

Article

Mobile App Privacy Disclosures on Google Play in the Post-GDPR Context: A Large-Scale Analysis of Data Safety Section and Permissions

Gerasimos S. Magoulas *  and Spyros E. Polykalas

Department of Digital Media and Communication, Ionian University, 28100 Kefalonia, Greece;
s.polykalas@ionio.gr

* Correspondence: gmagoulas@ionio.gr

Abstract

Mobile apps are essential for communication, transactions and leisure and frequently rely on access to personal data. This study examines Google Play's Data Safety section and declared permissions five years after the GDPR came into force, focusing on how developers disclose data collection, sharing, security practices and deletion controls. We use metadata from 49,578 Android apps and analyze self-reported disclosures in relation to permission categories, app categories, installs and user ratings. The results show that free apps request broader permission access than paid ones and that declared permission use has gradually increased over time. In addition, 25.44% of the sampled apps had not completed any part of the Data Safety section and non-completion was associated with app age, installation band and pricing model. Among apps with completed relevant Data Safety section disclosures, 11% of developers explicitly declared that data are not encrypted in transit and 34% explicitly declared that no user-initiated data deletion mechanism is available. Category-level differences in declared data collection and sharing were modest, while the relationship between permission breadth and user ratings was small. Overall, the findings indicate that structured disclosure mechanisms can improve visibility of privacy-related information, but do not necessarily ensure its completeness or consistency.

Keywords: Google Play store; mobile apps; app permissions; data safety; GDPR; privacy by design; right to erasure; encryption; platform governance; compliance auditing

1. Introduction

Mobile phones have become an essential tool in our daily lives that serve not only for communication and leisure but also for accomplishing various daily tasks. They play an important role in authenticating and authorizing our interactions with government agencies and financial institutions through applications. This use of mobile phones and apps involves the exchange of personal data, often as a necessary part of completing transactions. As a result, concerns arise regarding the security of these data exchanges and whether apps follow data protection requirements. Previous studies have shown that many mobile applications do not meet the transparency and security standards expected under data protection frameworks, with common issues including incomplete privacy policies, insecure data transmission and unauthorized third-party tracking [1,2]. In addition, questions arise regarding whether the personal data requested by an application are relevant to its scope and whether such data are used as described in the application's privacy policy.



Academic Editor: Xinming Zhang

Received: 1 February 2026

Revised: 29 March 2026

Accepted: 31 March 2026

Published: 2 April 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

The substantial exchange of personal data between EU citizens and organizations, whether in electronic or traditional transactions, became a significant concern for the European Union. Existing data privacy guidelines were insufficient to address the evolving needs of citizens and EU member states had not uniformly implemented these guidelines in their national legislations. This fact forced the EU to introduce the General Data Protection Regulation (GDPR) in 2016, a regulation whose main aim was to protect EU citizens from the indiscriminate collection and use of their personal data. The regulation came into effect in 2018 to face these challenges.

According to the GDPR, the data controller is required to inform data subjects about the reasons for collecting personal data, the duration for which data will be collected, the intended processing activities and whether personal data will be transferred to third countries outside of the EU. The developers and owners of mobile applications, whether they are the same or different entities, may act as data controllers. Application users are data subjects. Developers are expected to provide a privacy policy describing the scope of personal data collection and the types of personal data collected. Data collection should also comply with the principle of data minimization [3], which requires that only personal data strictly necessary for an app's purpose be collected. Failure to comply with these obligations may result in significant fines.

Even though the GDPR dictates legal obligations, its practical implementation within mobile app ecosystems relies highly on mechanisms based on disclosures reported by the developers. Mobile app stores operate as mediators and require developers to provide privacy policies, declare requested permissions and complete structured privacy disclosures. In 2022, Google Play implemented the Data Safety section, establishing a structured disclosure mechanism for reporting data collection, data sharing and security practices. In this study, the term Data Safety section disclosures refers to the specific developer-reported statements contained within that section. These disclosures are designed to inform users and support regulatory review. They are reported by the developers and they are not systematically verified.

As described in the following literature review, there is a lot of research that examines mobile app privacy practices using permissions, privacy policies and static or dynamic analysis. These studies consistently document persistent data collection, extensive permission use and gaps between stated policies and observed behavior. However, much of this work focuses either on technical behavior or on legal text analysis, often using either small or specific domain samples. On the other hand, less is known about how large-scale developer-reported disclosures in the Google Play Data Safety section relate to declared permissions, app characteristics and disclosure non-completion several years after the GDPR entered into force.

This study addresses that gap by providing a large-scale empirical analysis of privacy-related disclosures in the Google Play ecosystem. Using metadata from 49,578 popular Android applications collected in 2023, we examine developers' declared permissions, Data Safety section disclosures on data collection and sharing, reported security-related practices and Data Safety section non-completion. Rather than assessing GDPR compliance per se or auditing actual app behavior, this study analyzes developer-reported permissions and Data Safety section disclosures as indicators of how privacy-related practices are presented within the Google Play ecosystem.

Specifically, we investigate how declared privacy practices vary across app categories, pricing models (free versus paid) and popularity indicators (installs, ratings). We further examine whether market-related indicators, such as user ratings and install counts, are associated with permission breadth or declared data practices. Finally, we assess declared

data collection and sharing across app categories to identify those with higher reported data activity that may need closer examination.

This study examines disclosure practices within the Google Play ecosystem several years after the introduction of the GDPR, rather than the causal effects or regulatory efficacy of the GDPR itself. It provides empirical evidence on platform-mediated disclosure practices and highlights some limitations of disclosure-based transparency mechanisms. The findings may be useful as a large-scale descriptive reference for researchers, regulators and platform operators seeking to better understand how privacy-related information is presented within Google Play.

2. Literature Review

Privacy and data protection practices in mobile applications have been the subject of extensive empirical research over the past decade. One part of this research has examined mobile apps through the analysis of requested permissions, tracking mechanisms and app metadata, showing that applications often request broad access to device resources and personal data. In particular, studies based on Google Play metadata [4–7] show that permission use varies systematically across app categories and pricing models. It seems that free applications typically request more permissions than paid ones, reflecting monetization strategies that rely on advertising and services based on data. Importantly, these patterns appear persistent over time. Large-scale analyses conducted before and after the introduction of the GDPR report little evidence of a sustained reduction in permission use, while related work on SDK usage also suggests that regulatory intervention has not fundamentally transformed data-related practices in Android app ecosystems [7–9].

In parallel, a growing body of literature has evaluated mobile app ecosystems from the perspective of GDPR compliance, often focusing on privacy policies as the primary site of regulatory disclosure. These studies consistently identify substantial shortcomings, including missing mandatory information, undefined data retention periods and incomplete descriptions of data processing activities [10–12]. Automated analyses of large numbers of apps show that many privacy policies do not fully comply with GDPR requirements, even when they explicitly claim to follow the Regulation. Additional work has examined specific regulatory obligations, such as data transfers outside the EU [13], consent mechanisms [14] and data retention practices [12], supporting the conclusion that formal compliance is inconsistent and difficult to enforce. More recent research has also explored automated approaches to compliance detection, further illustrating the difficulty of relying on formal disclosures alone as indicators of actual data practices [15]. This literature suggests that disclosure-based compliance mechanisms often function more as formal signals than as reliable indicators of actual data-handling practices, raising questions about their effectiveness.

Although these studies provide valuable insight into legal texts and technical behavior, they often treat disclosure and compliance as equivalent. Privacy governance in mobile app ecosystems increasingly operates through platform disclosure infrastructures which formulate how developers prove data practices to users and regulators. In response to regulatory pressure, major app platforms have introduced standardized privacy labels intended to improve transparency and comparability. Empirical research on these labels, including Apple's App Privacy Labels and Google Play's Data Safety section, reveals widespread inconsistencies across platforms and frequent mismatches between reported disclosures by developers and observed app behavior [16,17]. Recent studies focusing specifically on Google Play's Data Safety section demonstrate that disclosures reported by developers often diverge from technical data flows, which highlights the limitations of developer-reporting without systematic verification [18].

At the same time, there is evidence that disclosure transparency has limited influence on user behavior. Several studies report weak or non-existent relationships between privacy indicators and app popularity metrics such as installs, ratings or reviews [4–6]. These findings raise questions about the effectiveness of market dynamics in encouraging privacy-conscious design and suggest that user choice alone may be insufficient to discipline data-intensive practices.

Platforms such as app stores increasingly function as regulatory mediators, translating legal expectations into private governance mechanisms, including disclosure requirements, review processes and enforcement tools [19–21]. Research in this area shows that these arrangements are shaped by public regulation, while practical oversight and enforcement remain uneven across platforms and over time [22–25]. From this perspective, disclosure governance has been criticized for placing responsibility on users and regulators while providing limited assurance about actual practices, particularly where verification mechanisms are weak or absent.

