-all-apps-preinstalled->
- German Competition Act. (2013). *Competition Act (Gesetz gegen Wettbewerbsbeschränkungen—GWB)*. Federal Ministry of Justice Germany. https://www.gesetze-im-internet.de/englisch_gwb/
- Google. (n.d.a). *Enforcement*. Developer Policy Center. <https://support.google.com/googleplay/android-developer/topic/9877468>
- Google. (n.d.b). *Review how your app collects and shares user data*. Android Developers. <https://developer.android.com/privacy-and-security/declare-data-use>
- Google. (n.d.c). *Understand app privacy & security practices with Google Play's Data safety section*. Google Play Help Centre. https://support.google.com/googleplay/answer/11416267?hl=en&ref_topic=3171690
- Google. (n.d.d). *User data*. Google Play Help Centre. <https://support.google.com/googleplay/android-developer/answer/10144311?hl=en>
- Google. (2024). *Developer program policy* [Policy statement]. <https://support.google.com/googleplay/android-developer/answer/14444345?hl=en>
- Greene, D., & Shilton, K. (2017). Platform privacies: Governance, collaboration, and the different meanings of “privacy” in iOS and Android development. *New Media & Society*, 20(4), 1640–1657. <https://doi.org/10.1177/1461444817702397>
- Iqbal, M. (2024). *App revenue data (2024)*. Business of Apps. <https://www.businessofapps.com/data/a>

pp-revenues/

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralized data processing: Personal data stores and the GDPR. *International Data Privacy Law*, 10(4), 356–384. <https://doi.org/10.1093/idpl/ipaa016>

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A 'nutrition label' for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1–12. <https://doi.org/10.1145/1572532.1572538>

Koch, S., Wessels, M., Altpeter, B., Olvermann, M., & Johns, M. (2022). Keeping privacy labels honest. *Proceedings on Privacy Enhancing Technologies*, 486–506. <https://doi.org/10.56553/popets-2022-0119>

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 508–520. <https://doi.org/10.1145/3531146.3533116>

Krämer, J. (2024). *The death of privacy policies* [dataset]. Open Science Framework (OSF). <https://doi.org/10.17605/OSF.IO/TNG5F>

Li, Y., Chen, D., Li, T., Agarwal, Y., Cranor, L. F., & Hong, J. I. (2022). Understanding iOS Privacy nutrition labels: An exploratory large-scale analysis of app store data. *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–7. <https://doi.org/10.1145/3491101.3519739>

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543–568. <http://hdl.handle.net/1811/72839>

Parker, L., Halter, V., Karliychuk, T., & Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry*, 64, 198–204. <https://doi.org/10.1016/j.ijlp.2019.04.002>

Perez, S. (2020, December 14). Apple launches its new app privacy labels across all its App Stores. *TechCrunch*. <https://techcrunch.com/2020/12/14/apple-launches-its-new-app-privacy-labels-across-all-its-app-stores/>

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1425>

Polčák, R. (2020). Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 398–412). Oxford University Press. <https://doi.org/10.1093/oso/9780198826491.003.0042>

Regulation 2016/67. (2016). *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)*. European Parliament and Council. <http://data.europa.eu/eli/reg/2016/679/oj>

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903. <http://www.jstor.org/stable/23415060>

Statista. (September 1, 2023a). *Market share of leading mobile operating systems in Europe from 2010 to 2022* [dataset]. <https://web.archive.org/web/20240203111948/https://www.statista.com/statistics/639928/market-share-mobile-operating-systems-eu/>

Statista. (September 5, 2023b). *Number of available applications in the Google Play Store from December 2009 to June 2023* [dataset]. <https://web.archive.org/web/20231218133923/https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>

Statista. (December 8, 2023c). *Number of apps available in leading app stores Q3 2022* [dataset]. <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

Story, P., Zimmeck, S., & Sadeh, N. (2018). Which apps have privacy policies? An analysis of over one million Google Play Store apps. In M. Medina, A. Mittrakas, K. Rannenberg, E. Schweighofer, & N. Tsouroulas (Eds.), *Privacy Technologies and Policy* (Vol. 11079, pp. 3–23). Springer. https://doi.org/10.1007/978-3-030-02547-2_1

TrackerControl. (n.d.). *TrackerControl for iOS*. <https://ios.trackercontrol.org/>

van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1414>

van Hoboken, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, 41, 1–18. <https://doi.org/10.1016/j.clsr.2021.105557>

Viennot, N., Garcia, E., & Nieh, J. (2014). A measurement study of google play. *The 2014 ACM International Conference on Measurement and Modeling of Computer Systems*, 221–233. <https://doi.org/10.1145/2591971.2592003>

Waldman, A. E. (2021). *Industry unbound: The inside story of privacy, data, and corporate power*. Cambridge University Press. <https://doi.org/10.1017/9781108591386>

Xiao, Y., Li, Z., Qin, Y., Bai, X., Guan, J., Liao, X., & Xing, L. (2022). *Lalaine: Measuring and characterizing non-compliance of Apple privacy labels at scale* (Version 2). arXiv. <https://doi.org/10.48550/ARXIV.2206.06274>

Zanfir-Fortuna, G. (2020). Article 13 Information to be provided where personal data are collected from the data subject. In C. Kuner, L. A. Bygrave, C. Docksey, & L. Drechsler (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 413–433). Oxford University Press New York. <https://doi.org/10.1093/oso/9780198826491.003.0044>

Zhang, S., Feng, Y., Yao, Y., Cranor, L. F., & Sadeh, N. (2022). How usable are iOS app privacy labels? *Proceedings on Privacy Enhancing Technologies*, 204–228. <https://doi.org/10.56553/popets-2022-0106>

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Lui, B., Schaub, F., Wilson, S., Sadeh, N., Bellovin, S. M., & Reidenberg, J. (2016). *Automated analysis of privacy requirements for mobile apps* (Technical Report FS-16-04; The 2016 AAAI Fall Symposium Series: Privacy and Language Technologies, pp. 286–296). <https://sebastianzimmeck.de/zimmeckEtAlCompliance2017ShortPaper.pdf>

Appendix

A. Additional figures and tables

TABLE A1: Sample characteristics privacy labels

Notes: The number of apps in the Apple App Store and Google Play Store that either have any privacy label, or state they do not collect data. Apps that categorise data at least once within the data type “Data not Linked”, “Data Linked”, and “Data used to track” in the Apple App Store, and “Data Collected” and “Data Shared” in the Google Play Store. The data has been scraped with German geolocation in December 2022.

| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA NOT LINKED | DATA LINKED | DATA USED TO TRACK |
|-------------------|---------|---------------|-------------------|-----------------|-------------|--------------------|
| APPLE APP STORE | | | | | | |
| Total sample | 845375 | 298117 | 212653 | 142281 | 142890 | 48572 |
| BY DEVELOPER | | | | | | |
| Apple | 80 | 68 | 9 | 38 | 45 | 0 |
| Google | 60 | 58 | 0 | 58 | 19 | 0 |
| Meta | 15 | 15 | 0 | 15 | 0 | 2 |
| Amazon | 30 | 27 | 0 | 24 | 6 | 1 |
| Microsoft | 83 | 59 | 2 | 46 | 23 | 4 |
| BY CATEGORY | | | | | | |
| Games | 127031 | 38926 | 13680 | 15485 | 19140 | 19428 |
| Education | 88512 | 26255 | 24827 | 8875 | 12573 | 2675 |
| Health & Fitness | 86774 | 38049 | 20255 | 21964 | 15318 | 3526 |
| Business | 84684 | 29153 | 28712 | 15405 | 11770 | 1455 |
| Utilities | 69090 | 18717 | 24270 | 7642 | 9048 | 2218 |
| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA COLLECTED | DATA SHARED | |
| GOOGLE PLAY STORE | | | | | | |
| Total sample | 1663879 | 1338599 | 325280 | 295484 | 228209 | |
| BY DEVELOPER | | | | | | |
| Apple | 7 | 6 | 1 | 6 | 0 | |
| Google | 140 | 137 | 3 | 112 | 8 | |
| Meta | 16 | 15 | 1 | 15 | 10 | |
| Amazon | 34 | 33 | 1 | 33 | 21 | |
| Microsoft | 76 | 73 | 3 | 69 | 19 | |

| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA NOT LINKED | DATA LINKED | DATA USED TO TRACK |
|------------------|--------|---------------|-------------------|-----------------|-------------|--------------------|
| APPLE APP STORE | | | | | | |
| Total sample | 845375 | 298117 | 212653 | 142281 | 142890 | 48572 |
| BY DEVELOPER | | | | | | |
| Apple | 80 | 68 | 9 | 38 | 45 | 0 |
| Google | 60 | 58 | 0 | 58 | 19 | 0 |
| Meta | 15 | 15 | 0 | 15 | 0 | 2 |
| Amazon | 30 | 27 | 0 | 24 | 6 | 1 |
| Microsoft | 83 | 59 | 2 | 46 | 23 | 4 |
| BY CATEGORY | | | | | | |
| Games | 127031 | 38926 | 13680 | 15485 | 19140 | 19428 |
| Education | 88512 | 26255 | 24827 | 8875 | 12573 | 2675 |
| Health & Fitness | 86774 | 38049 | 20255 | 21964 | 15318 | 3526 |
| Business | 84684 | 29153 | 28712 | 15405 | 11770 | 1455 |
| Utilities | 69090 | 18717 | 24270 | 7642 | 9048 | 2218 |
| | OBS. | PRIVACY LABEL | NO DATA COLLECTED | DATA COLLECTED | DATA SHARED | |
| BY CATEGORY | | | | | | |
| Education | 194359 | 152253 | 42106 | 36961 | 31562 | |
| Tools | 108479 | 80592 | 27887 | 12938 | 9339 | |
| Business | 107117 | 87442 | 19675 | 18667 | 7678 | |
| Entertainment | 95173 | 75747 | 19426 | 10219 | 10672 | |
| Music & Audio | 94651 | 77661 | 16990 | 9480 | 21168 | |

B. Results robustness scrape: Dutch geolocation

TABLE B1: Sample characteristics
Notes: The sample size and app characteristics of the dataset, including total observations, average price, average rating, and the average number of ratings. Observations are from December 2022, scraped with Dutch geolocation.

| | OBS. | PRICE | RATING | NUMBER OF RATINGS |
|-----------------|--------|----------|------------|-------------------|
| APPLE APP STORE | | | | |
| All | 827249 | 0.53 EUR | 3.94 stars | 2198 |
| Free | 754623 | 0 EUR | 3.96 stars | 2477 |
| Paid | 69551 | 6.29 EUR | 3.77 stars | 134 |
| Offering IAP | 144411 | 0.34 EUR | 4.07 stars | 2643 |

| | OBS. | PRICE | RATING | NUMBER OF RATINGS |
|------------------------|---------|----------|------------|-------------------|
| Privacy Policy link | 735913 | 0.55 EUR | 4.02 stars | 2573 |
| No privacy policy link | 91336 | 0.39 EUR | 3.46 stars | 35 |
| Privacy label | 499457 | 0.52 EUR | 4.1 stars | 3580 |
| GOOGLE PLAY STORE | | | | |
| All | 1663879 | 0.21 EUR | 4 stars | 30621 |
| Free | 1577660 | 0 EUR | 3.99 stars | 31316 |
| Paid | 57077 | 6.06 EUR | 4.21 stars | 7540 |
| Offering IAP | 825042 | 0.05 EUR | 4.03 stars | 34494 |
| Privacy policy link | 1437632 | 0.19 EUR | 4 stars | 31890 |
| No privacy policy link | 226247 | 0.36 EUR | 3.88 stars | 6473 |
| Privacy label | 702534 | 0.21 EUR | 4.06 stars | 38647 |