Despite this growing body of research, less is known about how large-scale developer-reported disclosures in the Google Play Data Safety section relate to declared permissions, app characteristics and disclosure non-completion several years after the GDPR entered into force. Existing studies tend to focus either on technical behavior, legal documentation, or specific compliance obligations. They pay less attention to the Google Play disclosure interface itself as a platform-mediated mechanism of privacy communication. This study addresses the gap by analyzing developers' declared permissions, Google Play Data Safety section disclosures, reported security-related practices and Data Safety section non-completion across 49,578 Android applications. Rather than assessing GDPR compliance per se or auditing app behavior directly, it examines how privacy-related practices are presented through platform-mediated disclosures. In this way, the study contributes a broader platform-level view of disclosure practices in Google Play, including temporal permission trends, category-level disclosure associations and the structurally important issue of non-participation in the disclosure mechanism itself.

3. Analysis

Our research was conducted in May 2023, five years since the implementation of the GDPR. We focused on the Android ecosystem and specifically on the Google Play repository, as it was the largest mobile app platform during the period of our survey [26]. The data collected from Google Play included app name, rating, number of ratings and reviews, number of downloads, version, in-app purchases, last updated date, minimum Android version required, price and the permissions requested during installation.

In April 2022, Google Play introduced a new Data Safety section. This section consists of disclosures provided by developers and contains the app's data collection, sharing and security practices. We gathered all available information from this Data Safety section as part of our research.

Our research collected data from Google Play repository for applications across all categories. The primary criterion for selecting these apps was their inclusion among the most popular apps in the Free, Paid and Grossing lists using the relevant tags used by the store. Many apps appeared in multiple top lists, such as Top Grossing and Top Free or Top Grossing and Top Paid, because an app's revenue can derive either from its purchase price or from in-app purchases.

Initially, we collected data for 65,747 apps. After filtering out duplicates, we retained data and metrics from 49,578 distinct applications. During the research period, the Google Play apps' main categories were Applications and Games. The distribution across these

categories was 66% Applications and 34% Games. The download of this data was done by a terminal located in a European country so we may further analyze the GDPR requirements.

Each category is further divided into subcategories. The subcategories of Applications include Art & Design, Auto & Vehicles, Beauty, Books & Reference, Business, Comics, Communication, Dating, Education, Entertainment, Events, Finance, Food & Drink, Health & Fitness, House & Home, Libraries & Demo, Lifestyle, Maps & Navigation, Medical, Music & Audio, News & Magazines, Parenting, Personalization, Photography, Productivity, Shopping, Social, Sports, Tools, Travel & Local, Video Players & Editors and Weather. The subcategories of Games include Action, Adventure, Arcade, Board, Card, Casino, Casual, Educational, Music, Puzzle, Racing, Role Playing, Simulation, Sports, Strategy, Trivia and Word.

The mobile app distribution per subcategory fluctuates between 1.0% and 3.67% of the total apps, as depicted in Figure 1.

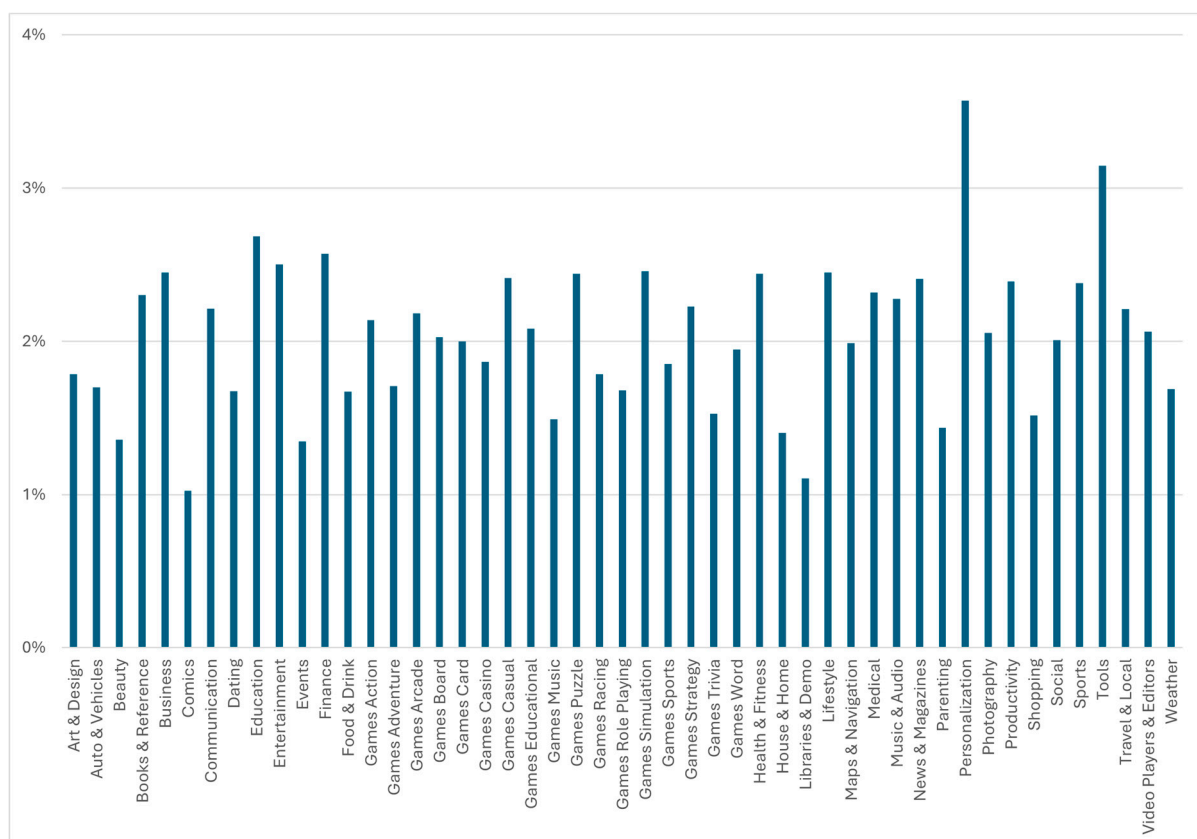


Figure 1. Mobile app distribution per subcategory.

The main criterion for downloading these apps is that they are the most popular apps of the Free, Paid and Grossing categories and the distribution per these categories is shown in Figure 2. These apps have a Top Free, Top Paid and Top Grossing tag. In the Top Grossing category (25,345 apps) 83.65% are free apps and the rest (16.35%) are paid apps, which means that the number of free apps giving profits is greater than the relevant top-grossing paid apps.

As mentioned above, Top Grossing apps may be either free or paid. The overall distribution by pricing model is depicted in Figure 3, where 13% of the apps are paid and 87% are free. This confirms that the biggest percentage of the most popular 49,578 applications are free applications rather than the paid ones.

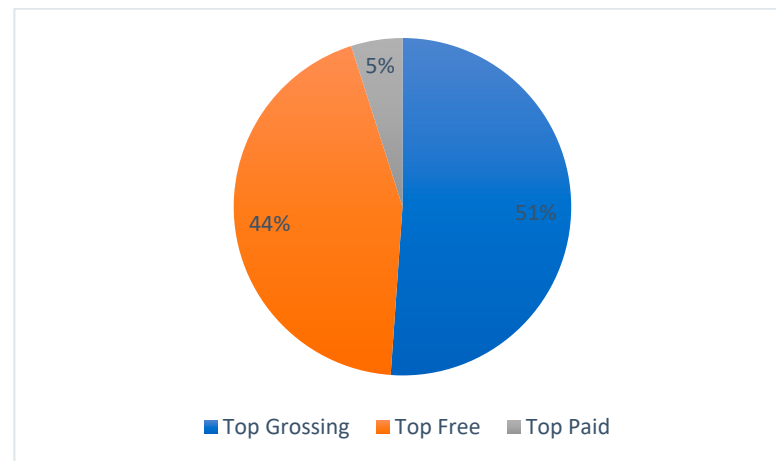


Figure 2. Most popular mobile app distribution per tag: Grossing, Paid, Free.

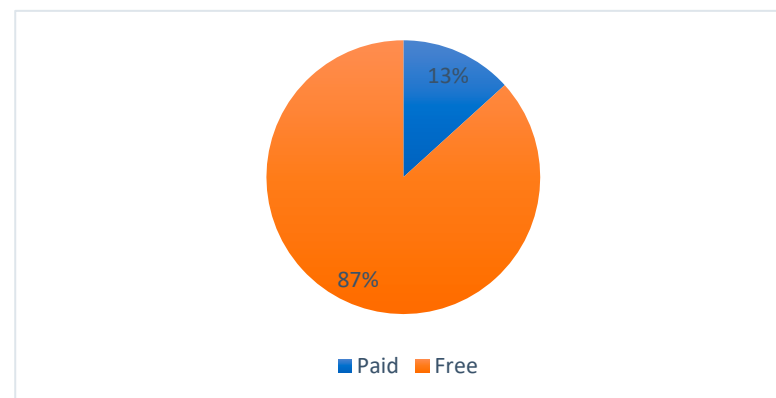


Figure 3. Most popular mobile apps distribution per tag: Free, Paid.

Under the GDPR, apps are expected to provide a privacy policy describing the purpose of personal data collection, retention periods, categories of personal data processed, data sharing practices and data subject rights. In our dataset, 1080 apps (2% of the sample) did not provide a link to a privacy policy.

This represents an improvement relative to earlier periods, as most apps in the research period provide a link to a privacy policy. Even if there was a link to the privacy policy we did not verify whether the links are functional or if the privacy policies include all the mandatory information required by the GDPR. We then analyzed apps without a privacy policy based on their last update. We concluded that almost 30% of these apps were last updated before the GDPR took effect (in May 2018) from 2011 to April 2018. This fact can explain why these apps do not have a privacy policy since it was not compulsory before the GDPR took effect. The remaining 70% were apps that have been updated after the GDPR took effect, which is May 2018, and still did not provide a privacy policy. We should note that no mobile applications updated in 2023 (0%) were found to lack a privacy policy, indicating that apps without a privacy policy were not updated in 2023.

In addition, we examined the distribution of mobile apps with and without a privacy policy per number of installations. Approximately 65% of apps without a privacy policy had been downloaded more than 10,000 times, suggesting that the absence of a privacy policy is not strongly associated with lower installation counts.

In the case of apps without a privacy policy, only 1% were free and the remaining 99% were paid. Despite being paid applications, these apps did not provide a privacy policy link in the Google Play listing.

3.1. Permissions

Google Play apps request permissions from users to operate fully. These permissions allow mobile apps to access personal data or specific device features, such as the camera.

During installation or use, applications may access various device components and personal data. Developers specify requested device features and data access through permissions, which are described in the app listing and, in many cases, in the associated privacy policy. Google Play organizes permissions into categories based on the resources and personal data they involve.

Our study documents the permission categories requested by the analyzed applications, including Photos/Media/Files, Location, Storage, Camera, WiFi Connection Information, Contacts, Identity, Phone, Microphone, Calendar, Device & App History, Wearable Sensors/Activity Data, Device ID & Call Information and Other. Each permission category includes one or more individual permissions; for example, the Photos/Media/Files category includes permissions such as “read the contents of your USB storage”, “modify or delete the contents of your USB storage” and “access USB storage filesystem”.

Permission categories consist of one or more permissions that may either involve access to personal data or interaction with device components that do not necessarily involve personal data, such as the flashlight. In our dataset, the applications counted in each permission category represent apps that request at least one permission from that category. Each app is counted only once per category, even if it requests multiple permissions within the same category.

The distribution of apps per permission category is depicted in Figure 4.

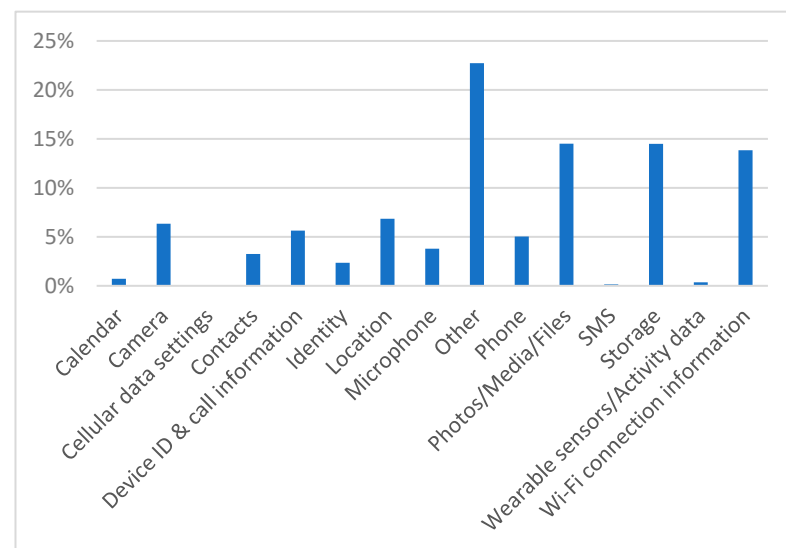


Figure 4. Mobile app distribution per permission category.

From this distribution, the permission categories Other, Photos/Media Files, Storage and WiFi Connection Information are the most frequently requested, followed by Camera and Location. These results align closely with findings reported in earlier studies [5,6] conducted prior to the GDPR implementation, where the most commonly requested permission categories included Other, Photos/Media Files and WiFi Connection Information.

Another relevant aspect concerns the number of permission categories requested per app. The distribution of mobile apps by number of permission categories is shown in Figure 5.

Most apps (16%) request permissions from four categories, while apps requesting one, two, three, five or six categories each account for approximately 10% of the sample.

A similar distribution was reported by [6], where most apps requested permissions from four categories and the remaining apps were relatively evenly distributed across other permission counts.

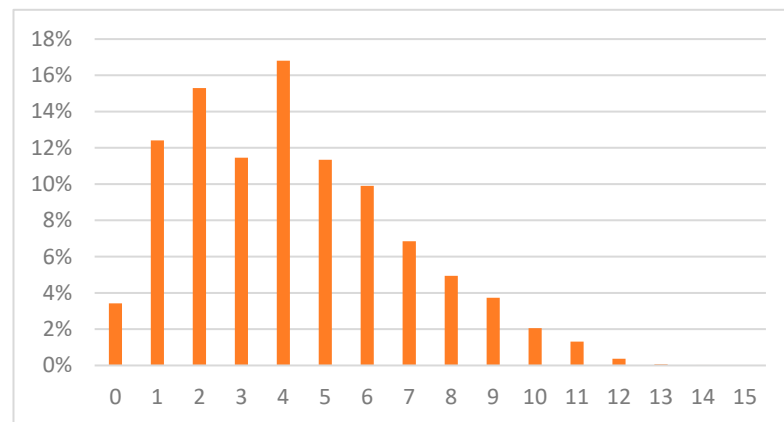


Figure 5. Mobile app distribution per number of permission categories.

These findings suggest that permission usage patterns observed in the post-GDPR period closely resemble those reported in pre-GDPR studies [5,6]. Rather than indicating regulatory outcomes directly, this continuity highlights the persistence of established permission practices within the mobile app ecosystem.

An examination of permissions by pricing model shows that paid apps tend to request fewer permission categories than free apps, as shown in Figure 6. This pattern is consistent with earlier findings reported by [5], which associate free app models with more extensive data access. The persistence of this pattern suggests that business models remain an important factor shaping declared permission use, particularly in apps based on data usage and ads.

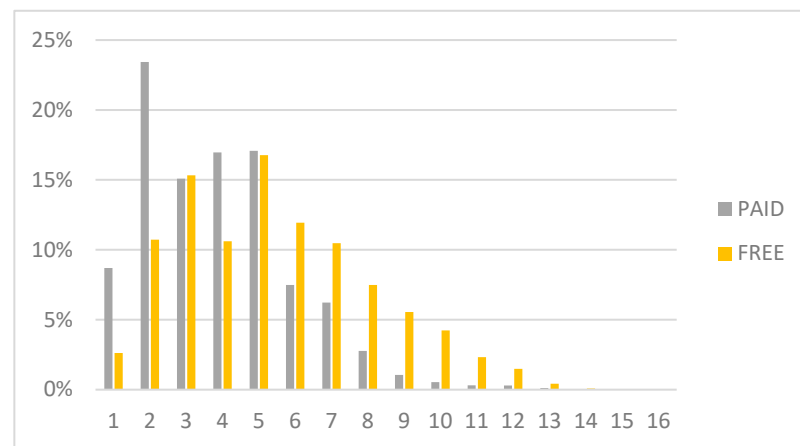


Figure 6. Mobile app distribution per number of permission categories for free and paid criteria.

It is informative to examine the average number of permission categories requested by app subcategories. This distribution is depicted in Figure 7.

The app subcategories that request the highest average number of requested permission categories are Social (approximately seven), Communication (six), Dating (six), Business (six) and Shopping (six). This pattern is consistent with the functional characteristics of these subcategories, which commonly involve communication, interaction or transaction-related features that require access to multiple device resources and data types.