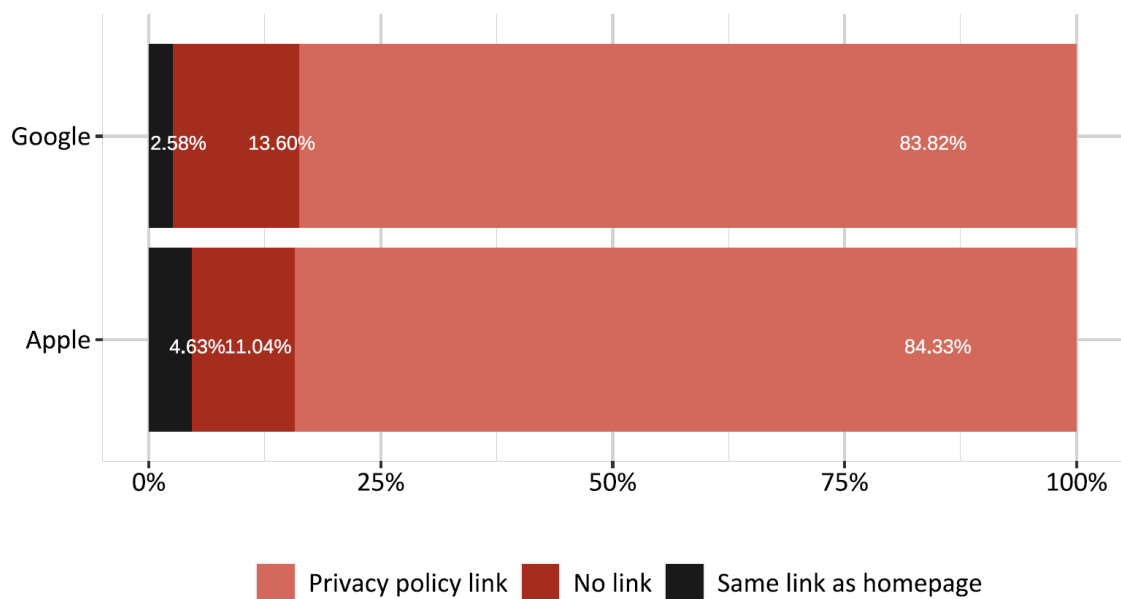


Figure B1: Apps with privacy policies. The figure presents the percentage of apps in the Apple App Store (N=827,249) and Google Play Store (N=1,663,879), observations from December 2022, Dutch geolocation.

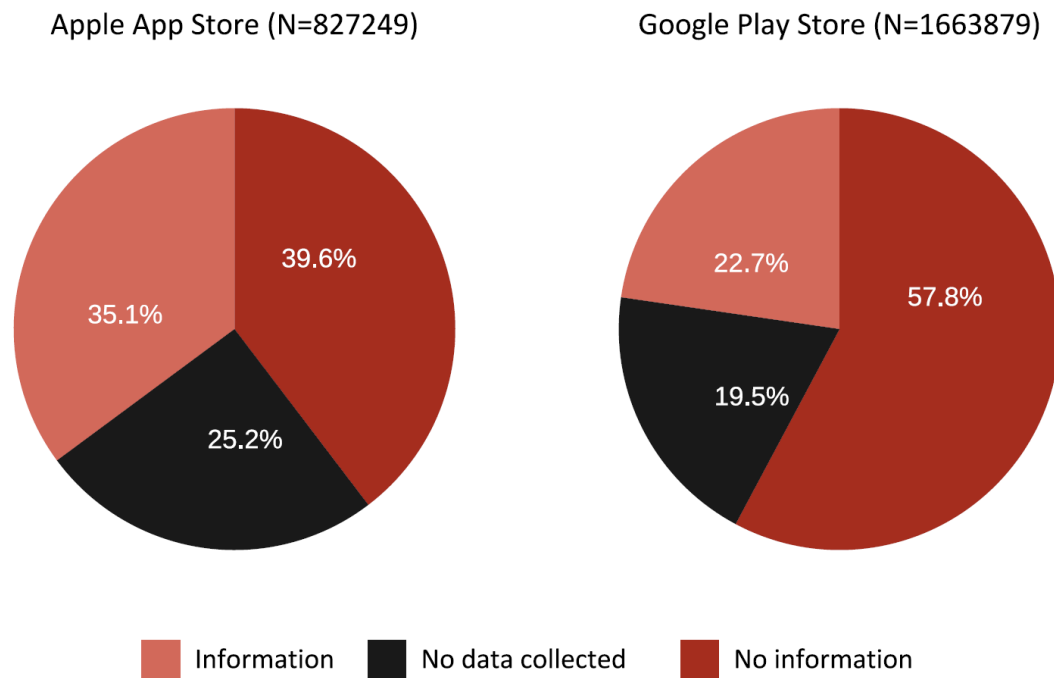


Figure B2: Number of apps with privacy label. The figure presents the shares of apps with privacy labels in the Apple App Store (N=827,249) and the Google Play Store (N=1,663,879), observations from December 2022, Dutch geolocation.