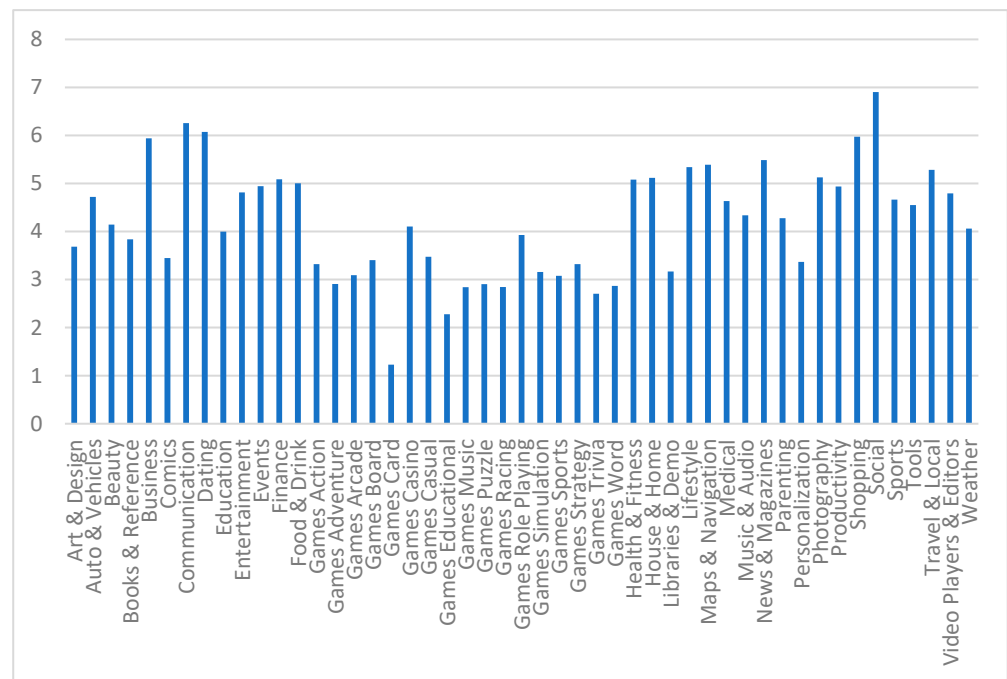


Figure 7. Average number of permission categories per app subcategories.

Finally, we conducted a correlation analysis (Table 1) between the number of installs (Ninstalls), number of reviews (Nreviews), number of ratings (Nratings), rating score (Ratingscore) and the number of permission categories (NPermissions). The analysis indicates no strong bivariate association between the number of permission categories and the other popularity-related metrics. In contrast, a strong correlation is observed between the number of reviews and the number of ratings (correlation coefficient = 0.80), which is expected, as users who submit reviews typically also provide ratings.

Table 1. Correlation matrix.

	Ninstalls	RatingScore	Nratings	Nreviews	Npermissions
Ninstalls	1				
RatingScore	0.046688	1			
Nratings	0.472626	0.032176	1		
Nreviews	0.411188	0.047639	0.047639	1	
				0.79903	1

In addition, moderate correlations are observed between the number of installs and the number of reviews (correlation coefficient = 0.41), as well as between the number of installs and the number of ratings (correlation coefficient = 0.47). Even if the bivariate correlation between rating score and the number of permission categories is weak, this result should be interpreted carefully given the large sample size.

To further examine the relationship between permission use and user evaluations after accounting for potential confounding factors, we estimated a multivariate linear regression model with the rating score as the dependent variable. The model was specified as follows:

$$Rating\ Score_i = \beta_0 + \beta_1 NPermissions_i + \beta_2 Free_i + \beta_3 AppAge_i + \sum_{k=1}^{K-1} \gamma_k Category_{ik} + \varepsilon_i$$

where

$Rating\ Score_i$: the average user rating of application i .

$NPermissions_i$: the number of permission categories declared by the app.

$Free_i$: a binary variable if the app is free (1) or paid (0).

$AppAge_i$: year of data collection minus the year of last update.

$Category_{ik}$: the app category used as a categorical predictor using dummy-variable encoding based on Google Play categories, with Art & Design used as the reference category.

The model was estimated using ordinary least squares (OLS). Categorical variables were encoded as binary indicators. Essential regression assumptions were assessed. Multicollinearity was examined using generalized variance inflation factors (GVIF). All adjusted GVIF values of predictors ranged between 1.00 and 1.14, indicating no evidence of problematic multicollinearity among the predictors.

Heteroskedasticity was assessed using the Breusch–Pagan test, which was statistically significant ($BP = 5741.2, p < 0.001$), indicating non-constant error variance. We therefore report heteroskedasticity-robust (HC3) standard errors as a robustness check and the key results remained unchanged. Since the sample size is large, results are interpreted with emphasis on coefficient magnitude and confidence intervals rather than statistical significance alone.

Although the dependent variable (rating score) is bounded between 1 and 5, OLS was selected because the variable is observed at many intermediate values as an average user score. In this context, OLS provides an interpretable estimate of average associations. This makes it suitable for the study's descriptive purpose, which is to assess the direction and substantive size of relationships. The results should therefore be interpreted as descriptive associations rather than causal effects or exact marginal changes.

The number of permission categories exhibited a statistically significant but substantively small association with the rating score in the fully adjusted model that controls for app category, free/paid status, and app age ($\beta = 0.043$, 95% CI [0.038, 0.048]). Based on the 1–5 rating scale, this effect corresponds to a marginal change in user ratings even for substantial increases in permission requests.

To examine whether permission-category breadth is better interpreted as a proxy for feature richness or application complexity rather than user tolerance of data access, we estimated nested models. First, we estimated a bivariate model with the rating score regressed only on permission-category breadth (Model 0). Next, we added category fixed effects to account for systematic differences across app types (Model 1). Finally, we estimated the fully adjusted model that additionally includes free/paid status and app age (Model 2). The coefficient for permission-category breadth changes across these specifications was $\beta = 0.038$ in Model 0, $\beta = 0.066$ in Model 1, and $\beta = 0.043$ in Model 2. This sensitivity to the inclusion of category and controls suggests that app type and related characteristics explain part of the observed association. Therefore, the positive coefficient should not be interpreted as evidence that users reward broader data access or that users are indifferent to privacy. A more plausible interpretation is that apps with richer functionality tend to require access to more device resources and may also receive higher ratings because users value their utility.

Another perspective is to examine whether the average number of permission categories varies over time based on the last update date of each app. For this purpose, we used the year of the last update and calculated the average number of permission categories for all apps updated in each year. The yearly averages were used to carry out a descriptive trend analysis, the results of which are shown in Figure 8.

Figure 8 presents the average number of permission categories for apps by year of last update from 2011 to 2023 including 95% confidence intervals and a fitted linear trend. The equation of the trend line is $y = 0.2384x + 1.4492$ and the R^2 value is 0.83. This trend is based on yearly averages rather than panel data of individual apps so the high R^2 reflects aggregate smoothing and should be interpreted as a descriptive indication of

overall direction rather than as evidence of a causal relationship. Confidence intervals were wider in earlier years, reflecting smaller sample sizes and greater heterogeneity among apps updated in the early stages of the platform.

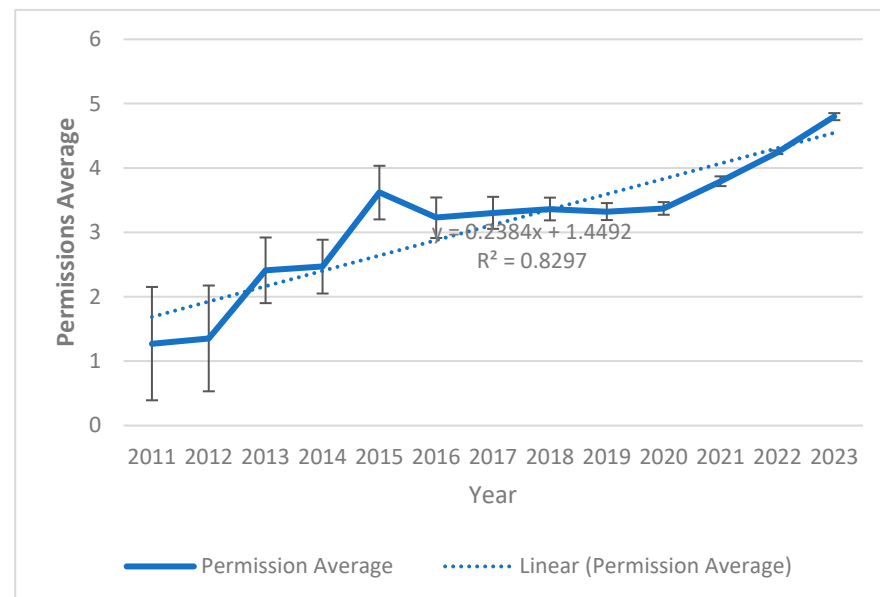


Figure 8. Average number of permission categories of apps updated per year with 95% confidence intervals. The dashed line shows a linear fit to aggregate yearly means.

In the linear model, y represents the average number of permission categories and x represents the year. The slope of 0.2384 indicates an average increase of approximately 0.24 permission categories per year. While the confidence intervals indicate that year-to-year changes are modest, the positive slope reflects an ongoing rise in declared permission use, suggesting that permission breadth did not decrease in this sample over the period examined.

3.2. Data Safety Section

In April 2022, Google Play introduced a new Data Safety section, in which developers provide self-reported disclosures regarding an app's data collection, data sharing and security practices. Analyzing this section is central to our study, as it offers insight into how developers represent their data practices and security measures through disclosures presented in the platforms. We collected all available information from the Data Safety section as part of our analysis.

The Data Safety section is organized into three parts: Data Shared, which covers data that may be shared with external companies or organizations; Data Collected, which outlines data the app may gather; and Security Practices, which describe declared measures related to secure communication and data protection.

The Data Shared and Data Collected sections refer to the following data categories: Location, Personal Information, Financial Information, Health and Fitness, Messages, Photos and Videos, Audio Files, Files and Documents, Calendar, Contacts, App Activity, Web Browsing, App Information and Performance and Device or Other IDs. The Security Practices section includes disclosures on whether developers commit to the Play Families Policy, whether data are encrypted in transit, whether data are not encrypted, whether an independent security review has been conducted, whether data can be deleted and whether users can request data deletion.

Of all the apps there were 12,614 apps (25.44%) that had not completed any of the three Data Safety sections (Data Shared, Data Collected or Security Practices). This is likely related to the introduction of the Data Safety section in April 2022 because approximately 23% of the apps in the dataset had not been updated after this date at the time of data collection.

The remaining 36,964 apps (74.56%) with at least one completed Data Safety section were included in the subsequent analysis. The declared data collection and data sharing categories, as well as the frequency with which data are reported as collected or shared, are presented in Table 2.

Table 2. Data Collected and Shared categories.

Data Collected/Shared Categories	Data Collected/Shared
Location	Approximate location Precise location
Personal info	Name Email address User IDs Address Phone number Race and ethnicity Political or religious beliefs Sexual orientation Other info
Financial info	User payment info Purchase history Credit score Other financial info
Health and fitness	Health info Fitness info
Messages	Emails SMS or MMS Other in-app messages
Photos and videos	Photos Videos
Audio files	Voice or sound recordings Music files Other audio files
Files and docs	Files and docs
Calendar	Calendar events
Contacts	Contacts
App activity	App interactions In-app search history Other user-generated content Other actions
Web browsing	Web browsing history
App info and performance	Crash logs Diagnostics Other app performance data
Device or other IDs	Device or other IDs

We examined the distribution of the mobile apps per Data Collected and Data Shared categories in Figure 9.

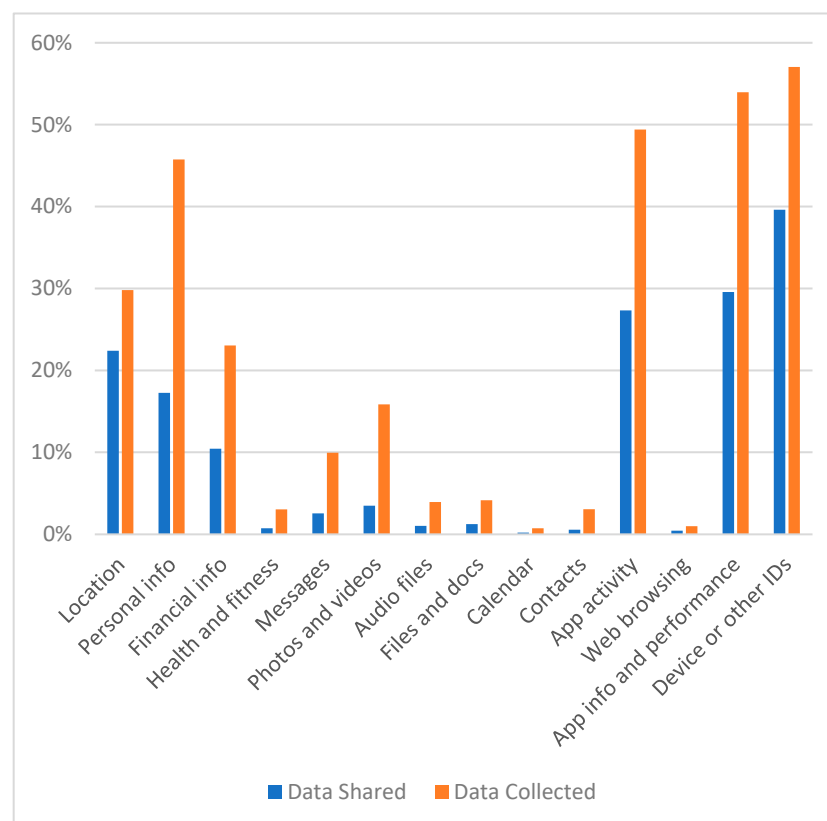


Figure 9. Mobile app distribution per Data Shared/Collected categories.

A general observation from the Data Safety section disclosures is that not all data declared as collected are also declared as shared with third parties. The most frequently declared data categories as collected are Device or Other IDs, App Information and Performance, and App Activity, followed by Personal Information and Location. These categories also appear most frequently among data declared as shared.

It is therefore useful to examine more closely data categories that are potentially identifying, such as Personal Information, as well as other categories that may reveal sensitive or contextual information about users, including Location, Messages, Photos and Videos, Audio Files and Files and Documents.

The Personal Information category includes data types such as name, email address, user identifiers, address, phone number, race or ethnicity, political or religious beliefs, sexual orientation and other personal details. The distribution of mobile apps by declared data collection and data sharing for these personal data categories is shown in Figure 10.

Within the Personal Information data category, the most frequently declared data types collected are address, email address, user IDs, name and phone number. These data types are commonly associated with account management, communication and service provision within mobile applications.

Figure 11 further examines declared data collection and sharing for additional data categories, including Location (L), Messages (M), Photos and Videos (P), Audio Files (A) and Files and Documents (F), which are generally regarded as more sensitive forms of personal data.

The personal data categories most frequently reported as both collected and shared are Approximate Location, Photos, Videos and Precise Location. These data categories

are commonly associated with a wide range of app functionalities across communication, content sharing and location-based services.

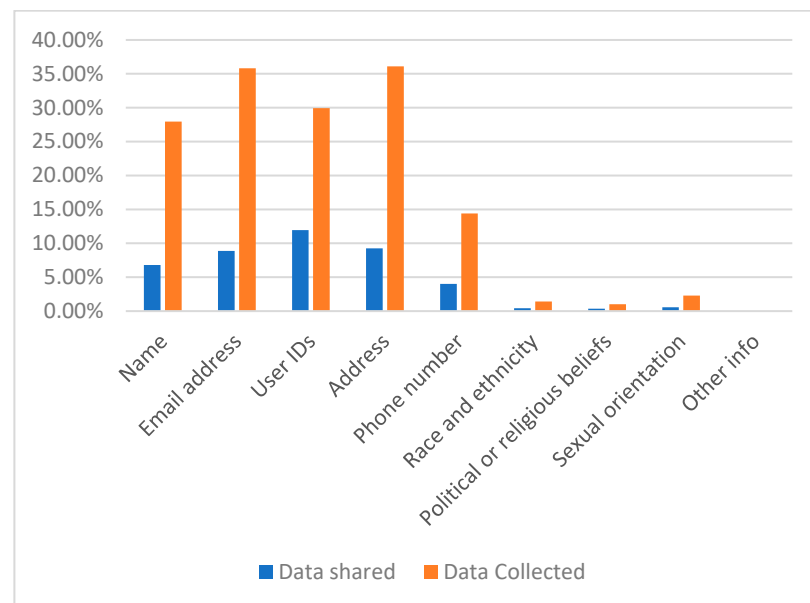


Figure 10. Mobile app distribution per Data Shared/Collected categories for data in Personal Info.

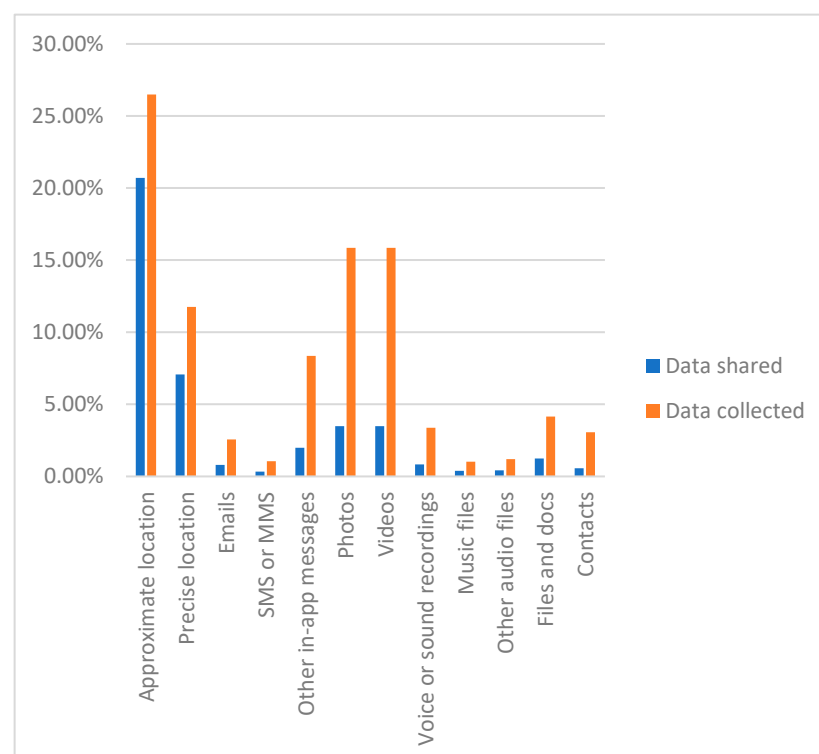


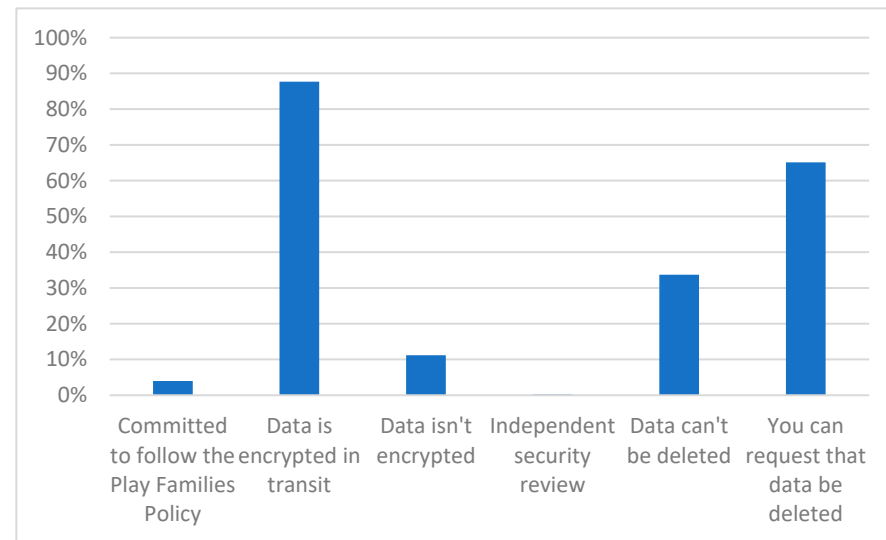
Figure 11. Mobile app distribution per Data Shared/Collected categories for data in (L), (M), (P), (A), (F).

The third component of the Data Safety section concerns security practices. Developers are asked to declare whether specific security-related measures are implemented, as summarized in Table 3.

The distribution of mobile apps per security practices followed by the developers is shown in Figure 12.

Table 3. Security Practices mentioned in Data Safety.

Security Practices
Committed to follow the Play Families Policy
Data isn't encrypted
Independent security review
Data can't be deleted
You can request that data be deleted

**Figure 12.** Mobile app distribution per security practices.

Approximately 11% of the apps that completed at least one section of the Data Safety section disclosures explicitly declared that data are not encrypted in transit and 34% explicitly declared that no user-initiated data deletion mechanism is available. These declared practices indicate uneven adoption of security and user-control measures within platform-mediated privacy disclosures. However, these variables reflect explicit negative declarations in the Google Play Data Safety form rather than independently verified technical properties of the apps. Additionally, 4% of apps positively report a commitment to following the Play Families Policy and the remaining apps either did not complete this field or reported that the policy does not apply.

These findings indicate limitations in how privacy-related practices are presented through developer-reported disclosures in large app ecosystems. They suggest that additional verification and greater consistency may improve the reliability of platform-based disclosure mechanisms.

The analysis was extended to examine which applications in the dataset did not complete the Data Safety section disclosure. Specifically, we investigated whether non-completion was associated with app category, number of installations, pricing model or app age. To assess these relationships, we estimated a binary logistic regression model in which Data Safety non-completion served as the dependent variable. The model was specified as follows:

$$\begin{aligned}
 \log\left(\frac{P(\text{NonCompletion}_i = 1)}{1 - P(\text{NonCompletion}_i = 1)}\right) \\
 = \alpha + \sum_{m=1}^{M-1} \beta_m \text{InstallBand}_{im} + \beta_F \text{Free}_i \\
 + \sum_{a=1}^{A-1} \delta_a \text{AppAgeGroup}_{ia} + \sum_{k=1}^{K-1} \gamma_k \text{Category}_{ik}
 \end{aligned}$$

where

NonCompletion_i: whether the app did not complete any section of the Data Safety section (1 = no completed Data Safety section, 0 = at least one completed section).

InstallBand_{im}: the app's installation range (<1K, 100K–1M, 10K–100K, 10M+, 1K–10K, 1M–10M).

Free_i: a binary variable indicating whether the app is free (1 = free, 0 = paid).

AppAgeGroup_{ia}: grouped app age.

Category_{ik}: app category included as a categorical predictor using dummy-variable encoding based on Google Play categories.

App age was operationalized as the difference between the data collection year (2023) and the year of the app's last update and was entered into the model as four categories: 0–1 years, 2–3 years, 4–5 years and 6+ years.

Categorical predictors were entered using dummy-variable encoding, with Tools as the reference category for app category, 10M+ installs as the reference category for installation band, Paid as the reference category for pricing model and 0–1 years as the reference category for app age.

The results showed that non-completion was clearly associated with both installation scale and app age. Using apps in the highest installation band (10M+ installs) as the reference category, apps with fewer installations were significantly more likely not to complete the Data Safety section. The odds ratios ranged from 1.63 (95% CI [1.44, 1.84], $p < 0.001$) for apps with 1M–10M installs to 7.06 (95% CI [6.07, 8.21], $p < 0.001$) for apps with fewer than 1K installs.

App age also emerged as a strong predictor. Apps aged 2–3 years in comparison with apps aged 0–1 years, had 11.09 times higher odds of non-completion (95% CI [10.37, 11.85], $p < 0.001$), apps aged 4–5 years had 18.09 times higher odds (95% CI [15.85, 20.64], $p < 0.001$) and apps aged 6 years or more had 20.71 times higher odds (95% CI [16.79, 25.53], $p < 0.001$).

In addition, free apps were less likely than paid apps to have an incomplete Data Safety section (OR = 0.24, 95% CI [0.22, 0.27], $p < 0.001$). These findings suggest that missing Data Safety disclosures were not randomly distributed across the sample. They were concentrated among older apps and apps with lower installation counts.

A correlation analysis between permission categories and Data Safety section disclosures shows no meaningful association. This divergence reflects the different purposes of these two mechanisms. According to [27], the permissions list specifies the device features and data access technically available to an app, including permissions required for core functionality or requested during use. In contrast, the Data Safety section reflects developer-reported descriptions of data handling practices, which are not derived directly from technical permission specifications.

According to [27], discrepancies between the permissions list and the Data Safety section may arise for several reasons, including data processed locally without collection or sharing, data collected in ways that do not require explicit permissions and permissions that are not covered by the Data Safety section disclosures.

A correlation analysis between general popularity indicators (number of installs, number of reviews and number of ratings) and the Data Safety section disclosure sections shows no meaningful associations. This suggests that disclosure-based privacy information, as presented in the Data Safety section, is not systematically associated with user engagement or download-related metrics.

Following the correlation analysis, we applied a chi-square test of independence to examine whether app categories are associated with the data categories reported as collected or shared in the Data Safety section. The hypotheses tested were:

H_0 : There is no association between app categories and the data categories reported as collected or shared in the Data Safety section.

H_1 : There is an association between app categories and the data categories reported as collected or shared in the Data Safety section.

To conduct the test, we constructed contingency tables with app categories as rows and Data Safety section data categories as columns. Each cell contained the number of apps within a category that reported collecting or sharing the corresponding data category. Separate tables were constructed for data collected and data shared. The chi-square statistics were calculated as:

$$X^2 = \sum \frac{(O - E)^2}{E}$$

where O represents observed values and E represents expected values.

For both the Data Collected and Data Shared tables, the p -values were below 0.05, leading to rejection of the null hypothesis. Given the large sample size, statistical significance was expected, so effect sizes (Cramér's V) were calculated to assess the substantive magnitude of the associations.

$$V = \sqrt{\frac{X^2}{N(k-1)}}$$

where N is the number of apps and k is the minimum of the number of app categories and the number of data categories. For declared data collection, the association was small to moderate ($\chi^2 = 20,621.51$; Cramér's V = 0.18), while for declared data sharing the association was small ($\chi^2 = 7989.11$; Cramér's V = 0.11). These results indicate systematic but modest category-level differences in declared data practices.

To further examine the structure of these associations, standardized residuals were calculated for individual cells of the contingency tables using:

$$\text{Standardized residuals} = \frac{O - E}{\sqrt{E}}$$

where

O: Observed values.

E: Expected values.

Positive residuals greater than +2 indicate category–data combinations occurring more frequently than expected under independence, while negative residuals less than −2 indicate combinations occurring less frequently than expected. Examination of the residuals suggests that deviations from independence are distributed across multiple app categories and data types, consistent with the modest effect sizes observed. Standardized residuals are used here as a diagnostic tool to identify where category-level deviations are concentrated, rather than to conclude in strong or deterministic differences at the individual application level.

Although the overall association between app categories and declared data collection is modest (Cramér's V = 0.21), standardized residuals reveal localized deviations from independence across multiple category–data combinations. For instance, social apps are over-represented in the collection of messaging (12.26) and photos and videos (17.52), while business apps show a higher-than-expected collection of messages (4.77), calendars (10.56) and contacts (12.51). Parenting apps exhibit clear over-representation in health-related data collection (6.21), photos and videos (7.43) and calendar (4.63) reflecting functional specialization. These deviations are dispersed across categories and data types and do not concentrate on a small number of dominant patterns, consistent with the modest overall effect size.

In contrast, data sharing shows a weaker overall association with app categories (Cramér's $V = 0.13$) and standardized residuals reveal localized deviations from independence. For example, Communication apps are over-represented in declared sharing of messaging data (4.23), contacts (7.51) and audio files (11.41), while Finance apps show higher-than-expected sharing of personal (6.84) and financial information (7.03) as well as contacts (10.36). Shopping apps similarly exhibit over-representation for sharing of personal (7.52) and financial information (9.33) and photos and videos (7.68). These deviations are dispersed across multiple categories and data types, aligning with the modest overall effect size.

Statistical testing confirms that category-level differences in privacy disclosures exist, but effect-size analysis shows that these differences are modest and dispersed, highlighting the limits of disclosure-based governance rather than providing user-level guidance.

4. Discussion

This study analyzed a large sample of 49,578 popular Google Play applications. It examined app popularity, pricing, permission requests and the Data Safety section. The Data Safety section contains privacy-related information disclosed by developers. The data were collected five years after the GDPR's introduction. The study does not assess legal compliance. It describes how privacy-related practices are presented through developer disclosures. All findings are based on developer-reported metadata and disclosures, which are not independently verified.

Several consistent patterns emerge from the analysis. First, most popular apps in the dataset are free (87%). Free apps systematically request more permission categories than paid apps. This finding is consistent with earlier work by [5], despite differences in dataset size and time period. It indicates that business models remain associated with declared permission practices. Data access practices are often shaped by an app's design and monetization model, rather than by a single isolated decision.

A slight improvement is that approximately 98% of apps now provide a link to a privacy policy. This indicates adoption of platform-level transparency mechanisms. However, the presence of a link does not imply full alignment with GDPR requirements, which were not assessed in this study.

Permission use remains concentrated in certain app categories. Social, Communication, Dating, Business and Shopping apps consistently request the highest average number of permission categories. Bivariate correlation analysis indicates weak associations between permission breadth and popularity indicators such as installs, ratings and reviews. Multivariate regression analysis further shows that permission breadth has a statistically significant but substantively small association with user ratings after controlling app category, pricing model and app age. To examine whether this association is better interpreted as a proxy for feature richness or application complexity rather than user tolerance of data access, we compared nested model specifications. The coefficient for permission-category breadth changes across these models was $\beta = 0.038$ in the bivariate model, $\beta = 0.066$ with category fixed effects, and $\beta = 0.043$ in the fully adjusted model. This sensitivity to model specification suggests that app type and related characteristics explain part of the association. The positive coefficient should therefore not be interpreted as evidence that users reward broader data access. A more plausible interpretation is that feature-rich apps often require more device resources and may receive higher ratings because users value their utility.

The large sample size required statistical significance to be interpreted together with effect size and substantive magnitude. In large datasets, even very small associations may reach conventional significance thresholds.

Trend analysis based on app update history indicates a gradual increase in the average number of permission categories requested over time. This trend is derived from yearly averages rather than panel data of individual apps. It should be therefore interpreted as a descriptive indication of persistence in permission practices rather than as evidence of regulatory impact.

Analysis of Google Play's Data Safety section disclosures further highlights differences between reported data collection and reported data sharing. Firstly, not all collected data are reported as shared. Secondly, device identifiers, app activity, app performance data, personal information and location are among the most frequently declared categories. Security-related disclosures also indicate uneven reporting of practices such as encryption in transit and user-initiated data deletion. Specifically, the reported percentages correspond to explicit negative developer declarations in the Google Play Data Safety section. They do not reflect independently verified technical properties of the apps. These findings highlight limits in what can be inferred from disclosure-based mechanisms alone. They suggest that additional verification or consistency checks could improve interpretability.

A further important finding is that a substantial share of the sample apps did not complete any part of the Data Safety section. The additional regression analysis showed that non-completion was associated with app age, installation band, pricing model and app category. The strongest association for non-completion was observed for older apps and a lower number of installations. This suggests that participation in the disclosure mechanism itself is uneven across the Google Play ecosystem. It also suggests that missing disclosures are concentrated in specific app segments rather than being randomly distributed.

Finally, chi-square analysis reveals statistically significant but modest associations between app categories and declared data collection and sharing patterns. Cramér's *V* values indicate a small-to-moderate association for data collection and a small association for data sharing. Standardized residuals identify localized app category and data category combinations in which certain data types are declared more often than expected. At the same time, these deviations are dispersed across categories and data types. They are not concentrated on a small number of dominant patterns. These findings suggest structured but limited category-level differentiation. They do not support strong or deterministic structural claims.

This study has several limitations that should be acknowledged. First, the analysis is based exclusively on metadata and developer-reported Data Safety section disclosures retrieved from Google Play. We did not conduct dynamic analysis, static code inspection, network traffic analysis or other technical verification of actual data flows. As a result, the study captures how privacy and security-related practices are presented through platform-mediated disclosures. It does not measure how applications necessarily behave in operation. Second, declared permissions should not be interpreted as a direct proxy for actual runtime behavior. Applications may request permissions without using them in the same way across contexts, versions or user interactions. Third, although the data were collected from a European IP address, this does not imply that all applications in the dataset are necessarily governed by the GDPR in a direct legal sense. Therefore, the findings should not be interpreted as evidence of GDPR applicability or legal compliance. More broadly, no direct conclusions regarding legal compliance can be drawn solely from disclosure patterns, permissions or platform metadata. The results should instead be interpreted as large-scale indicators of disclosure practices within the Google Play ecosystem at the time of data collection.

A further limitation concerns sampling and access context. The dataset was drawn from the Google Play Top Free, Top Paid and Top Grossing lists. It therefore reflects popular applications rather than the full population of Android apps available on Google

Play. As a result, the findings should not be generalized to all Android applications. In addition, we recorded the presence or absence of privacy policy links. We did not verify whether the linked documents were functional, current or substantively compliant with legal requirements.

5. Conclusions

This study provides a large-scale empirical examination of privacy-related disclosures in the Google Play ecosystem five years after the GDPR's implementation. It does not evaluate the causal effectiveness of the GDPR. Instead, it examines how privacy-related practices are presented through platform-mediated disclosures in this later regulatory context. The analysis focuses on how developers present privacy-related information through declared permissions and Data Safety section disclosures at the time of data collection.

The findings show that several structural patterns identified in earlier research remain visible. At the same time, the study contributes a broader platform-level analysis of Data Safety section disclosures, category-level disclosure differentiation, temporal permission trends and Data Safety section non-completion. Free apps tend to request broader access to device resources than paid apps. Permission use also varies across app categories. Popularity indicators such as installs, ratings and reviews show only weak associations with privacy-related disclosures. Multivariate analysis indicates that permission breadth has a statistically detectable but substantively small relationship with user ratings. This suggests that market signals alone may provide limited incentives for reducing permission breadth.

Data Safety section disclosures also reveal uneven reporting of security and user control-related practices, including encryption in transit and user-initiated data deletion. A further important finding is that a substantial share of apps did not complete any part of the Data Safety section. This non-completion was associated with app age, installation band, pricing model and app category. These results indicate that both the content of disclosures and participation in the disclosure mechanism itself vary across the Google Play ecosystem. These patterns indicate the limitations of platform mediated transparency when systematic verification is absent.

Overall, the study contributes empirical evidence on disclosure-based privacy transparency in mobile app platforms. It highlights both the reach and the limitations of current disclosure mechanisms and identifies modest category-level differentiation in permissions and Data Safety section disclosures. The effect sizes are weak to moderate, so the implications are necessarily cautious. The results suggest that limited, targeted verification or consistency checks could improve the interpretability of disclosures. However, this study does not evaluate the effectiveness of specific governance interventions. Future work is needed to test whether such measures lead to measurable improvements.

6. Future Work

This study is limited to a single platform and to a snapshot of Data Safety section disclosures. Future research could extend the analysis to other app ecosystems, such as iOS. It could also examine longitudinal changes in disclosures to assess how platform-based transparency practices evolve over time. Future studies could include a broader range of Google Play applications beyond the Top Free, Top Paid and Top Grossing lists. Further work could also combine disclosure analysis with technical audits, static code inspection or network traffic analysis. This would allow a more direct comparison between developer-reported disclosures and actual data practices.

7. Implications for Platform Governance

The results suggest that Google Play plays an important role in shaping how privacy-related information is presented to users through permissions, Data Safety section disclosures and related transparency features. The observed differences between declared permissions and Data Safety section disclosures, together with uneven reporting of security and user-control-related practices, indicate limitations in the consistency of current disclosure mechanisms. Some developers explicitly declare that data is not encrypted in transit or that no user-initiated data deletion mechanism is available. These self-reported statements identify apps with limited disclosed safeguards and user controls regarding the right to erasure and the security of the transmission of personal data. In such cases the platform could require clearer, standardized explanations when developers select these options and flag such declarations for targeted review or follow-up checks.

In addition, the finding that a substantial share of apps did not complete any part of the Data Safety section suggests that participation in the disclosure mechanism itself remains uneven. Additional verification and consistency checks may therefore improve the reliability of platform-based disclosures. Most relationships are weak to moderate in magnitude (e.g., Cramér's V), so the implications should be read as cautious, aggregate-level indications.

The findings also suggest that automated cross-checks between declared permissions and Data Safety section disclosures may help identify potential inconsistencies on scale. Such checks could be used as exploratory screening tools, particularly in app categories that exhibit higher-than-expected levels of declared data collection or sharing. Likewise, the analysis of Data Safety section non-completion may help identify segments of the marketplace in which disclosure participation is less consistent, especially among older and lower-install apps.

Popularity indicators show only weak associations with privacy-related disclosures. This suggests that transparency mechanisms are unlikely to rely on market signals alone to encourage more complete or consistent reporting. Although the category-level differences identified in this study are modest in magnitude, the analytical approach used to detect higher-than-expected data collection and sharing may still provide a useful basis for exploratory monitoring and more targeted follow-up review in systems that rely on developer disclosures.

This study is descriptive and relies on platform metadata and developer-reported disclosures. Therefore, the governance implications should be interpreted as cautious indications rather than as direct evidence for specific policy interventions.

Author Contributions: Conceptualization, G.S.M. and S.E.P.; methodology, G.S.M.; software, G.S.M.; validation, G.S.M. and S.E.P.; formal analysis, G.S.M.; investigation, G.S.M.; resources, G.S.M.; data curation, G.S.M.; writing—original draft preparation, G.S.M.; writing—review and editing, G.S.M. and S.E.P.; visualization, G.S.M.; supervision, S.E.P.; project administration, G.S.M. and S.E.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The dataset is the snapshot of 49,578 Google apps metadata presented in Google Play store in May 2023 and it is available on request from the authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Fan, M.; Yu, L.; Chen, S.; Zhou, H.; Luo, X.; Li, S.; Liu, Y.; Liu, J.; Liu, T. An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps. In *Proceedings of the 2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*, Coimbra, Portugal; IEEE: New York, NY, USA, 2020; pp. 253–264.
2. Paci, F.; Pizzoli, J.; Zannone, N. A Comprehensive Study on Third-Party User Tracking in Mobile Applications. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023)*, Benevento, Italy; Association for Computing Machinery (ACM): New York, NY, USA, 2023; p. 8.
3. European Parliament & Council of the European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). 2016. Available online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (accessed on 1 May 2023).
4. Rabea, A.; Mutlutürk, M.; Metin, B. Privacy Concerns on Mobile Applications for Google Play Store Market. In *Proceedings of the 2019 11th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, Turkey; IEEE: New York, NY, USA, 2019; pp. 968–972.
5. Polykalas, S.E.; Prezerakos, G.N. When the Mobile App Is Free, the Product Is Your Personal Data. *Digit. Policy Regul. Gov.* **2019**, *21*, 89–101. [\[CrossRef\]](#)
6. Magoulas, G.S.; Polykalas, S.E. Access to Personal Data Is Still Tempting for Mobile Apps Even after the GDPR Implementation. In *Proceedings of the 2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Piraeus, Greece; IEEE: New York, NY, USA, 2023; pp. 1–6.
7. Alkinoon, A.; Dang, T.C.; Alghuried, A.; Alghamdi, A.; Choi, S.; Mohaisen, M.; Wang, A.; Salem, S.; Mohaisen, D. A Comprehensive Analysis of Evolving Permission Usage in Android Apps: Trends, Threats and Ecosystem Insights. *J. Cybersecur. Priv.* **2025**, *5*, 58. [\[CrossRef\]](#)
8. Kollnig, K.; Binns, R.; Van Kleek, M.; Lyngs, U.; Zhao, J.; Tinsman, C.; Shadbolt, N. Before and after GDPR: Tracking in Mobile Apps. *Internet Policy Rev.* **2021**, *10*, 4. [\[CrossRef\]](#)
9. Jin, G.Z.; Liu, Z.; Wagman, L. *The GDPR and SDK Usage in Android Mobile Apps*; National Bureau of Economic Research: New York, NY, USA, 2024.
10. Zaeem, R.N.; Barber, K.S. The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Trans. Manag. Inf. Syst.* **2020**, *12*, 2. [\[CrossRef\]](#)
11. Xiang, A.; Pei, W.; Yue, C. PolicyChecker: Analyzing the GDPR Completeness of Mobile Apps' Privacy Policies. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, New York, NY, USA; Association for Computing Machinery (ACM): New York, NY, USA, 2023; pp. 3373–3387.
12. Rodríguez, D.; Fernández-Aller, C.; Alamo, J.M.D.; Sadeh, N. Data Retention Disclosures in the Google Play Store: Opacity Remains the Norm. In *Proceedings of the 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria; IEEE: New York, NY, USA, 2024; pp. 19–23.
13. Guamán, D.S.; Rodríguez, D.; del Alamo, J.M.; Such, J. Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications. *Comput. Secur.* **2023**, *130*, 103262. [\[CrossRef\]](#)
14. Muchagata, J.; Ferreira, A. Mobile Apps for People with Dementia: Are They Compliant with the General Data Protection Regulation (GDPR)? In *Proceedings of the 12th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2019)—HEALTHINF*; SciTePress: Setúbal, Portugal, 2019; pp. 68–77.
15. Ran, H.; Zhang, H.; Tang, X. GDPR-Bench-Android: A Benchmark for Evaluating Automated GDPR Compliance Detection in Android. *arXiv* **2025**, arXiv:2511.00619. [\[CrossRef\]](#)
16. Rodríguez Torrado, D.; Jain, A.; del Alamo Ramiro, J.M.; Sadeh, N. Comparing Privacy Label Disclosures of Apps Published in Both the App Store and Google Play Stores. In *Proceedings of the 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Delft, The Netherlands; IEEE: New York, NY, USA, 2023; pp. 150–157.
17. Khandelwal, R.; Nayak, A.; Chung, P.; Fawaz, K. Comparing Privacy Labels of Applications in Android and iOS. In *Proceedings of the 2023 ACM CHI Conference on Human Factors in Computing Systems (CHI '23)*, Copenhagen, Denmark; Association for Computing Machinery (ACM): New York, NY, USA, 2023; pp. 61–73.
18. Baalous, R.; Althobaiti, A.; Alyoubi, D.; Alzahrani, R.; Aljohani, M. Detecting the Inconsistency between Android Apps' Data Collection and Google Play's Data Safety Using Static Analysis. *Cybern. Inf. Technol.* **2025**, *25*, 110–125. [\[CrossRef\]](#)
19. Abbott, K.W.; Levi-Faur, D.; Snidal, D. Theorizing Regulatory Intermediaries: The RIT Model. *Ann. Am. Acad. Political Soc. Sci.* **2017**, *670*, 14–35. [\[CrossRef\]](#)
20. Héritier, A.; Lehmkuhl, D. The Shadow of Hierarchy and New Modes of Governance. *J. Public Policy* **2008**, *28*, 1–17. [\[CrossRef\]](#)
21. Medzini, R. Credibility in Enhanced Self-Regulation: The Case of the European Data Protection Regime. *Policy Internet* **2021**, *13*, 366–384. [\[CrossRef\]](#)
22. Gorwa, R. What Is Platform Governance? *Inf. Commun. Soc.* **2019**, *22*, 854–871. [\[CrossRef\]](#)

23. Greene, D.; Shilton, K. Platform Privacies: Governance, Collaboration and the Different Meanings of “Privacy” in iOS and Android Development. *New Media Soc.* **2017**, *20*, 1640–1657. [[CrossRef](#)]
24. van Dijck, J. Seeing the Forest for the Trees: Visualizing Platformization and Its Governance. *New Media Soc.* **2020**, *23*, 2801–2819. [[CrossRef](#)]
25. Törnberg, P. How Platforms Govern: Social Regulation in Digital Capitalism. *Big Data Soc.* **2023**, *10*, 20539517231153808. [[CrossRef](#)]
26. Statista. Number of Apps Available in Leading App Stores [Infographic]. Available online: <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/> (accessed on 1 May 2023).
27. Google Play Help. Understand App Privacy & Security Practices with Google Play’s Data Safety Section. Available online: <https://support.google.com/googleplay/answer/11416267?hl=en&co=GENIE.Platform%3DAndroid> (accessed on 1 May 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.