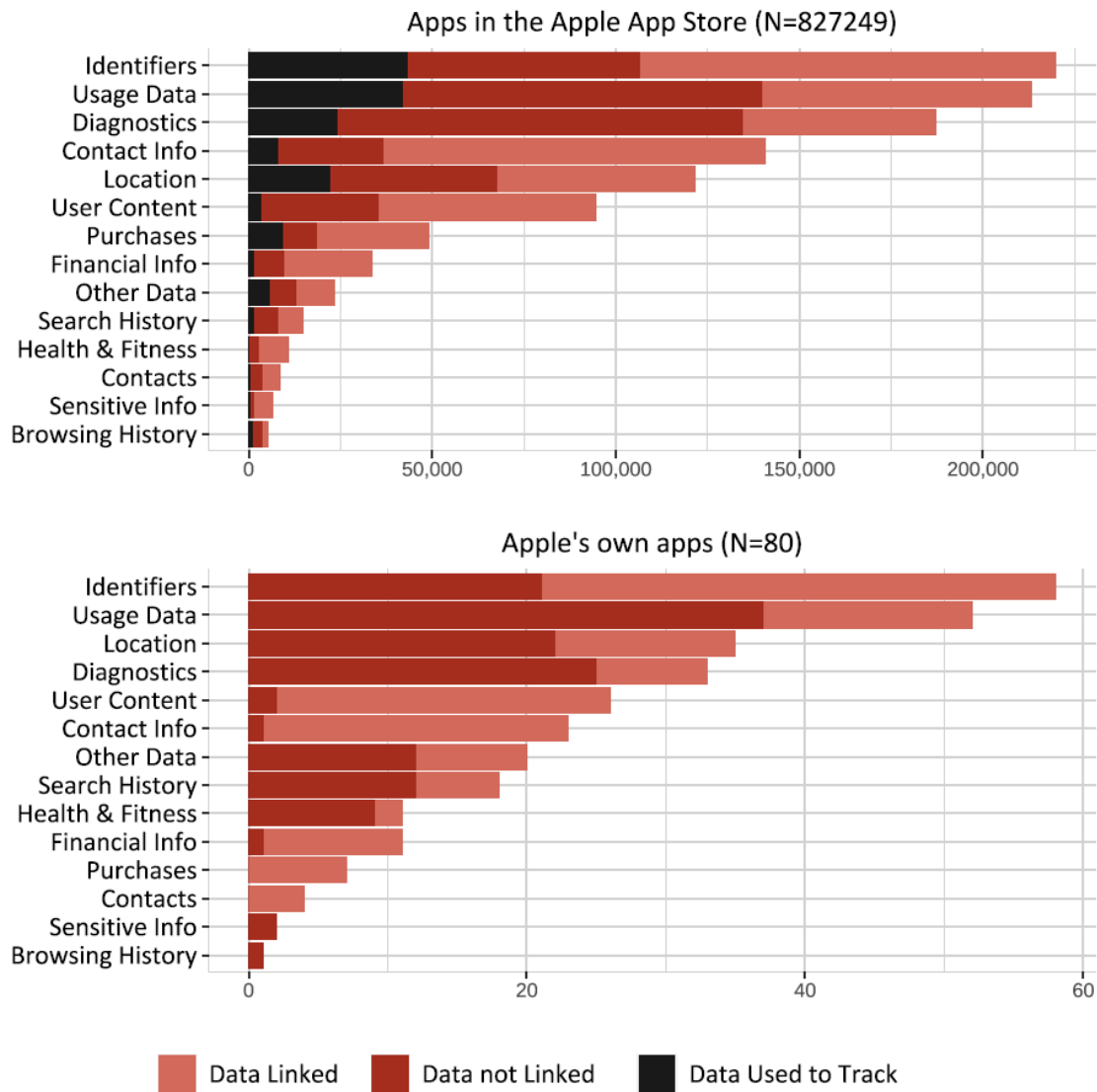


Figure B3: Observations by data category (Apple App Store). The figure presents the data categories and data types of apps in the Apple App Store (N=845,375), observations are from December 2022, Dutch geolocation.

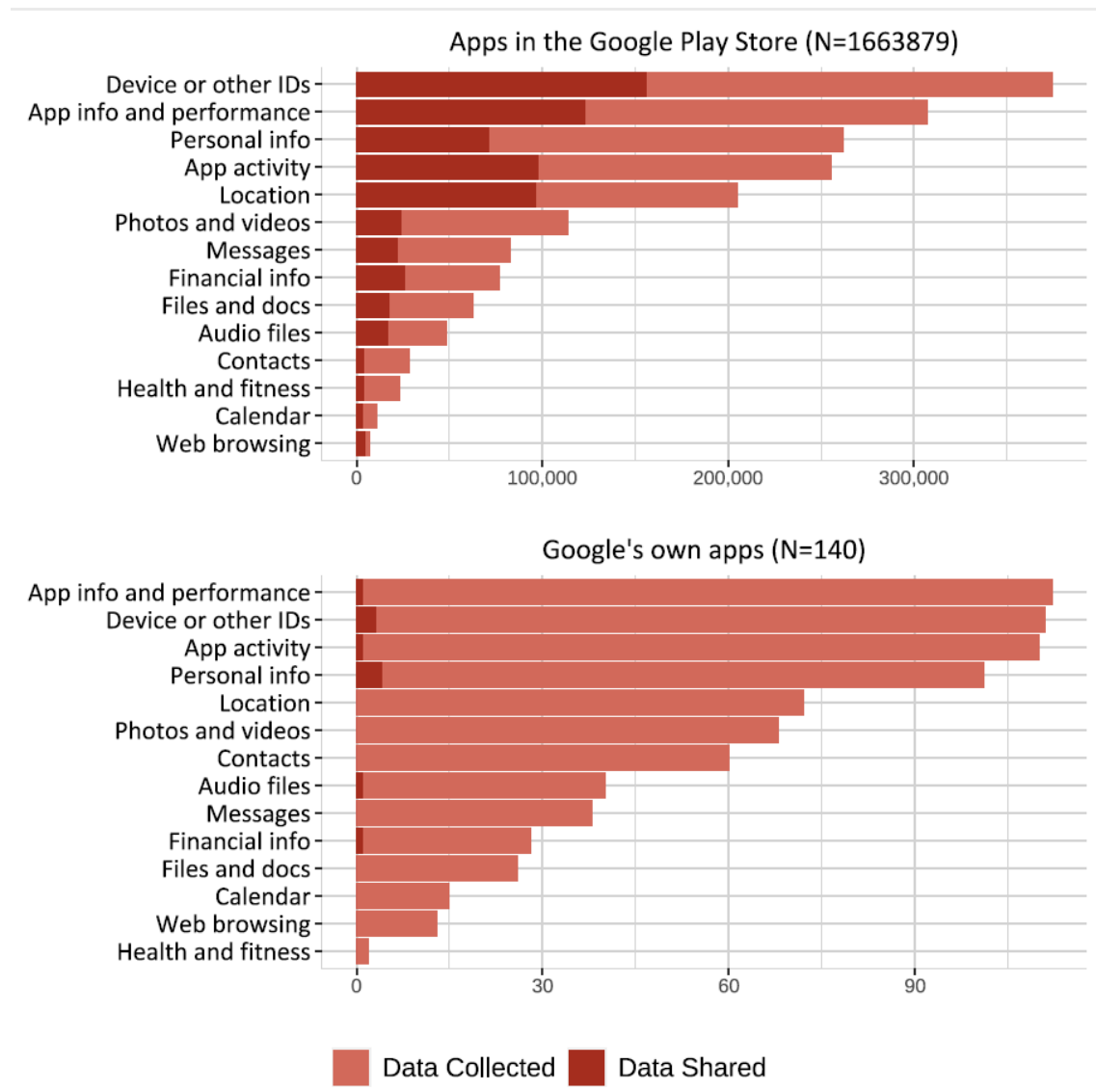


Figure B4: Observations by data category (Google Play Store). The figure presents the data categories and data types of apps in the Google Play Store (N=1,663,879), observations are from December 2022, Dutch geolocation.

Published by



ALEXANDER VON HUMBOLDT
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with



CREATE



centre
internet
et
société



UOC R&I
IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya



UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies