Improving Mobile App Selection through Transparency and better Permission Analysis

Ilaria Liccardi,[*†] *Joseph Pato*[*], *Daniel J. Weitzner*[*]

Abstract

Our personal information, habits, likes and dislikes can be all deduced from our mobile devices. Safeguarding mobile privacy is therefore of great concern. Transparency and individual control are bedrock principles of privacy but it has been shown that it is difficult to make informed choices about which mobile apps to use. In order to understand the dynamics of information collection in mobile apps and to demonstrate the value of transparent access to the details of their access permissions, we gathered information about 528,433 apps on Google Play, and analyzed the permissions requested by each app. We developed a quantitative measure of the risk posed by apps by devising a *'sensitivity score'* to represent the number of occurrences of permissions that read personal information about users where network communication is possible. We found that 54% of apps do not access any personal data. The remaining 46% collect between 1 and 20 sensitive permissions and have the ability to transmit it outside the phone. The sensitivity of apps differs greatly between free and paid apps as well as between categories and content ratings. Sensitive permissions are often mixed with a large number of no-risk permissions, and hence are difficult to identify. Easily available sensitivity scores could help users make more informed decisions, leading them to choose apps that could pose less risk in collecting their personal information. Even though an app is "self-described" as suitable for a certain subset of users (e.g. children), it might contain content ratings and permission requests that are not appropriate or expected. Our experience in doing this research shows that it is difficult to obtain information about how personal data collected from apps is used or analyzed. Only 6.6% (34,935) of the apps in the collected dataset have declared a "privacy policy" within the app page. In order to make real control available to mobile users, app distribution platforms should provide more detailed information about how personal data is accessed. To achieve greater transparency and individual control, app distribution platforms which do not currently make raw permission information accessible for analysis could change their design and operating policies to make this data available prior to installation.

Keywords: Privacy, Transparency, Mobile Apps, Personal Information, Android.

[*]Massachusetts Institute of Technology
[†]INRIA Saclay Île-de-France

1 Introduction

The mobile phone has become ubiquitous in today's society, to the extent that many people will never leave their house without it in their pocket. People generally feel secure in using them to store personal information, including contact information, emails and photos. Carrying a smartphone every moment of our daily lives, however, means that our personal information, habits, likes and dislikes can all be deduced from a single device. Anyone with access to this information can use it to identify users' home and work locations, hobbies, musical tastes and other personal information. It is therefore important that this information is maintained in an environment with strong privacy practices.

Many of the very apps that make smartphones compelling are key conduits for access to and release of users' personal information. Therefore, we explore the potential for disclosure of private sensitive information by mobile apps, together with the question of whether users have effective access to information on the behaviors of apps in relation to privacy risk.

Unlike previous research, which has analyzed the mere appearance of sensitive permissions [24], we analyze apps' potential behavior by looking at the appearance of personal permissions in conjunction with the ability to transmit this information. However, while it is feasible to collect information about the requirements of apps based on their permission requests, it is impossible to understand why each app requests such permissions and what our personal information is used for. This raises questions about whether users are currently able to exercise basic privacy rights such as individual control and transparency [36]. While apps developed by well-known companies generally provide some means by which users can learn about their personal data practices (by reading long and vague privacy policies), many apps that request personal permission do not disclose what that personal data is used for.

To make smartphone users aware of the personal information an app might access, the Android operating system requires users to review and grant a set of permissions for the app to function. Android apps must declare permissions for nearly everything, from controlling vibration, Internet access and writing to the SD card, to monitoring your location and sending SMS messages. However, prior research demonstrates that few users are well equipped to evaluate the set of permissions requested by apps, hence permissions are often ignored even though they might appear irrelevant to the proper function of the app [25]. Some users do not know what the permissions enable due to technical jargon [17]. Others value the use of the app more than their personal information [16], particularly social networking apps (Facebook is one of the most popular apps on Google Play, despite the fact that it collects lots of personal information about users, both for functionality and to power their ads system). Some simply think that the information that is collected is harmless [35].

We have studied the Android app market to more precisely define the nature of privacy risks in different categories of apps and to investigate if there are better ways to guide users into making reasoned decisions about the applications they choose to use. Our analysis is based on an exhaustive examination rather than a statistical sampling of the applications available in the Google Play Store. This kind of static analysis of the entire marketplace is feasible for the Android platform because it allows users to review permission information prior to installation. This method does not work for other platforms. For example, Apple iOS requires installation and execution to be able to

analyze the permissions needed by the app complicating the process for gathering information and requiring orders of magnitude more time and computational resources.

We studied 528,433 apps, roughly 88% of the Android marketplace (Section 5) and found that it is relatively easy to recognize applications which might pose privacy risks and that this represents a large number of available applications (46% of the apps collected). To distinguish between low/no risk applications and those that have the potential to release sensitive data, we developed a *quantitative* metric for characterizing apps. This ***sensitivity score***, described in section 3.2, measures the occurrence of sensitive permissions that have the ability to access users' personal data when the app also has the ability to disclose this information externally (i.e. has Internet access). The sensitivity score is 0 when an app does not have the ability to disclose sensitive information and increases in value as the app gains the ability to disclose more information. This score could be used as a clear and simple metric to convey how much information users might be giving away, and allow them to make more informed decisions without needing to understand each permission's functionality. Previous research has analyzed apps' permission requests by the mere appearance of sensitive permissions [24] or by measuring the appearance of dangerous permissions that access the state of any personal information whether to read or write [7], however we use the sensitivity score to identify which apps can *read* and *transmit* personal information over the Internet.

The sensitivity score can be used as an indicator when an app is either installed or updated. It can help users make more informed decisions when first choosing to install an app and it can also be used to identify possible changes in the permission set when a new version is released. Since apps can change the permissions they need in newer versions, using a simple indicator like the sensitivity score makes it easier for users to identify when an app transitions to have the potential to disclose data. In section 4.3 we explain how we collected the data and how we parsed the information for each app. In section 5 we compare app sensitivity scores within categories, install ranges and content ratings to assess differences in possible app privacy risks of disclosure of personal information both in free and paid apps. We find that paid apps often have lower sensitivity scores than free apps (section 5.1 and 5.2), that popular apps are not generally safer than less popular apps (section 5.3), and that self-descriptions of target markets (such as "for children") are not always a good indicator for the potential to access sensitive data (section 5.4.1). We show that even though an app is self-described as suitable for children, it might contain content ratings and/or permission requests that are not appropriate or expected.

2 Related Research

Research from a wide variety of sources demonstrates that mobile apps can both collect and infer a considerable amount of personal information about their users. Despite the fact that both users and policy makers express concerns about the privacy practices of mobile apps, existing approaches for users and regulators alike to evaluate and act on privacy practices have considerable shortcomings. As background to the new approach that we present in this paper, we review research on user reactions to privacy in order to understand current barriers to transparency and individual control.

Patterns of mobile phone usage are valuable in detecting behavior trends, especially for marketing [23], as well as customizing and personalizing services offered to users. Research has shown that it is possible to predict new app installations based only on information collected using the

sensors found in smartphones [31], and that it is also possible to infer friendship network structure [9]. Obtaining personal information via mobile phone apps has become very popular and hence privacy in mobile phones has become a popular topic for research [33] and policy regulation, to the extent that the European Commission [19], [29], the Federal Trade Commission [14], [12], [13] and the US National Telecommunications and Information Administration [30] are analyzing and providing guidelines for app store markets and app developers to improve mobile privacy.

Apps can intentionally or unintentionally [32] expose personal information to advertisers and expose personal data publicly, often without the user's knowledge [21]. Even when the app is in an 'idle' mode, it is not guaranteed that the app is not sending personal information [6],[37]. Some developers provide free and paid versions of their apps, where the free version obtains revenue from advertising support, while the paid version does not collect personal information. Users however tend not to buy apps even if they are as cheap as $0.99 [22] - in fact, for developers it is often more lucrative to have a free app that uses advertising for revenue [26]. Not all requests for access to personal information lead to information disclosures. Some apps use personal information as a legitimate part of their operation. In addition, some developers mistakenly request more permissions than the app requires due to insufficient third-party API documentation [15].

Users generally have some awareness about mobile privacy issues, but many still do not take steps to protect their privacy [18]. Researchers have tried to understand how people perceive risks related to privacy leaks [16], how they protect their mobile phones [5] and, where they don't, the reasons why [17],[8]. A 2012 Pew Internet & American Life Project report showed that more than half (57%) of the users interviewed (2,254 adults age 18+) did not install apps when they realized that personal information could be collected, or removed apps from their phone if they found that personal information was collected [5]. However, apps that collect personal information are still extremely popular. We know that users have a difficult time understanding conventional privacy statements [27]. Possibly users do not understand the technical jargon explained in the permissions [17], or are completely unaware of the personal information that they are sharing and need to be educated on the dangers posed to their privacy [34]. Others think that they have nothing to hide [35] or that there is no danger to them.

Regardless of where users fall in the spectrum of privacy concerns, privacy law and practice depends on the ability to make informed decisions on how to choose apps. To increase transparency and individual control, researchers have tried different approaches. Meurer & Wismuller [28] allow the users to filter apps by permission type [28] while Barrera et al. [2] propose a method to improve app permission expressiveness without increasing its overall complexity. Others [11], [20], [38], have tried detecting malicious apps. Zhou et al. [38] introduced DroidRanger, which tries to detect known Android malware families by applying a heuristic-based filtering scheme to identify certain inherent behaviors of unknown malicious families. Enck et al. [11] propose identifying malware based on sets of permissions (Kirin certification) rather than individual permissions, to reduce the number of false positives. Jarabek et al. [20] developed ThinAV, an anti-malware system that uses pre-existing web-based file scanning services for malware detection.

Researchers have enhanced Android itself in order to monitor the flow of information leaving the phone. Enck et al. [10] developed TaintDroid, a modified version of Android able to perform real-time analysis capable of tracking information that leaves the phone. The TaintDroid approach requires a modified version of the Android virtual machine to be installed on the phone by jail-breaking it. While it tracks information, it does not allow the user to stop the information from

being distributed. Mockdroid [4] tries to tackle this problem by allowing users to revoke access to particular permissions at run-time, sacrificing functionality to stop disclosure of (and hence collection of) personal information.

However while all these tools have provided useful information and approaches to allow users to understand the inner working and collection of their personal information, they are hard to set up and require specialized knowledge and technical skills. Therefore, we propose a new method to provide users with more comprehensive and accessible assessments of the privacy practices of mobile apps.

3 Measuring potential riskiness in apps

We quantify the sensitivity of apps by assessing their ability to read personal information. This will allow us to measure the likelihood of third parties accessing, storing and collecting users' information. This measure can be used as an *"awareness mechanism"* to help users identify the number of possible types of information that could be collected about them. This score could be used by users when deciding to download an app and can help them focus on permissions that could pose any risk to their privacy (i.e. have the ability to collect and use personal information) without requiring users to understand and analyze each individual request.

When users search for an app, the search results might present several, if not dozens of options. To choose an app that is relevant to them, users might read the description to understand the features that it offers, look at screenshots, read reviews and ratings from other users, and examine the permissions that the app requests.

However, examining permissions implies that the user has knowledge of how their phone operates and and can differentiate between indifferent permissions (i.e. permissions that are used to interact with the hardware of the phone), permissions that manipulate preferences and information (i.e that have the ability to write), permissions that can read preferences and information (i.e permissions that have the ability to read users' information and manipulate them) and network-based permissions (i.e permissions that allow information exchange via the Internet). Apps come with a multitude of permissions and reading each permission and description in order to understand what they enable can take a lot of effort and/or specialized knowledge.

Previous research [1], [25] has shown that when users are aware of the types of information collected about them by an app, perceptions of the app change to the point that they may consider uninstalling it. The danger posed by individual permissions depends on how the phone is used. For example, if the app is granted access to the contact list, personal relationships might be disclosed, but only if contacts are stored on the phone. Similarly, access to bookmarks and history might only be invasive if the user browses the web via his phone.

Some permissions might be more invasive than others as they might disclose more information about the user. For example, location access can disclose patterns of behavior, while reading photos might be more difficult to interpret. Providing awareness is the key factor in alerting users to potentially invasive permissions, so that they can decide if it is worth the risk.

We will first identify which permissions deal with reading and accessing sensitive information

(section 3.1) and then show how we calculate the sensitivity score (section 3.2), providing an example that calculates the score for two real apps.

3.1 Flagging permissions types

In order to infer the likelihood of apps accessing personal information, we identify permissions that can *read personal* information from the mobile device, for example, permissions that read information relating to call logs or contacts. Some permissions allow personal information to be collected from sources outside the device - for example, reading photos from Picasa albums. Even though this information is not directly collected from the phone, it is accessed through apps running on the phone.

For the purposes of this research we categorized the permissions according to whether they allow access to personal information via the phone or external sources and whether they allow read or write access (Table 1).

Tab. 1: Categories of permission flags according to type of information accessed (personal and system), type of source (mobile or external), and type of access (read/write).

	MOBILE		**EXTERNAL**	
PERSONAL	These permissions read personal data from the phone - for example: **Read call Logs**	These permissions write to personal information on the phone - for example: **Write Contacts**	These permissions read personal data from an external source - for example: **Read pictures from Picasa**	These permissions write personal data to an external source - for example: **Write Pictures to Picasa**
SYSTEM	These permissions read mobile system information - for example: **View Network state**	These permissions can change system settings on the phone - for example: **Change Orientation**	These permissions read external system data - for example: **Market License Check**	These permissions write to external sources - for example: **Google Docs**
	READ	**WRITE**	**READ**	**WRITE**

We then analyzed each permission and flagged it according to Table 1. Using these flags we then categorized each permission into sensitive, indifferent or network permission:

1. **Sensitive Permissions**: if the permission is flagged as *read mobile personal* or *read external personal*, we flag it as sensitive since it allows direct access to personal information. While *write mobile personal* or *write external system* can be considered dangerous (since they might corrupt personal data) they do not grant access to personal data and are therefore not flagged as sensitive. Past research [7] also flagged "write" permissions such as WriteContacts as risky; however, while these permissions can be used in harmful ways by malicious apps, we do not consider the ability to write data as affecting the sensitivity of an app, since this does not allow personal data to be accessed.

We were also interested in understanding the dangers posed by apps sending personal information to developers or third parties. Because of this, we need to flag permissions that can use phone or network access or send data via the Internet.

2. **Network Permission**: These permissions allow apps to modify or enable settings related to connection to the Internet, which allows an app to send data without the owner's permission. While there are different types of network permission that deal with settings configurations, only FULL INTERNET ACCESS allows transmission of data. This permission is the one used in order to calculate the sensitivity score.
3. **Indifferent Permissions**: if the permission is not flagged as *sensitive* or *network*, it is classified as indifferent. Indifferent permissions do not have the ability to access/read personal data, but can set system settings unrelated to the collection of personal data. Indifferent permission can also write to personal data, even though this access might cause problems to the device it does not allow for personal data to be leaked to external sources.

Some permissions fall into more than one category set in Table 1; hence, when a permission would read mobile personal and also write mobile personal it was flagged as a sensitive permission. A full list of all permission categorizations according to sensitive, indifferent or network permissions is shown in Table 9 in Appendix A, where the permissions are listed with their permission type, name, categorization flag, description and frequency of appearance within apps.

3.2 Sensitivity Score

In order to present users with the potential riskiness of apps, we introduce a *sensitivity score*. We use the permission categorization described in Section 3.1.

The **Sensitivity Score** is measured as the occurrence of sensitive permissions within an app's permission list if network permission (FULL INTERNET ACCESS) is also present. The idea is to measure the sensitivity score if the information can leave the phone. There might be cases in which sensitive data can be read but not sent since it was used for functionality only.

$$\textbf{\textit{Sensitivity Score}} = \begin{cases} \sum_{k=1}^{n} \boldsymbol{P_{S_k}}, & \text{if } \boldsymbol{P_N} \neq 0 \\ 0, & \text{if } \boldsymbol{P_N} = 0 \end{cases}$$

where $\boldsymbol{P_S}$ = *sensitive permissions* and $\boldsymbol{P_N}$ = *network permission*.

We also define an **Indifferent Score** which measures the occurrence of non-sensitive and non-network permissions requested by the app:

$$\textbf{\textit{Indifferent Score}} = \sum_{j=0}^{n} \boldsymbol{P_{I_j}}$$

where $\boldsymbol{P_I}$ = *indifferent permissions*.

For example in Figure 1 we show how we compute the sensitivity score of two apps[1]. App 1 requests seven sensitive permissions and one network permission (Figure 1 (a)), while app 2 requests nine sensitive permissions but no network permissions (Figure 1 (b)). For app 1 the sensitivity

[1] These are two real apps, we have anonymized the data since we do not want to imply that one is more malicious than the other. We show the order of permission requests as they appear within each app.

score is seven while for app 2 the sensitivity score is zero. We can see from Figure 1 that sensitive permissions can be embedded with a number of indifferent permissions. While a user trying to download app 2 might be overwhelmed by the permission requests since the app requests seven indifferent permissions and nine sensitive permissions, a simplified sensitivity score could allow them to understand immediately that the app does not have the ability to disclose any personal data. Similarly, for app 1, which requests seven indifferent permissions, seven sensitive permissions and one network permission, the user can see that there are seven relevant permissions that have the ability to access and disclose personal data. For each app we computed the two scores, as well as the total number of permissions requested.

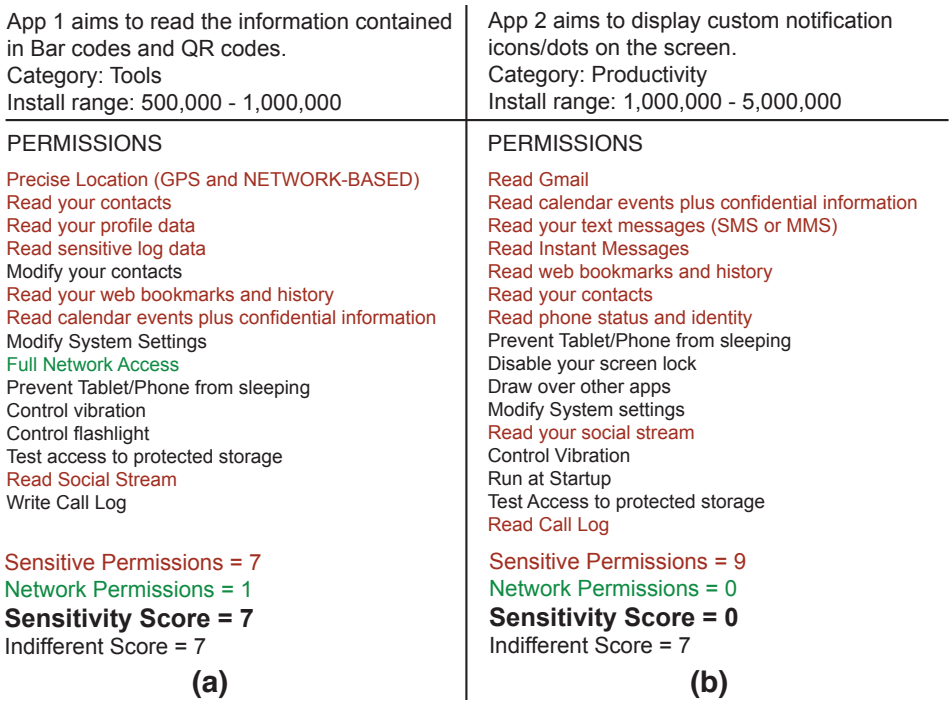


Fig. 1: Example showing how the sensitivity score is calculated for two apps.

3.3 Relationship between sensitivity scores and traditional privacy notices

We propose the sensitivity score as a way of augmenting written privacy notices. While the transparency and accountability function of privacy notices has been historically important, numerous researchers and policy makers have demonstrated the shortcomings of relying solely on privacy policies to enable transparency and individual control. Our work supports this concern. First, we found that a very large percentage of apps have no privacy policy whatsoever. Of the hundreds of thousands of apps we studied, only 34,935 apps (6.6%) have a "*privacy policy*" linked from the page on the Google Play app store from which users select and download the apps. It may be that some of these apps have privacy notices elsewhere, but there is no indication where users

would find them, so their value in making choices about apps is very limited. Second, for users to understand what companies are doing with their personal data (in cases where it is collected) it is often necessary to read long, confusing and sometimes vague descriptions of what, with whom and how personal information is used and shared. These can be hard to read, especially on a mobile device.

Analyzing the actual permissions that control the personal data an app is able to access adds an important dimension to the transparency function of the traditional privacy notice. The permissions, as they are directly related to the technical functions available to an app, establish a 'ground truth' about what data the app has and what it does not have. The privacy notice is important to explain how the app will use that data, but in cases where that notice is either unclear or missing (over 93 % of the apps studied here), the raw description of what data is available to the app can be helpful to both users and others seeking to assess the overall risk associated with using the app. Further elaboration of usage restrictions undertaken by app developers is also important, especially when the app requests a large amount of personal data. That elaboration can come in the form of privacy notices or tagging schemes yet to be developed. Nevertheless, analysis of the baseline permissions requested will always be an important tool for both users and regulators to understand apps' privacy behavior and it fills a gap that exists in today's environment.

Current metadata associated with app behavior may be useful, but we have found that further analysis and categorization is required in order to develop a more complete measure of privacy risk. Google Play provides categories of permission types in the form of "Personal Information", "Your Location", "Your Accounts", "System tools", "Default", "Storage", etc. However, it does not provide a way for users to easily identify permissions that deal with access to their personal information. For example, the READ CALL LOGS permission is within the "Default"[2] category. Similarly the "Personal Information"[3] category includes permissions that deal with writing to personal information (i.e. WRITE CONTACTS) which grant the ability to write it, but not to read it.

4 Methodology: Data Collection and Parsing

In this section we explain how we collected the data for each app (section 4.1), the type of metadata we could collect and how we extracted such information (section 4.2). We also present an overview of Google Play with respect to the collected metadata (section 4.3).

4.1 Fetching

We gathered different apps by performing searches for dictionary words on the Google Play website, and retrieving the page for each app that was found[4]. The search results are split onto multiple

[2] Google recently changed the permission description of READ CALL LOGS from "Default" to "Your Social Information".

[3] The "Personal Information" permission category has been renamed to "Your Social Information".

[4] At the time of this study, the permission information was part of each app page. However, Google recently changed the way that Google Play works in the browser making the fetching of the data needed for this analysis more difficult and more time consuming. Permissions needed for each app are only reported when the *"install"*

pages, so we retrieved each page of search results; Google Play enforces a maximum limit of 20 pages of results for any given search.

We used different dictionaries to collect the apps. We used a large English dictionary and dictionaries for French, Italian, and Spanish to create different queries. After a first round of collection, we also created a custom dictionary using the company names of the apps collected. The Google Play website enforces rate limiting if a large number of requests are made; we therefore included logic that would detect error messages, pause and retry. The script ran for a total of 4 months and 10 days.

4.2 Parsing

For each app there are a number of pieces of information that can be collected. These are described below:

- **Category:** Each app is placed within a category by its developers. This category represents the type of app content. There are two main category types[5]: Games, with 7 categories and Applications with 25.

- **Company:** The name of the company that created the app.

- **Free vs. Paid:** Some apps can be downloaded and installed for free, while others must be purchased.

- **Price:** The price of the app. This does not apply to free apps.

- **Install Range:** The number of installs of the app. The Play store does not provide an exact number of installs; only a general range.

- **Content Rating:** The content rating indicates whether an app is for everyone, or has a maturity rating (these ratings are set by Google). Developers must rate their apps in accordance with Google's content rating guidelines[6].

- **Average Rating:** The average rating of an app based on feedback from users. Users can rate apps from 1 to 5, with 5 being the most positive.

- **Number of users that rated the app:** The total number of ratings from users.

button is pressed and when the browser's user is logged in to an account associated with a smartphone compatible with the current app.

[5] `http://support.google.com/googleplay/android-developer/bin/answer.py?hl=en&answer=113475`

[6] `https://support.google.com/googleplay/android-developer/bin/answer.py?hl=en&answer=188189`

- **Update Date:** The most recent date when the app was updated.

- **Permissions Set:** The permissions that each app requires. A user cannot decide to grant access to one permission and not to another, so installing an app is an all or nothing decision. The *Android manifest* lists 130 different permission types that any app can request. After an app requests these permissions, developers run a script that automatically compiles the permission requests within the app. This is done so that developers cannot omit permissions that they are requesting.

- **Privacy Policy:** The presence of a privacy policy link or description within the app's page.

We are not using three of the factors identified above: (1) average rating, (2) number of users who rated the app and (3) update date. The number of users who rated the app and the average rating is not taken into account in this research since it shows a large discrepancy with the install range. We noted that the number of users who rated an app ranges from 0.00005% to 0.299% of the users who actually installed the app itself. This distinction is made because not everyone who installed an app would rate it. In order to get a more linear measure of popularity we use the install range. For this reason, the average rating is ignored, since it is not based on a proper population size for the app. We don't use the app's "last updated" date since this does not give us any indication of when the app first appeared on the market. Some apps that have been downloaded recently have not been updated recently, so we can not even use this factor to identify dead apps.

4.3 Data Set

We collected metadata on 528,433 apps spanning 31 categories, which represents 88% of the estimated 600,000 apps[7] in the Play store. Using regular expressions, we extracted the following information from each app's page.

- **Category:** We identified a total of 32 categories within Google Play. The website shows which categories are available; however we did not use the "Widget" category since it does not represent a type of app.

  The Games category type contains different types of games, including arcade, puzzles and racing games. This category also includes live wallpapers and casual[8].

  The Application category type includes many different types of app, including Books & References, Sport and Weather apps. It also includes a Live Wallpaper category. For the purposes of this study we therefore divided this into Live Wallpaper Games and Live Wallpaper Applications.

- **Company:** We identified 140,824 companies. The number of apps developed by different companies varies widely from 1 to 2528.

[7] `http://techcrunch.com/2012/06/27/google-play/`
[8] Examples of this category of games are: music, dice and airport control games

- **Free vs. Paid:** We found a large difference in the number of free and paid apps. There were a total of 386,625 free apps and 141,808 paid apps. A full breakdown is shown in Table 3.

- **Price:** The price of apps varies - apps cost between $0.25 and $200.

- **Install Range:** There are 17 different ranges for the number of installs (18 if zero installs is counted). This ranges from 1-5 to 100,000,000-500,000,000.

- **Content Rating:** There are four different content ratings: "Everyone", "Low Maturity", "Medium Maturity" and "High Maturity". An app which has not placed within one of these four rating is shown as "Not rated".

- **Permissions:** We collected the permission type, title and description of each permission. We identified 217 different requested permission labels. Different apps require different sets of permissions, based on functionality and what they are trying to collect about the user. A list of all permissions is shown in Table 9 in Appendix A.

Tab. 2: Distribution of permissions divided into sensitive, indifferent and network types

Sensitive	**Indifferent**	**Network**
55	152	10
25.3%	70.1%	4.6%

- **Privacy Policy**: Only 34,935 specified a *"privacy policy"*, covering 13,539 companies.

5 Analysis

We analyzed the behavior of 528,433 apps on Google Play Store using each app's sensitivity score (section 3.2) as a quantitative indicator of the risk of possible access to personal information. We will present an overview of the dataset (section 5.1) to show the different types of access and then focus on apps that have the ability to disclose personal information. Within each category we compare sensitivity scores by free versus paid apps (section 5.2), installs (hence the popularity) of apps (section 5.3) and content ratings (section 5.4).

We will show that there is a higher concentration of free apps that access personal information compared to paid apps. We will also show that more than 50% of apps within our dataset have a sensitivity score of 0 and therefore do not have the ability to collect personal data. We will highlight the usefulness of a sensitivity score in identifying *sensitive* permissions which are often combined with *indifferent* permissions, and in understanding when sensitive permissions access personal information that may or may not be disclosed to developers or third parties.

5.1 Overview of the dataset

Google Play has two main category types: Games (which has 7 subcategories specifying the type of game) and Applications (which has 25 subcategories which includes different scopes). Games represent 13.76% of the apps we collected, while Applications represent 86.23% of the apps. There are 386,625 free apps compared to 141,808 paid apps.

Table 3 shows the distribution of apps in each category, showing the total number of free and paid apps respectively. It also shows the number of apps that request *sensitive permissions* (at least one sensitive permission), highlighting the percentage of these apps with respect to the total number of apps in each category and considering whether it is free or paid. If an app requests both sensitive and indifferent permissions it is placed in the sensitive category.

Tab. 3: Number of total, free and paid apps in each category, showing the number of free and paid apps that request one or more sensitive permissions, with percentages calculated with respect to the total number of apps in the corresponding free and paid sets.

C.I.	Category Name	Total Apps	Free Apps	Paid Apps	Apps requesting one or more sensitive permission(s)			
					Free		Paid	
					Count	%	Count	%
GAMES (72,717 total apps (13.76%))								
0	Arcade & Action	18,467	13,612	4,855	6,664	48.96%	1,386	28.55%
1	Brain & Puzzle	25,271	19,645	5,626	9,087	46.26%	1,234	21.93%
2	Cards & Casino	4,001	2,920	1,081	1,339	45.86%	211	19.52%
3	Casual	16,441	12,918	3,523	6,268	48.52%	863	24.50%
4	Racing	1,337	1,034	303	602	58.22%	108	35.64%
5	Sports Games	3,027	2,182	845	1,192	54.63%	338	40.00%
6	Live Wallpapers Games	4,173	3,301	872	1,779	53.89%	40	4.590%
APPLICATIONS (455,716 total apps (86.23%))								
7	Books & Reference	36,054	18,695	17,359	7,784	41.64%	3,408	19.63%
8	Business	21,702	19,909	1,793	13,983	70.23%	629	35.08%
9	Comics	2,962	1,878	1,084	565	30.09%	187	17.25%
10	Communication	10,442	8,399	2,043	5,418	64.51%	1,302	63.73%
11	Education	32,324	21,502	10,822	10,271	47.77%	2,144	19.81%
12	Entertainment	51,930	41,604	10,326	24,508	58.91%	3,182	30.82%
13	Finance	10,885	9,413	1,472	5,298	56.28%	314	21.33%
14	Health & Fitness	13,487	9,347	4,140	5,004	53.54%	1,217	29.40%
15	Libraries & Demo	1,940	1,751	189	644	36.78%	32	16.93%
16	Lifestyle	32,463	25,819	6,644	14,670	56.82%	1,811	27.26%
17	Media &Video	8,365	6,693	1,672	3,543	52.94%	726	43.42%
18	Medical	6,347	3,868	2,479	2,061	53.28%	724	29.21%
19	Music & Audio	20,550	17,724	2,826	12,817	72.31%	1,148	40.62%
20	News & Magazines	13,249	12,219	1,030	6,713	54.94%	418	40.58%
21	Personalization	16,068	7,268	8,800	2,748	37.81%	536	6.090%
22	Photography	5,261	3,223	2,038	2,157	66.93%	1,464	71.84%

Continued on next page

Table 3 – continued from previous page

C.I.	Category Name	Total Apps	Free Apps	Paid Apps	Apps requesting one or more sensitive permission(s)			
					Free		Paid	
					Count	%	Count	%
23	Productivity	14,815	10,892	3,923	5,141	47.20%	1,448	36.91%
24	Shopping	6,409	5,918	491	3,581	60.51%	153	31.16%
25	Social	10,291	9,036	1,255	5,945	65.79%	639	50.92%
26	Sports	16,850	13,018	3,832	7,493	57.56%	1,449	37.81%
27	Tools	36,262	27,883	8,379	12,086	43.35%	2,956	35.28%
28	Transportation	5,545	4,583	962	3,215	70.15%	564	58.63%
29	Travel & Local	23,038	15,780	7,258	11,604	73.54%	4,435	61.10%
30	Weather	2,006	1,625	381	968	59.57%	234	61.42%
31	Live Wallpapers Applications	56,471	32,966	23,505	21,028	63.79%	1,705	7.25%
	Total	**528,433**	**386,625**	**141,808**	**216,176**	**55.91%**	**37,005**	**26.10%**

Fewer than 50% (47.93%) of collected apps requested at least one sensitive permission (Table 3), of these, 40.92% of total apps were free (accounting for 55.94% of total free apps) while only 7.01% of apps were in the paid category (accounting for 26.11% of paid apps). This demonstrates that in general, apps in the *paid* category pose lower privacy risk than those in the *free* category.

This implies that 52% (275,252) cannot plausibly collect any personal information: 78,864 apps (31,615 free and 47,249 paid apps) *require NO permissions*, 78,448 apps (64,130 free and 14,358 paid apps) have only *Internet-based permissions*, 117,900 (74,704 free and 43,196 paid apps) have *indifferent permissions*.

There are more paid apps that *require NO permissions* (Figure 5.1 (b)) (47,279 paid apps with respect to 31,615 free apps) than apps that *only have Internet-based permissions* (Figure 5.1 (a)) (14,358 paid apps compared to 64,130 free apps). This could be because apps with no permissions cannot make any revenue unless they are paid, while apps that have only Internet-based permissions can make revenue using advertisements within the app.

Using the sensitivity score we found that within the 48% of apps that request sensitive permissions, 10,446 apps that were initially flagged as sensitive (since they requested one or more sensitive permissions) do not request access to any network permissions that would allow data to be sent outside the device (sensitivity score = 0). Hence, even though an app has access to sensitive permissions, it does not necessarily mean that it has the ability to disclose personal information. A breakdown of sensitive permissions with a corresponding number of apps is shown in Table 4. An example of an app that has a high number of sensitive permission is *Social Manager* by SmallBell. If we look at the permission set, there are no permissions that would allow this app to send this information out of the phone. So while this app could look suspicious, a deeper inspection shows otherwise. A list of permissions for this app is shown in Table 10 in Appendix B.

We characterize apps that do not have the ability to disclose personal information as “safe apps”. This includes apps that only request Internet-based permissions (Figure 5.1 (a)), apps

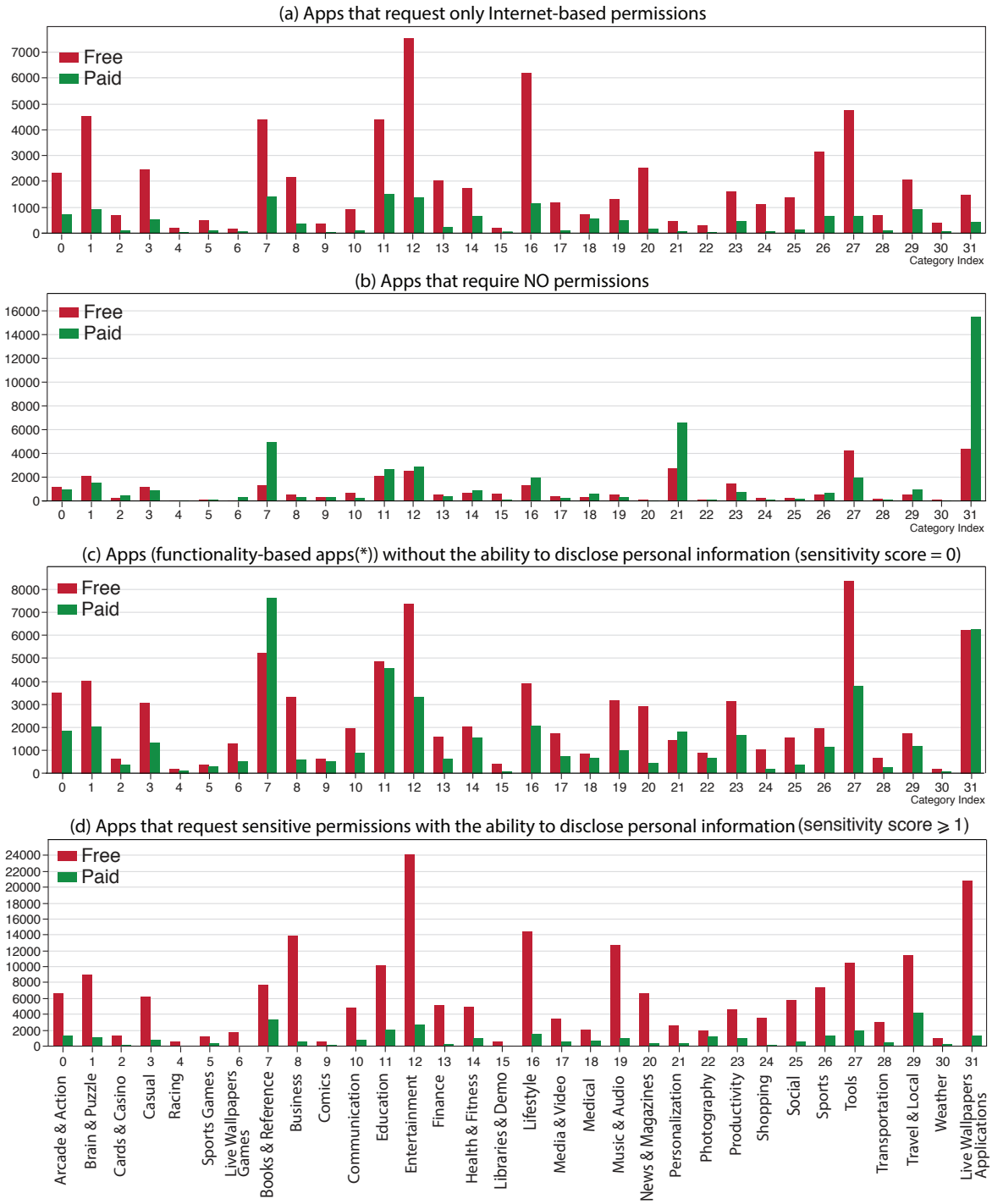


Fig. 2: Overview of apps across categories, grouped according to free and paid sets and divided by different types of permission request.

(*) Functionality-based permission apps are apps that request indifferent permissions or sensitive permissions without Internet access.

Tab. 4: Apps that can access sensitive information but not send it to outside sources such as the developers or advertisers.

# Sensitive Permissions	Total Apps	Free Apps	Paid Apps
1	7,382	3,682	3,700
2	1,878	1,030	848
3	763	432	331
4	271	133	138
5	97	56	41
6	32	20	12
7	15	5	10
8	5	3	2
9	1	-	1
10	1	1	-
13	1	1	-

that request no permissions (Figure 5.1 (b)) and functionality-based apps which either request indifferent permissions or sensitive permissions without Internet access[9](Figure 5.1 (c)). The total number of "safe apps" is 285,599 which is 54% of the collected data set.

In apps that only request Internet permissions (Figure 5.1 (a)), we can see a clear predominance of free apps, while in apps that request no permissions, paid apps are clearly prevalent (Figure 5.1 (b)). In functionality-based apps (Figure 5.1 (c)), free apps constitute the largest group (80,068 free versus 48,278 paid apps) with the exception of two categories - 7 and 31 - where there are more paid apps than free apps in each category. For other categories there are always more free apps, with varying levels of distribution.

However, in apps that request sensitive and Internet permissions (sensitivity score is ≥ 1), we can see a clear predominance of free apps (Figure 5.1 (d)) (210,812 free and 31,923 paid apps). Within these apps, the sensitivity score varies from 1 to 20. However, the number of apps (both paid and free) decreases with respect to the increase of sensitivity scores (Figure 3).

In apps where sensitivity score is ≥ 1, the sensitive permissions are often combined with indifferent permissions (as shown in the example in Figure 1) making them harder to identify. Figure 4 shows all possible combinations between sensitive permissions with indifferent permissions. App permission sets can vary from having a small number of different types of permissions to varying number of permissions. For example, an app can have a small number of sensitive permissions together with a large number of indifferent permissions, or have a large number of sensitive permissions with a small number of indifferent permissions. App permission lists can include up to 125 permissions (126 including network access).

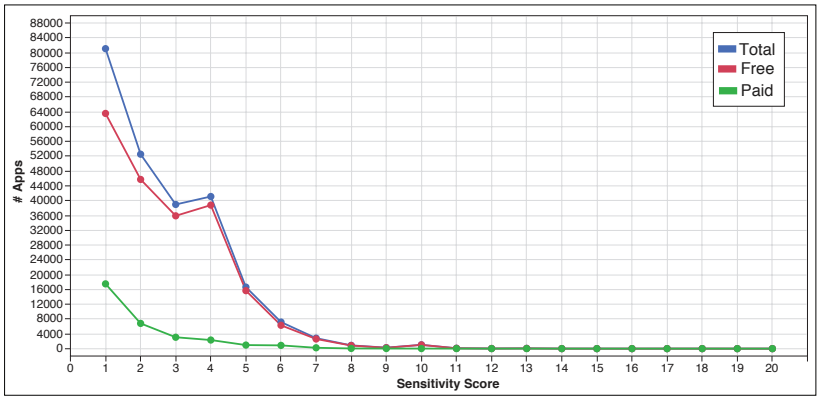
[9] 10,446 apps request sensitive permissions without Internet permissions i.e have a sensitivity score = 0.

S.S	Total	Free	Paid
0	285,698	175,813	109,885
1	81,231	63,656	17,575
2	52,470	45,717	6,753
3	39,067	35,989	3,078
4	41,118	38,795	2,323
5	16,444	15,487	957
6	7,167	6,290	877
7	2,831	2,599	232

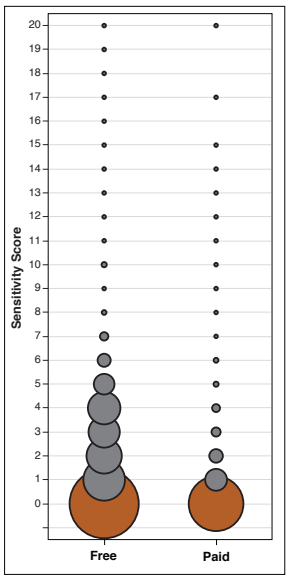
S.S	Total	Free	Paid
8	882	833	49
9	262	233	29
10	1,026	1,008	18
11	99	87	12
12	33	29	4
13	70	59	11
14	13	11	2
15	4	3	1

S.S	Total	Free	Paid
16	2	2	0
17	7	6	1
18	5	5	0
19	2	2	0
20	2	1	1

(a) Breakdown of *"sensitivity score"* across Total, Free and Paid Apps



(b) Number of Apps (total, free and paid) versus *"sensitivity score" where rows representing sensitivity scores of zero have been excluded.*



(c) Bubble plot of "sensitivity score" of free & paid apps. The size of the bubble represents the number of apps.

Fig. 3: Distribution of sensitivity score across the dataset.

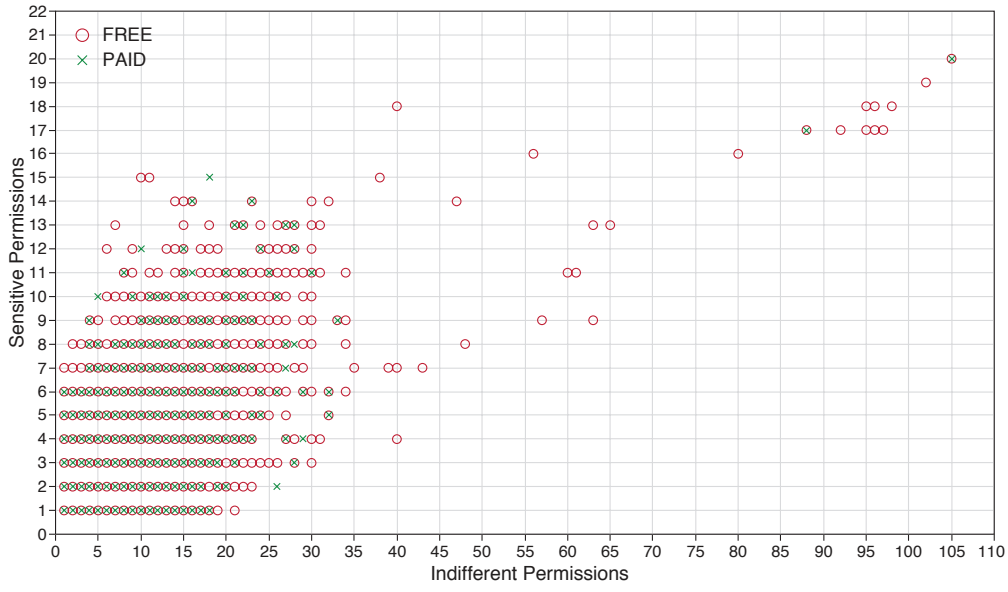


Fig. 4: Number of sensitive permissions vs. number of indifferent permissions in each app where sensitivity score ≥ 1.

5.2 Free vs. Paid: The Price of Lowering Privacy Risk

Within the collected dataset, there are 386,625 free apps compared to 141,808 paid apps. Using the sensitivity score, we see in Figure 3(c) and Figure 5 that free apps usually request on average more sensitive permissions than paid apps (with the exception of category 15, which contains only 40 paid apps). This might be due to free apps requiring personal information to tailor advertisements to users' needs to make them more effective [3]. Figure 3(a) & (c) shows that while the number of paid apps decreases radically with the increase of the sensitivity score, the number of free apps is distributed with sensitivity scores of 1 to 6, decreasing greatly when sensitivity is > 6.

We observe a large disparity between the number of free and paid apps with sensitivity score ≥ 1. Figure 5.1 shows that while the numbers of *apps that request no permissions*, *apps that request only Internet-based permissions* and *apps that request functionality based-permissions* is relatively close, there is a notable disparity within the *apps with a sensitivity score* $\geq$ *1*.

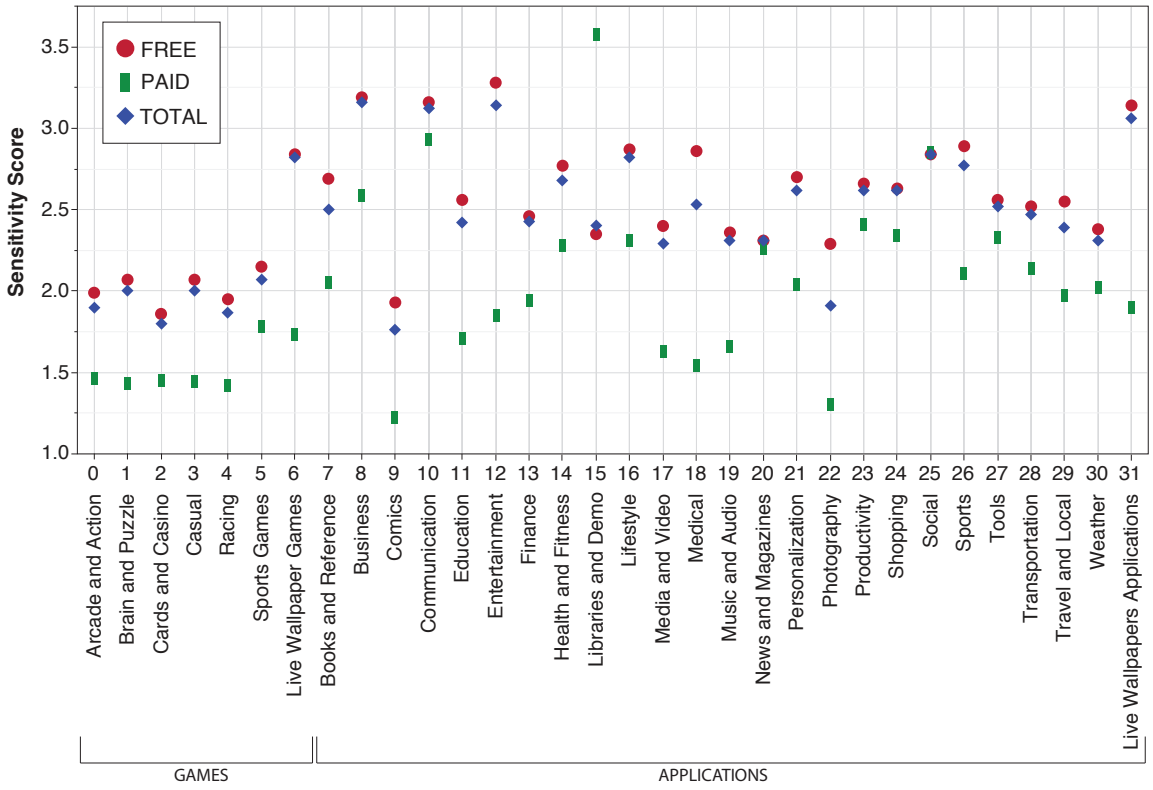


Fig. 5: Mean of sensitivity score across categories, showing both the free and paid sets, and the combined total.

The disparity might be due to app developers being less likely to collect personal data for paid apps. There are instances where developers use different permissions for free and paid apps. Rovio

is one example of a company that produces free apps that collect limited amount of personal data, and paid versions as low as $0.99 that do not display ads and collect no information. However while the paid versions limit the information that is collected, the free version of the app requests access to both the Coarse (Network-Based) Location and Read Phone State and Identity permissions, which could be used to provide advertisements related to location as well as being able to profile users' behavior.

Within the set of paid apps, there are still some apps that request personal information (Figure 3(c)); however, the number of apps exhibiting this behavior represents a lower percentage than the rest (Figure 3 (a)). An example of such a company is *World Media Labs, Inc.* which provides apps for horoscopes (as well as three book apps about Buddhism, Jesus and Chocolate) - it charges $1.99 per app. Each app released by this company has a sensitivity score of 6 and has the ability[10] to collect personal data using the Read Phone State and Identity, Precise Location, Read Calendar Events Plus Confidential Information, Read Call Logs, Take pictures and videos and Read your contacts permissions.

Tab. 5: Mean, median and standard deviation of sensitivity score across categories, showing both the free and paid sets, and the total number of apps in each set.

		Paid Apps				**Free Apps**			
C.I.	**Category Name**	**#Apps**	**Mean**	**Med.**	**Std. Dev.**	**#Apps**	**Mean**	**Med.**	**Std. Dev.**
0	Arcade and Action	1,326	1.45	1	0.976	6,612	1.99	1	1.314
1	Brain and Puzzle	1,164	1.44	1	0.973	9,000	2.06	2	1.289
2	Cards and Casino	196	1.45	1	0.805	1,332	1.86	1	1.187
3	Casual	774	1.44	1	0.936	6,188	2.06	2	1.326
4	Racing	105	1.42	1	0.731	597	1.95	1	1.274
5	Sports Games	328	1.78	2	0.981	1,185	2.14	2	1.446
6	Live Wallpaper Games	37	1.70	1	1.199	1,779	2.82	3	1.479
7	Books and Reference	3,348	2.05	1	1.548	7,710	2.69	2	1.847
8	Business	554	2.58	2	1.657	13,865	3.18	3	1.745
9	Comics	178	1.22	1	0.748	557	1.93	1	1.215
10	Communication	808	2.92	3	1.821	4,816	3.15	3	1.936
11	Education	2,048	1.70	1	1.402	10,132	2.56	2	1.590
12	Entertainment	2,703	1.85	1	1.440	24,184	3.28	3	2.178
13	Finance	259	1.95	1	1.349	5,200	2.45	2	1.390
14	Health and Fitness	1,025	2.28	2	1.457	4,910	2.76	3	1.478
15	Libraries and Demo	24	3.58	3	2.263	563	2.34	2	1.710
16	Lifestyle	1,493	2.30	2	1.507	14,412	2.87	3	1.560
17	Media and Video	553	1.63	1	1.049	3,433	2.39	2	1.424
18	Medical	678	1.53	1	1.204	2,030	2.86	3	1.696
19	Music and Audio	1,042	1.65	1	1.327	12,722	2.36	2	1.271
20	News and Magazines	416	2.26	2	1.611	6,701	2.31	2	1.364

Continued on next page

[10] We are not implying any malicious intent by *World Media Labs, Inc.* or that it collects its users' personal information, simply that it has the ability to do so.

Table 5 – continued from previous page

		Paid Apps				Free Apps			
C.I.	**Category Name**	**#Apps**	**Mean**	**Med.**	**Std. Dev.**	**#Apps**	**Mean**	**Med.**	**Std. Dev.**
21	Personalization	335	2.04	1	1.665	2,600	2.70	3	1.392
22	Photography	1,227	1.30	1	0.776	1,949	2.29	2	1.459
23	Productivity	1,058	2.41	2	1.776	4,665	2.66	2	1.905
24	Shopping	131	2.34	2	1.362	3,551	2.62	2	1.383
25	Social	559	2.84	2	1.757	5,832	2.84	3	1.630
26	Sports	1,382	2.10	2	1.372	7,398	2.89	3	1.520
27	Tools	1,956	2.33	2	1.922	10,530	2.56	2	1.899
28	Transportation	487	2.14	2	1.186	3,087	2.51	2	1.356
29	Travel and Local	4,178	1.97	2	1.157	11,430	2.54	2	1.358
30	Weather	226	2.02	2	0.975	960	2.37	2	1.088
31	Live Wallpaper Applications	1,325	1.90	1	1.385	20,882	3.13	4	1.357
	Total	**31,923**	**1.96**	**1**	**1.442**	**210,812**	**2.72**	**2**	**1.659**

This difference in personal data collection between free and paid apps is highlighted in the difference between the mean of the sensitivity score for free and paid apps (Figure 5). In some categories this difference is minimal, such as in categories 10 (Communication), 25 (Social) and 20 (News & Magazines) in which the mean and the median is either equal or increases by 1 in the case of category 25 (Social). In others the difference is quite evident, such as in categories 6 (Live Wallpaper Games), 17 (Media Video), 18 (Medical), 19 (Music & Audio) and 31 (Live Wallpaper Applications). In these categories the mean and median of the sensitivity score is always greater in free than in paid apps. In category 31 (Live Wallpaper Applications) the median varies from 1 in paid apps to 4 in free apps (Table 5). This indicates that the free apps within these categories collect more personal information. This also implies that in these categories, personal information might not be necessary for the app to function hence it is possible to pay for privacy and not have personal information collected by developers.

5.3 Installs: The popularity factor

The popularity of apps, as measured by the total number of installs, suggests that free apps gain more popularity than paid apps. Access to personal information, however, does not seem to influence the decision of users to download an app; other factors, possibly the the app's functionality, influence users' choices.

Fewer paid apps gain high numbers of installs compared to free apps. In fact only a small percentage of paid apps have exceed 5,000 installs (Figure 7), while apps that are free and collect personal information are present in a higher percentages within the different ranges of installs. It is unclear whether the install rate has any relation to the collection of personal information since we have no way of determining the length of time an app has really been on the Play store. Google Play provides information about the number of installs for each app in 17 different ranges as we

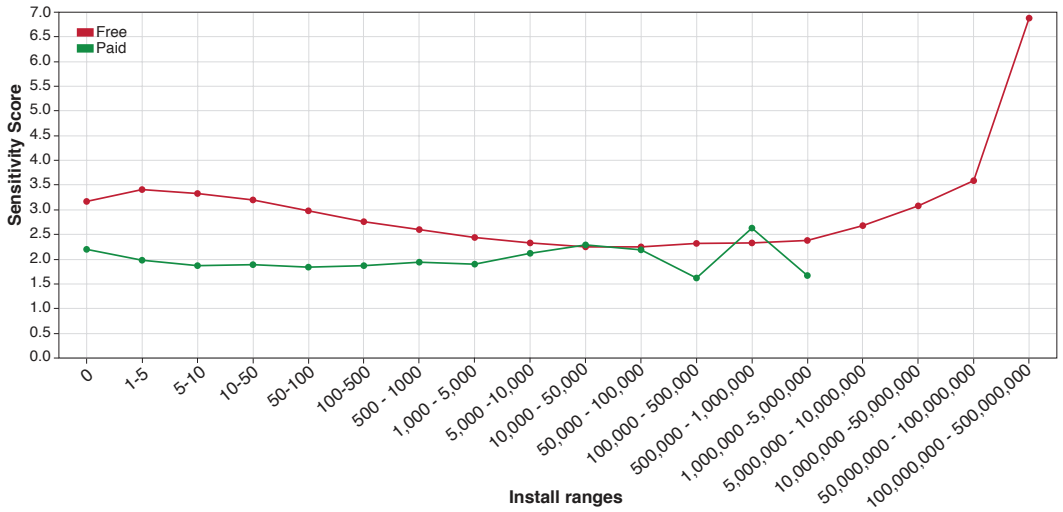


Fig. 6: Mean of sensitivity score plotted against install ranges, showing the free and paid sets.

have shown in Section 4.3. However, there is no information on when apps were first released on Google Play. If we look at the static situation we can see that the sensitivity score across install ranges does not vary greatly (Figure 6) between the free and paid sets, but paid apps still collect less information than free apps, with the exception of install ranges of 10,000-50,000 and 50,000-100,000 in which the mean of sensitivity score is nearly equal (Table 6).

Tab. 6: Mean, median and standard deviation of sensitivity score across different install ranges, showing both the free and paid sets, and the overall total in each set.

	Free Apps			Paid Apps		
Installs	**Mean**	**Std. Dev.**	**#Apps**	**Mean**	**Std. Dev.**	**#Apps**
0	3.17	1.610	5,770	2.20	1.594	4,636
1 - 5	3.41	1.706	11,117	1.98	1.493	6,771
5 - 10	3.33	1.774	6,276	1.87	1.397	2,166
10 - 50	3.20	1.814	28,958	1.89	1.329	6,840
50 - 100	2.98	1.739	14,984	1.84	1.321	2,432
100 -500	2.76	1.633	39,520	1.87	1.305	4,687
500 -1,000	2.60	1.572	17,596	1.94	1.436	1,321
1,000 - 5,000	2.44	1.513	36,112	1.90	1.432	1,787
5,000 - 10,000	2.33	1.466	12,692	2.12	1.777	468
10,000 - 50,000	2.25	1.413	21,221	2.29	1.815	564
50,000 - 100,000	2.25	1.448	5,890	2.19	2.048	108
100,000 - 500,000	2.32	1.586	7,181	1.62	1.552	118
500,000 - 1,000,000	2.33	1.720	1,510	2.63	1.928	16
1,000,000 - 5,000,000	2.38	1.749	1,517	1.67	0.707	9

Continued on next page

Table 6 – continued from previous page

	Free Apps			Paid Apps		
Installs	**Mean**	**Std. Dev.**	**#Apps**	**Mean**	**Std. Dev.**	**#Apps**
5,000,000 - 10,000,000	2.68	2.158	256	-	-	-
10,000,000 - 50,000,000	3.08	2.508	187	-	-	-
50,000,000 - 100,000,000	3.59	2.917	17	-	-	-
100,000,000 - 500,000,000	6.88	4.086	8	-	-	-
Total	**2.72**	**1.659**	**210,812**	**1.96**	**1.442**	**31,923**

Popularity of apps measured by the total number of installs, however, is not a good measure for judging an app's current behavior. Apps can change their behavior and permission request at any time, making it difficult to determine if an app's popularity was driven by the degree to which it accesses and makes use of personal information. An app could have gained significant popularity during a period of time when it needed few sensitive permissions and later changed its behavior to access more information. Similarly an app can add or remove compelling features changing its appeal to users. The total number of installs, however, will not reflect any loss in popularity due to changes in behavior. This information, moreover, is not available from the market and would need to be approximated by a longitudinal study of the apps to see how the rate of installation changes in response to changes in permission requests. Popularity measures based on installs are further hampered due to the lack of precision reported by the marketplace; the marketplace reports installation rates using large bucket ranges. If we look at the static situation we can see that apps with fewer than 100,000 - 500,000 installs make up 98.9% of the total dataset, while those with over 500,000 installs account for only 1.06% (Figure 7). Since a very small number of apps occupy the highest range, we can infer that the functionality of the app is highly desirable by users.

5.4 Content Rating: Who is this app for?

Each app is marked by developers (following Google's guideline[11]) to categorize the content type of their app. There are four levels: "everyone", "low maturity", "medium maturity" and "high maturity". Apps tagged as "everyone" must not collect location data or contain mature material or share the user's content or include social features. This includes all content, including user generated content, in-app products, and advertisements.

While the content rating might be used as a guide for the content type of the app itself, it does not appear to be an adequate indication of potential privacy risk. *Apps that have sensitivity score* $\geq$ *1* are present in a large numbers within the "everyone" and "low maturity rating" especially within the free set (Figure 5.4). Apps flagged as for "everyone" in the paid set present a lower distribution of apps with access to sensitive permission compared to the free set.

However, apps rated for "everyone" present a low mean sensitivity score – 1.55 for free and 1.31 for paid apps. The "Not rated" content rating (apps for which the developer did not select a

[11] `https://support.google.com/googleplay/bin/answer.py?hl=en&answer=1075738`

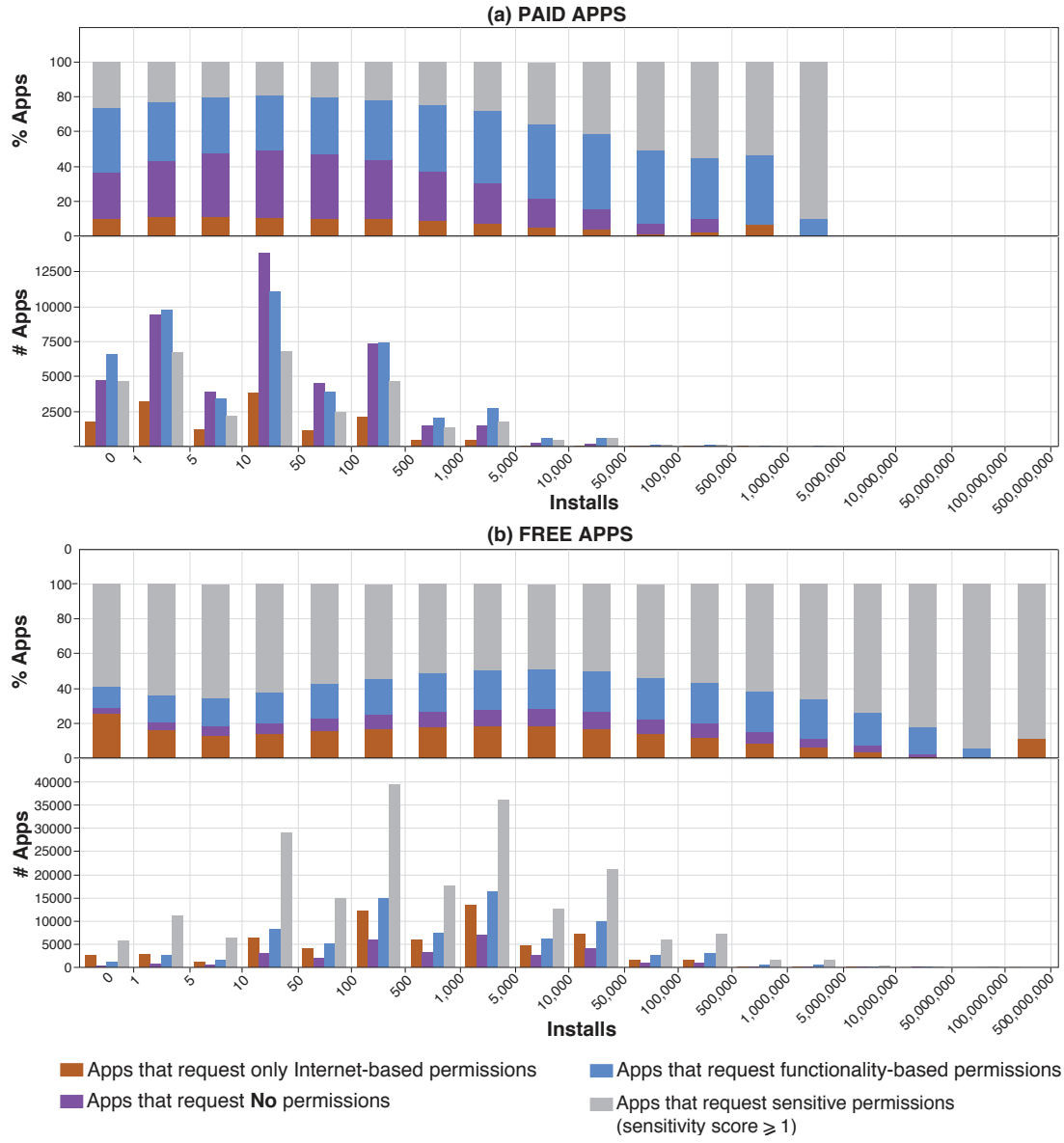


Fig. 7: Number and percentage of apps in the free and paid sets within different install ranges (as provided within the play store) divided by different type of permissions requests.

predefined content rating from the Google guidelines) have the second lowest sensitivity mean of 1.7 for free and 1.76 for paid apps (Table 7).

Further, sensitivity scores do not correlate to maturity ratings. Apps rated as “low maturity”

have the highest mean sensitivity rating (3.22 for free and 2.68 for paid apps) exceeding the sensitivity rating for "medium maturity" (2.83 for free and 2.09 for paid) and "high maturity" (2.68 for free and 1.94 for paid) suggesting that there is a greater potential privacy exposure from apps that might be considered appropriate for a larger audience than from those calling for more caution.

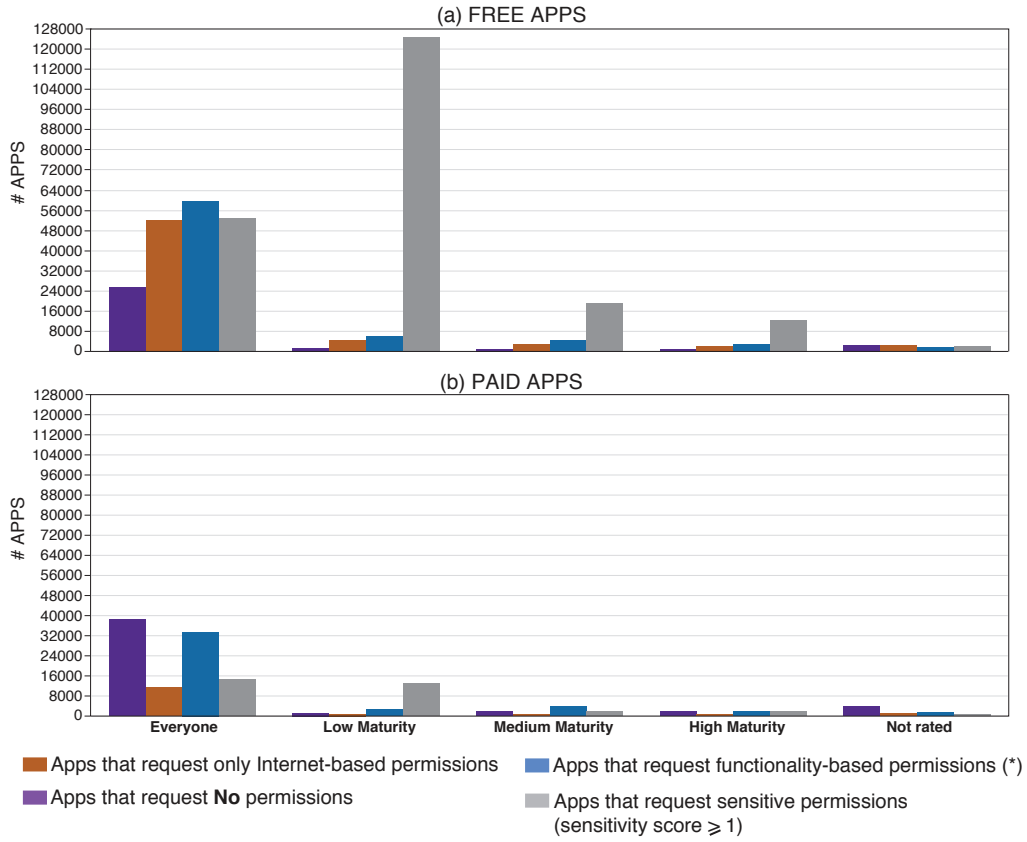


Fig. 8: Overview of the collected apps showing the number of apps in the free and paid sets within different content ratings, divided by different type of permission requests.

(*) Functionality-based permission apps are apps that request indifferent permissions or sensitive permissions without Internet access.

While apps rated for "everyone" present a low median value, $\mu = 1$, between the free and paid apps, the distribution of the sensitivity score differs between the free and paid sets in the low ($\mu = 3$ for free and $\mu = 2$ for paid), medium ($\mu = 3$ for free and $\mu = 2$ for paid) and high ($\mu = 3$ for free and $\mu = 1$ for paid) maturity. This shows that in apps with higher maturity rating, the possibility of disclosure of personal information is higher in the free than the paid sets.

Since we have shown that the content rating of "everyone" has the lowest sensitivity score between the different content rating sets, it should be considered and used when selecting apps for kids. However while content rating can be useful when selecting apps, they are not enforced

or checked by Google prior to the app's release on the Play store and hence can be violated[12]. According to Google guidelines, apps with a content rating of "everyone" should not collect any location information; however, we found that there are 327 apps that collected Coarse network-based location information and 578 apps that collected the fine GPS location, even though they are rated for "everyone". Hence even if an app is marked for "everyone" it does not imply it is an app that kids would like or should use. In the next section we analyze apps that are specifically self-designated to be for kids.

Tab. 7: Sensitivity score of the free and paid sets, distributed by content rating.

Content Rating	Mean	Median	Std. Dev.	Min.	Max.	# Total Apps
Free Apps						
Everyone	1.55	1	1.042	1	15	52,770
Low Maturity	3.22	3	1.653	1	20	124,680
Medium Maturity	2.83	3	1.568	1	14	19,086
High Maturity	2.68	3	1.497	1	17	12,312
Not rated	1.70	1	0.994	1	9	1,964
Total	**2.72**	**2**	**1.659**	**1**	**20**	**210,812**
Paid Apps						
Everyone	1.31	1	0.815	1	11	14,546
Low Maturity	2.68	2	1.662	1	20	12,911
Medium Maturity	2.09	2	1.421	1	9	1,914
High Maturity	1.94	1	1.35	1	10	1,987
Not rated	1.76	1	1.141	1	7	565
Total	**1.96**	**1**	**1.442**	**1**	**20**	**31,923**

5.4.1 Apps for kids

By analyzing the sensitivity scores of apps identified as being for kids, we demonstrate that these apps might still contain content ratings and permission requests that are not appropriate and/or expected. Even though an app can be self-described as for a particular subset of users (eg. *for children*), it can still access personal information that would otherwise seem unnecessary or unexpected. When installing apps, especially for children, other factors should be taken into consideration, such as permission requests and the app's content rating.

[12] While Google does not control if each app meets the content guidelines it states that: *"users can notify us if they believe an app is incorrectly rated. If we agree that the flagged app is incorrectly rated, we will re-rate it per our guidelines. Repeat offenders may be subject to further action, up to and including account termination".*

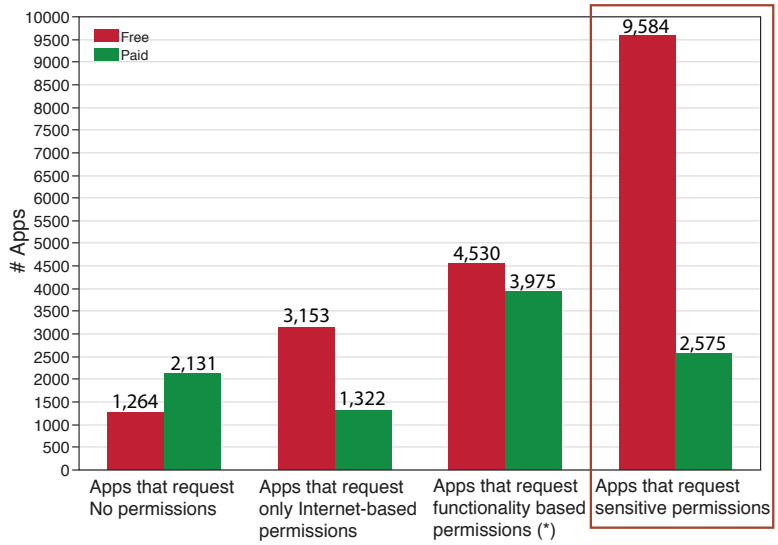


Fig. 9: Distribution of children's apps showing different "app types" based on the type of permissions that they request and grouped according to the free and paid sets.

(*) Functionality-based permission apps are apps that request indifferent permissions or sensitive permissions without Internet access.

We identified 28,534 apps (Table 8) self-described as for children, either in the title or in the description of app itself [13]. Only 2,268 apps for children (representing 1,004 companies) listed a *privacy policy*. Apps that self-identify as "for children" don't necessarily present a content rating of "everyone" (Figure 5.4.1). In fact 9,236 apps presented higher maturity ratings and 374 apps were not rated (Figure 5.4.1). This implies that the app's description might be misleading or ambiguous and that the content ratings of the app itself should be examined prior to installation.

Tab. 8: Apps self-designated as for children, according different type of permissions requested: App type 1: Apps that have a sensitivity score ≥ 1; App type 2: Apps that request indifferent (functionality-based) permissions; App type 3: Apps that request no permissions; App type 4: Apps that request only Internet-based permissions.

C.I.	Category Name	Total Apps	App Type 1		App Type 2		App Type 3		App Type 4	
			Free	Paid	Free	Paid	Free	Paid	Free	Paid
0	Arcade and Action	1,076	386	113	179	96	53	53	139	57
1	Brain and Puzzle	3,740	1288	200	631	345	229	233	671	143
2	Cards and Casino	103	38	6	11	9	5	5	26	3

Continued on next page

[13] Apps were identified by searching for words such as *kid*, *kids*, *child*, *children*, *preschooler* and *preschoolers*. If the app contained one or more of these it was flagged as targeted at kids. If a negation (*not*) was present within the same sentence where the word appeared we did not flag the app.

Table 8 – continued from previous page

C.I.	Category Name	Total Apps	App Type 1		App Type 2		App Type 3		App Type 4	
			Free	Paid	Free	Paid	Free	Paid	Free	Paid
3	Casual	2,216	842	125	445	207	99	119	274	105
4	Racing	84	46	6	12	4	0	3	9	4
5	Sports Games	103	45	25	8	8	2	3	8	4
6	Live Wallpaper Games	388	307	9	51	9	0	4	6	2
7	Books and Reference	2,610	392	178	449	871	67	349	183	121
8	Business	246	165	13	26	10	6	1	15	10
9	Comics	258	73	17	40	44	26	29	24	5
10	Communication	287	139	49	44	36	7	4	5	3
11	Education	6,616	1,556	678	1,062	1,264	392	621	718	325
12	Entertainment	2,814	1,039	178	539	267	103	160	384	144
13	Finance	103	38	2	19	7	7	7	19	4
14	Health and Fitness	937	363	90	114	115	33	67	88	67
15	Libraries and Demo	37	19	1	4	2	8	0	3	0
16	Lifestyle	1,304	571	108	126	162	28	87	108	114
17	Media and Video	313	121	24	63	39	6	20	35	5
18	Medical	418	85	75	37	54	21	57	45	44
19	Music and Audio	596	283	31	88	28	21	16	58	71
20	News and Magazines	149	59	5	46	11	0	1	24	3
21	Personalization	218	77	3	22	21	19	68	2	6
22	Photography	308	109	61	41	65	1	2	25	4
23	Productivity	323	97	56	51	41	13	20	22	23
24	Shopping	192	99	5	33	2	1	3	47	2
25	Social	316	175	32	30	35	10	5	22	7
26	Sports	242	70	21	27	37	15	22	35	15
27	Tools	665	264	92	129	82	31	20	43	4
28	Transportation	61	36	6	5	9	0	0	5	0
29	Travel and Local	744	274	320	47	12	4	15	59	13
30	Weather	17	7	3	1	1	1	0	2	2
31	Live Wallpaper Applications	1,050	521	43	150	82	56	137	49	12
	Total	**28,534**	**9,574**	**2,575**	**4,530**	**3,975**	**1,294**	**2,131**	**3,153**	**1,322**

While the content rating might be used as a guide, it is not an adequate rating for assessing privacy risk since there are still a number of apps that collect personal data with the “everyone” and “low maturity” ratings. Apps that have been self-described to be for children don‘t necessarily

have low sensitivity scores (Figure 11 & Figure 13). 12,159 (42.6%) apps for kids presented a sensitivity score ≥ 1 (Figure 9), meaning that they have the ability to access and possibly disclose personal information. Of these only 1,153 apps listed a *privacy policy*, representing 593 companies.

While in the "everyone" content rating the number of apps with a sensitivity score of 0 is greater than apps with a sensitivity score ≥ 1 – especially in the paid set – it is not true in the other maturity ratings in which apps with a sensitivity score ≥ 1 represent a much larger proportion (Figure 11 (a) & (b)). While the number of apps overall decreases – in particular in the apps for "everyone" – with an increase of sensitivity score, it increases with apps flagged "low maturity" and "medium maturity" only within the free set (Figure 11 (b)).

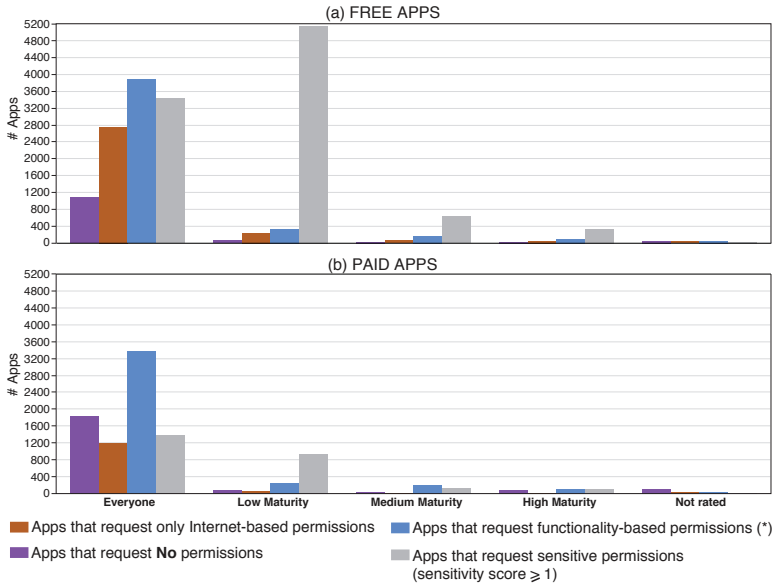
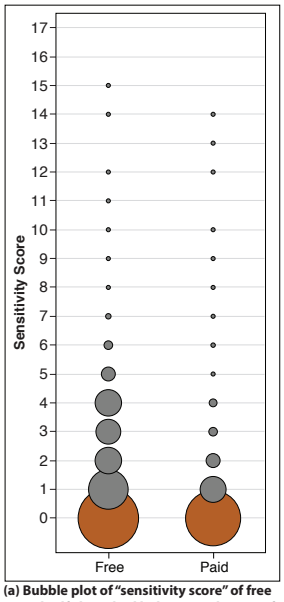


Fig. 10: Apps targeted at children showing the number of apps in the free and paid sets within different content ratings, divided by different type of permission requests.

(*) Functionality-based permission apps are apps that request indifferent permissions or sensitive permissions without Internet access.

For apps with the content rating of "everyone", the mean of the sensitivity score was lower compared to other content ratings (Figure 13). 2,666 free and 1,242 paid of apps flagged as "everyone" request only one personal permission (Figure 11 (b)). A higher number of sensitive permissions are accessed within the other types of content rating with the sensitivity score reaching the highest value of 3.13 within the free apps rated of "low maturity" (Figure 13).

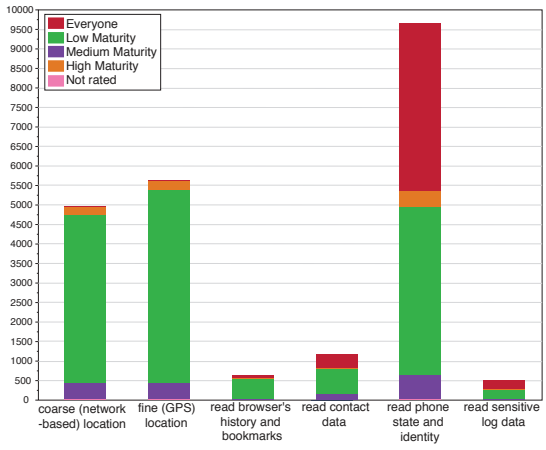


(a) Bubble plot of "sensitivity score" of free & paid self-described kids' apps. The size of the bubble represents the number of apps.

S.S	Total	Everyone	Low Maturity	Medium Maturity	High Maturity	Not rated
FREE						
0	8,947	7,711	649	257	181	149
1	3,836	2,666	843	202	103	22
2	1,721	571	992	97	56	5
3	1,508	135	1,216	81	73	3
4	1,708	37	1,453	143	71	4
5	474	18	366	68	21	1
6	182	4	148	26	4	0
7	72	1	59	8	3	1
8	33	1	22	9	1	0
9	16	0	15	1	0	0
10	13	0	12	1	0	0
11	16	0	16	0	0	0
12	2	0	2	0	0	0
14	2	0	1	1	0	0
15	1	0	1	0	0	0
PAID						
0	7,428	6,393	380	265	213	177
1	1,647	1,242	304	53	44	4
2	479	96	302	24	51	6
3	181	25	129	21	5	1
4	151	15	112	17	6	1
5	37	2	31	2	2	0
6	48	2	41	2	3	0
7	18	4	13	0	1	0
8	5	1	3	1	0	0
9	2	0	2	0	0	0
10	1	0	1	0	0	0
12	1	0	1	0	0	0
13	4	0	4	0	0	0
14	1	0	1	0	0	0

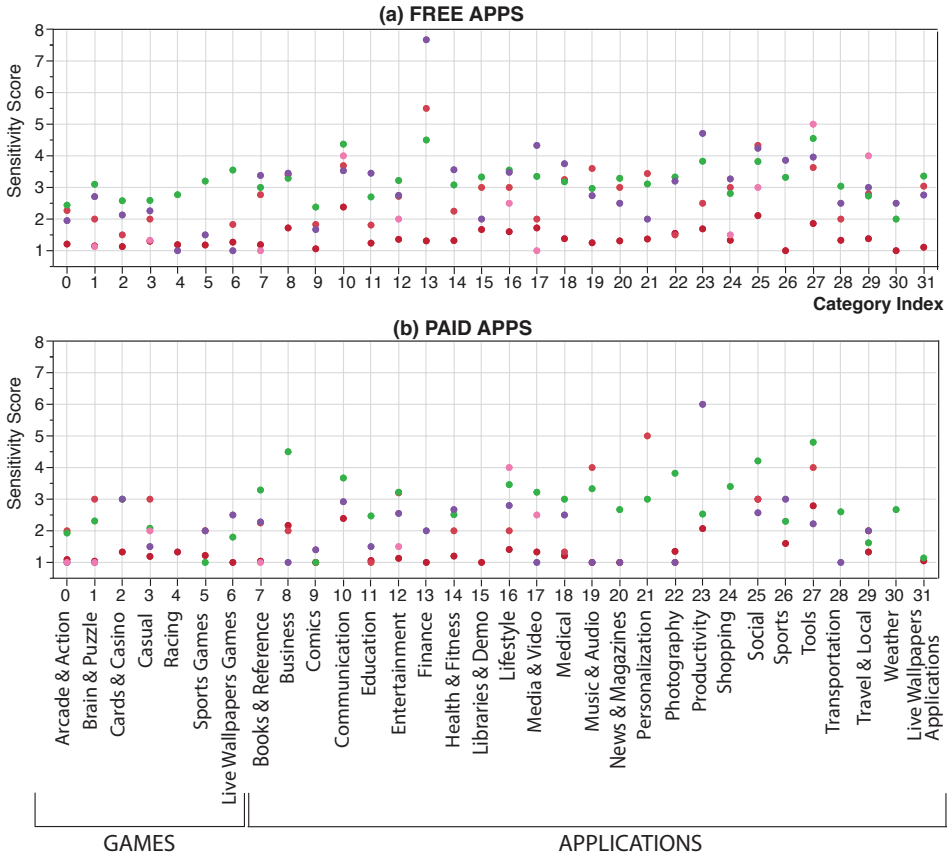
(b) Breakdown of "sensitivity score" across self-described kids' apps across content type grouped by Free and Paid Apps

Fig. 11: Distribution of sensitivity score across self-described children's apps.



Permission Name	Total	Everyone	Low Maturity	Medium Maturity	High Maturity	Not Rated
read sensitive log data	**480**	210	246	17	7	-
fine (GPS) location	**5,605**	10	4,956	409	209	21
read contact data	**1,171**	348	642	138	37	6
coarse (network-based) location	**4,856**	6	4,327	387	206	30
read phone state and identity	**9,638**	4,300	4,319	604	386	29
read browser's history and bookmarks	**631**	76	498	27	30	-

Fig. 12: Example of sensitive permission request, showing total number of apps requesting each permission and number of apps grouped by different content ratings.



FREE	Sensitivity Score Mean	Std. Dev.	# Apps
Everyone	1.31	0.69	3,433
Low Maturity	3.13	1.57	5,146
Medium Maturity	2.64	1.83	637
High Maturiy	2.65	1.44	332
Not Rated	1.92	1.46	36

(c)

PAID	Sensitivity Score Mean	Std. Dev.	# Apps
Everyone	1.18	0.64	1,387
Low Maturity	2.51	1.77	944
Medium Maturity	2.19	1.36	120
High Maturiy	1.98	1.22	112
Not Rated	1.92	0.90	12

(d)

Fig. 13: Children's apps with the ability to access personal information (sensitivity score ≥ 1) showing: 1) mean of sensitivity score across categories grouped by different content rating for free (a) and paid (b) sets and 2) overall mean, standard deviation of sensitivity score, total number of apps in each content rating grouped by free (c) and paid (d) sets.

In Figure 12, we show an example of six sensitive permissions, highlighting the number of apps present for each content rating. We can see that 16 apps rated as being for "everyone" actually violate Google Play guidelines since they collect location information. However, for the most part

this kind of of access is rare within the "everyone" rated apps, with the exception of access to PHONE STATE AND IDENTITY. Apps flagged with higher maturity ratings more commonly request access to sensitive permissions, particularly those flagged to be "low maturity".

Our findings suggest that the descriptions of apps that suggest they are suitable for children may be misleading. When choosing an app for children, a combination of the content rating and sensitivity score appears to give users a more suitable and useful indicator to make informed decisions rather than the description of the app itself.

6 Conclusion and Further Work

This research has presented a quantitative measure of possible privacy disclosures in 528,433 apps in Google Play. We have measured the risk posed by apps by devising a sensitivity score to represent the number of occurrences of sensitive permissions (ie. permissions that read personal information about users) when one or more network permissions are also present. We have seen that the sensitivity score can be a good indicator for privacy risk given potential access of sensitive information within different categories.

Using this information we can infer that the total number of "safe apps" is 285,599 which is 54% of the collected data set (apps with a sensitivity score of zero).

Different categories of apps pose different levels of risk. In general, paid apps are lower risk than free apps when it comes to collecting sensitive data. We have also seen that sensitive permissions often occur in conjunction with indifferent permissions which makes them harder to identify (Figure 4). Hence a sensitivity score could alert the user to investigate the app's behavior by directing the user's attention to the permissions that read personal information. These are the ones that have a heightened but unexpected privacy risk.

Some apps legitimately require access to personal information for functionality, we found 10,446 apps (Table 4) that were initially flagged as sensitive (since they present sensitive permission that read users' personal data) but do not request access to any network permissions that would allow data to be sent outside the device. Hence the sensitivity score for each app could make users aware if there are no risks or alert them to anomalous or unnecessary access. For example in category 31 (Live Wallpaper Applications), free apps collect on average 3.13 sensitive permissions with a $\mu = 4$. In comparison, paid apps collect on average 1.9 sensitive permissions with a $\mu = 1$. Users trying to look for wallpapers for their phone might be guided by the sensitivity score and choose more appropriate apps. Having the sensitivity score embedded within the app description could show users the difference in personal data collected between the free and paid apps and alert them by providing awareness of possible privacy disclosures.

We have seen that when an app is actually tailored for a particular set of users (for example kids in section 5.4.1), the app's description might be misleading. We found different content ratings are attached to apps that have been self-described as for kids. We would expect that an app tailored for kids would have a content rating of "everyone", contain no mature content and not collect personal data. However, that was not the case. We found different content ratings associated with apps specifically tailored for kids. While the "everyone" rating is a good signal for users, this should be used together with the sensitivity score since in some cases even within this particular

rating, personal information might be collected. The maturity rating also proved to be a useful inverse indicator of sensitivity. Low maturity tag ratings are associated with higher sensitivity scores compared to the higher ratings (medium and high maturity), which was surprising.

It is difficult for users to distinguish apps that have little privacy impact from those that pose higher privacy risk, especially when the app has complex permissions (Figure 1). Hence the sensitivity score of each app could be used as a potential quantitative measure to help users evaluate absolute and relative risk of unwanted privacy intrusion. A sensitivity score of 0 can be effective to provide awareness and alert users to pay attention to the app's permissions when it is greater than 0. This could help users to make more informed decisions by being able to identify how many sensitive permissions an app requests if network permission is present.

In future research we want to extend the sensitivity score in order to include the "confused deputy" attack in which one app leverages the privileges of another app through inter-process communication. We will also identify reasons which may lead users to choose apps which might disclose their personal information. We want to understand if users can identify permissions that might lead to personal disclosures both in the choosing and updating stage of apps. We will incorporate the sensitivity score within the current permission presentation and highlight the permissions that contribute to score. We will test our improved interface with users in order to understand if this might help focus them on the permissions that matter and if given this awareness mechanism they might choose different types of apps, less likely to access and disclose personal information or at the least understand the different permissions requests.

Recognizing the difficulty users have in making well-informed choices about the privacy relationships they enter into, we intend to continue this research. We will examine the effect of awareness of personal access with respect to users' choices. However, in addition to revealing various aspects of the privacy behavior of different types of mobile apps, the challenges we faced in even collecting the data necessary for this analysis raises a broader set of questions about the basic transparency of the mobile app environment. We were able to collect data on most of the Android apps in the Google Play App Store but only with considerable difficulty. The permission information on Apple iOS apps for the popular iPhone and iPad devices are entirely inaccessible. We hope that our analysis demonstrates the utility of making such data more accessible to the general public.

7 Acknowledgements

Our thanks to Hal Abelson, Tim Berners-Lee, Evan W. Patton and Fuming Shih for comments and suggestions on earlier drafts. Ilaria Liccardi was supported by the European Commission Marie Curie International Outgoing Fellowship grant 2011-301567 *Social Privacy.* Daniel J. Weitzner acknowledges support from National Science Foundation grant CNS-0831442 *CT-M: Theory and Practice of Accountable Systems* and the Department of Homeland Security grant N66001-12-C-0082 *Accountable Info Systems.*

References

[1] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. "little brothers watching you": raising awareness of data leaks on smartphones. In *Proceedings of the Ninth ACM Symposium on Usable Privacy and Security*, SOUPS'13, pages 12:1–12:11, 2013.

[2] D. Barrera, W. Enck, and P. C. van Oorschot. Seeding a security-enhancing infrastructure for multi-market application ecosystems. In *IEEE Mobile Security Technologies workshop*, MoST'12, pages 9:1–9:10, 2012.

[3] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji. A methodology for empirical analysis of permission-based security models and its application to android. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS'10, pages 73–84, 2010.

[4] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th ACM Workshop on Mobile Computing Systems and Applications*, HotMobile'11, pages 49–54, 2011.

[5] J. L. Boyles, A. Smith, and M. Madden. Privacy and data management on mobile devices. *Pew's Report: Mobile Identity*, pages 1–19, September 5th 2012.

[6] H. Bray. Mobile apps take data without permission. *Boston Globe*, September 2nd 2012.

[7] P. H. Chia, Y. Yamamoto, and N. Asokan. Is this app safe?: a large scale study on application permissions and risk signals. In *Proceedings of the 21st ACM international conference on World Wide Web*, WWW'12, pages 311–320, 2012.

[8] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the 8th ACM Symposium on Usable Privacy and Security*, SOUPS'12, pages 1:1–1:16, 2012.

[9] N. Eagle, A. Pentland, and D. Lazer. Inferring friendship network structure by using mobile phone data. *Proceedings of the National Academy of Sciences (PNAS)*, 106(36):15274–15278, 2009.

[10] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *proceedings of 9th USENIX conference on Operating systems design and implementation*, OSDI'10, pages 1–6, 2010.

[11] W. Enck, M. Ongtang, and P. McDaniel. On lightweight mobile phone application certification. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS'09, pages 235–245, 2009.

[12] Federal-Trade-Commission. Mobile apps for kids: Current privacy disclosures are disappointing. pages 1–23, February 2012.

[13] Federal-Trade-Commission. Mobile apps for kids: Disclosures still not making the grade. pages 1–21, December 2012.

[14] Federal-Trade-Commission. Mobile privacy disclosures: Building trust through transparency. pages 1–29, February 2013.

[15] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS'11, pages 627–638, 2011.

[16] A. P. Felt, S. Egelman, and D. Wagner. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, SPSM'12, pages 33–44, 2012.

[17] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the 8th ACM Symposium on Usable Privacy and Security*, SOUPS'12, pages 3:1–3:14, 2012.

[18] A. Gahran. Survey: Most cell phone users don't protect mobile privacy. *CNNTech*, September 2nd 2012.

[19] GSM-Assosiation. Gsma mobile and privacy, privacy design guidelines for mobile application development. pages 1–27, February 2012.

[20] C. Jarabek, D. Barrera, and J. Aycock. Thinkav: truly lightweight mobile cloud-based anti-malware. In *Proceedings of the 28th ACM Annual Computer Security Applications Conference*, ACSAC'12, pages 209–218, 2012.

[21] B. Krishnamurthy and C. E. Wills. On the leakage of personally identifiable information via online social networks. *SIGCOMM Comput. Commun. Rev.*, 40(1):112–117, 2010.

[22] A. Kumpati. Why you won't pay $0.99 for apps, but will spend $7.15 for coffee. *iCosmoGeeks*, 21 August 2012.

[23] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell. A survey of mobile phone sensing. *IEEE Communications Magazine*, 48(9):140 –150, 2010.

[24] I. Leontiadis, C. Efstratiou, M. Piconey, and C. Mascolo. Don't kill my ads! balancing privacy in an ad-supported mobile application market. In *Proceedings of 13th ACM Sigmobile Workshop on Mobile Computing Systems and Applications*, HotMobile'12, 2012.

[25] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp'12, pages 501–510, 2012.

[26] J. Manoogian. How free apps can make more money than paid apps. *TechCrunch*, August 26 2012.

[27] A. McDonald and L. F. Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. TPRC, pages 1–31. 2010.

[28] S. Meurer and R. Wismüller. Apefs: An infrastructure for permission-based filtering of android apps. In A. Schmidt, G. Russello, I. Krontiris, and S. Lian, editors, *Security and Privacy in Mobile Information and Communication Systems*, volume 107 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 1–11. Springer Berlin Heidelberg, 2012.

[29] MobileEurope. Gsma urges european mobile industry to adopt new privacy framework. *Press Wires*, January 30th 2013.

[30] National-Telecommunications-Information-Administration. Privacy multistakeholder process: Mobile application transparency. March 2013.

[31] W. Pan, N. Aharony, and A. S. Pentland. Composite social network for predicting mobile apps installation. In *proceeding of the ACM Association for the Advancement of Artificial Intelligence*, AAAI'11, pages 821–827, 2011.

[32] N. Perlroth and N. Bilton. Mobile apps take data without permission. *New York Times*, February 15th 2012.

[33] K. Shilton. Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 52(11):48–53, 2009.

[34] D. J. Solove. *Understanding Privacy.* Harvard University Press, March 30 2010.

[35] D. J. Solove. *Nothing to Hide: The False Tradeoff between Privacy and Security.* Yale University Press, May 31 2011.

[36] White-House. Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. February 2012.

[37] F. Zhang. Assessing intrusiveness of smarthphone apps. Master's thesis, MIT, 2012.

[38] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang. Hey, you, get off of my market: Detecting malicious apps in official and alternative android markets. In *proceedings of the 19th Annual Network and Distributed System Security Symposium*, NDSS'12, 2012.

Appendix A Permissions Category, Label, Description, Frequency and Type

Table 9 below shows the frequency of appearance of each permission across the entire dataset as well as the permission's category, label and description. Each permission is marked as sensitive (S), network (N) and indifferent permissions (I).

Tab. 9: Permissions Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Network communication	full Internet access	Allows the app to create network sockets.	433,314	(N)
Your personal information	read your contacts	Allows the app to read all of the contact (address) data stored on your tablet. Malicious apps may use this to send your data to other people. Allows the app to read all of the contact (address) data stored on your phone. Malicious apps may use this to send your data to other people.	334,281	(S)
Network communication	view network state	Allows the app to view the state of all networks.	298,291	(N)
Storage	modify/delete USB storage contents modify/delete SD card contents	Allows the app to write to the USB storage. Allows the app to write to the SD card.	212,729	(I)
Phone calls	read phone state and identity	Allows the app to access the phone features of the device. An app with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.	195,693	(S)
Your location	fine (GPS) location	Access fine location sources such as the Global Positioning System on the tablet, where available. Malicious apps may use this to determine where you are, and may consume additional battery power. Access fine location sources such as the Global Positioning System on the phone, where available. Malicious apps may use this to determine where you are, and may consume additional battery power.	135,445	(S)
Your location	coarse (network-based) location	Access coarse location sources such as the cellular network database to determine an approximate tablet location, where available. Malicious apps may use this to determine approximately where you are. Access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this to determine approximately where you are.	122,381	(S)
Your messages	receive SMS	Allows the app to receive and process SMS messages. Malicious apps may monitor your messages or delete them without showing them to you.	120,501	(S)
System tools	prevent tablet from sleeping prevent phone from sleeping	Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.	120,010	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Hardware controls	control vibrator	Allows the app to control the vibrator.	107,947	(I)
Network communication	view Wi-Fi state	Allows the app to view the information about the state of Wi-Fi.	71,958	(N)
System tools	automatically start at boot	Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.	71,407	(I)
Network communication	receive data from Internet	Allows apps to accept cloud to device messages sent by the app's service. Using this service will incur data usage. Malicious apps could cause excess data usage.	51,858	(I)
Hardware controls	take pictures and videos	Allows the app to take pictures and videos with the camera. This allows the app at any time to collect images the camera is seeing.	50,396	(S)
Your accounts	find accounts on the device	Allows the app to get the list of accounts known by the tablet. Allows the app to get the list of accounts known by the phone.	49,149	(S)
Your location	access extra location provider commands	Allows the app to access extra location provider commands. Malicious apps may use this to interfere with the operation of the GPS or other location sources.	42,772	(S)
Services that cost you money	directly call phone numbers	Allows the app to call phone numbers without your intervention. Malicious apps may cause unexpected calls on your phone bill. Note that this doesn't allow the app to call emergency numbers.	39,631	(I)
System tools	set wallpaper	Allows the app to set the system wallpaper.	26,433	(I)
Network communication	view network connections	Allows the app to view information about network connections such as which networks exist and are connected.	24,879	(N)
Hardware controls	record audio	Allows the app to access the audio record path.	24,841	(I)
Network communication	Market license check	Can check if you have a license for this application from Market	21,259	(I)
Your messages	read SMS or MMS	Allows the app to read SMS messages stored on your tablet or SIM card. Malicious apps may read your confidential messages. Allows the app to read SMS messages stored on your phone or SIM card. Malicious apps may read your confidential messages.	20,723	(S)
Your personal information	write contact data	Allows the app to modify the contact (address) data stored on your tablet. Malicious apps may use this to erase or modify your contact data. Allows the app to modify the contact (address) data stored on your phone. Malicious apps may use this to erase or modify your contact data.	19,747	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
System tools	retrieve running apps	Allows the app to retrieve information about currently and recently running tasks. Malicious apps may discover private information about other apps.	19,593	(I)
Default	Market billing service	Allows the user to purchase items through Market from within this application	19,376	(I)
Services that cost you money	send SMS messages	Allows the app to send SMS messages. Malicious apps may cost you money by sending messages without your confirmation.	17,715	(I)
Default	test access to protected storage test access to protected storage	Allows the app to test a permission for USB storage that will be available on future devices. Allows the app to test a permission for the SD card that will be available on future devices.	17,587	(I)
Your personal information	write Browser's history and bookmarks	Allows the app to modify the Browser's history or bookmarks stored on your tablet. Malicious apps may use this to erase or modify your Browser's data. Allows the app to modify the Browser's history or bookmarks stored on your phone. Malicious apps may use this to erase or modify your Browser's data.	15,921	(I)
System tools	modify global system settings	Allows the app to modify the system's settings data. Malicious apps may corrupt your system's configuration.	15,727	(I)
Your personal information	read Browser's history and bookmarks	Allows the app to read all the URLs that the Browser has visited, and all of the Browser's bookmarks	15,279	(S)
Your location	mock location sources for testing	Allows the app to create mock location sources for testing. Malicious apps may use this to override the location and/or status returned by real location sources such as GPS or network providers.	12,219	(I)
Hardware controls	change your audio settings	Allows the app to modify global audio settings such as volume and routing.	12,165	(I)
System tools	change Wi-Fi state	Allows the app to connect to and disconnect from Wi-Fi access points, and to make changes to configured Wi-Fi networks.	11,900	(N)
Your location	precise location (GPS and network-based)	Allows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are, and may consume additional battery power.	11,408	(S)
System tools	send sticky broadcast	Allows the app to send sticky broadcasts, which remain after the broadcast ends. Malicious apps may make the tablet slow or unstable by causing it to use too much memory. Allows the app to send sticky broadcasts, which remain after the broadcast ends. Malicious apps may make the phone slow or unstable by causing it to use too much memory.	10,901	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Hardware controls	control flashlight	Allows the app to control the flashlight.	10,550	(I)
Your personal information	read calendar events plus confidential information	Allows the app to read all calendar events stored on your tablet, including those of friends or coworkers. Malicious apps may extract personal information from these calendars without the owners' knowledge. Allows the app to read all calendar events stored on your phone, including those of friends or coworkers. Malicious apps may extract personal information from these calendars without the owners' knowledge.	10,512	(S)
Network communication	view Wi-Fi connections	Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.	9,719	(N)
Hardware controls	control vibration	Allows the app to control the vibrator.	9,032	(I)
Phone calls	intercept outgoing calls	Allows the app to process outgoing calls and change the number to be dialed. Malicious apps may monitor, redirect, or prevent outgoing calls.	8,254	(S)
Your personal information	read sensitive log data	Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the tablet, potentially including personal or private information. Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.	8,219	(S)
System tools	run at startup	Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.	8,084	(I)
Your personal information	add or modify calendar events and send email to guests without owners' knowledge	Allows the app to send event invitations as the calendar owner and add, remove, change events that you can modify on your device, including those of friends or co-workers. Malicious apps may send spam emails that appear to come from calendar owners, modify events without the owners' knowledge, or add fake events.	7,960	(S)
System tools	disable keylock	Allows the app to disable the keylock and any associated password security. A legitimate example of this is the phone disabling the keylock when receiving an incoming phone call, then re-enabling the keylock when the call is finished.	7,890	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Your messages	receive WAP	Allows the app to receive and process WAP messages. Malicious apps may monitor your messages or delete them without showing them to you.	7,557	(S)
System tools	kill background processes	Allows the app to kill background processes of other apps, even if memory isn't low.	7,331	(I)
System tools	mount and unmount filesystems	Allows the app to mount and unmount filesystems for removable storage.	6,390	(I)
Network communication	create Bluetooth connections	Allows the app to view the configuration of the local Bluetooth tablet, and to make and accept connections with paired devices. Allows the app to view the configuration of the local Bluetooth phone, and to make and accept connections with paired devices.	6,047	(I)
System tools	change your UI settings	Allows the app to change the current configuration, such as the locale or overall font size.	5,215	(I)
Your messages	edit SMS or MMS	Allows the app to write to SMS messages stored on your tablet or SIM card. Malicious apps may delete your messages. Allows the app to write to SMS messages stored on your phone or SIM card. Malicious apps may delete your messages.	4,854	(I)
System tools	change network connectivity	Allows the app to change the state of network connectivity.	4,818	(N)
System tools	Bluetooth administration	Allows the app to configure the local Bluetooth tablet, and to discover and pair with remote devices. Allows the app to configure the local Bluetooth phone, and to discover and pair with remote devices.	4,473	(I)
Default	directly install apps	Allows the app to install new or updated Android packages. Malicious apps may use this to add new apps with arbitrarily powerful permissions.	4,359	(I)
Your accounts	use the authentication credentials of an account	Allows the app to request authentication tokens.	4,068	(I)
Your accounts	view configured accounts	Allows apps to see the usernames (email addresses) of the Google account(s) you have configured.	3,179	(S)
System tools	display system-level alerts	Allows the app to show system alert windows. Malicious apps may take over the entire screen.	3,114	(I)
Your accounts	access other Google services	Allows apps to sign in to unspecified Google services using the account(s) stored on this Android device.	2,954	(S)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Default	enable or disable app components	Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important tablet capabilities. Care must be used with this permission, as it is possible to get app components into an unusable, inconsistent, or unstable state. Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important phone capabilities. Care must be used with this permission, as it is possible to get app components into an unusable, inconsistent, or unstable state.	2,842	(I)
Your accounts	manage the accounts list	Allows the app to perform operations like adding and removing account, and deleting their passwords.	2,623	(S)
Default	modify battery statistics	Allows the app to modify collected battery statistics. Not for use by normal apps.	2,592	(I)
Your messages	receive MMS	Allows the app to receive and process MMS messages. Malicious apps may monitor your messages or delete them without showing them to you.	2,564	(S)
Default	delete apps	Allows the app to delete Android packages. Malicious apps may use this to delete important apps.	2,375	(I)
Phone calls	modify phone state	Allows the app to control the phone features of the device. An app with this permission can switch networks, turn the phone radio on and off and the like without ever notifying you.	2,212	(N)
System tools	set wallpaper size hints	Allows the app to set the system wallpaper size hints.	2,158	(I)
Default	directly call any phone numbers	Allows the app to call any phone number, including emergency numbers, without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services.	2,115	(I)
Default	read call log	Allows the app to read your tablet's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge. Allows the app to read your phone's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge.	2,023	(S)
System tools	modify system settings	Allows the app to modify the system's settings data. Malicious apps may corrupt your system's configuration.	1,791	(I)
System tools	read sync settings	Allows the app to read the sync settings, such as whether sync is enabled for the People app.	1,783	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
System tools	write sync settings	Allows the app to modify the sync settings, such as whether sync is enabled for the People app.	1,762	(I)
Your accounts	act as an account authenticator	Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.	1,757	(S)
Default	power tablet on or off power phone on or off	Allows the app to turn the tablet on or off. Allows the app to turn the phone on or off.	1,583	(I)
Default	control location update notifications	Allows the app to enable/disable location update notifications from the radio. Not for use by normal apps.	1,577	(I)
System tools	connect and disconnect from Wi-Fi	Allows the app to connect to and disconnect from Wi-Fi access points and to make changes to device configuration for Wi-Fi networks.	1,541	(N)
Default	modify secure system settings	Allows the app to modify the system's secure settings data. Not for use by normal apps.	1,415	(I)
Your personal information	modify your contacts	Allows the app to modify the data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data. Allows the app to modify the data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data.	1,350	(S)
Network communication	control Near Field Communication	Allows the app to communicate with Near Field Communication (NFC) tags, cards, and readers.	1,297	(I)
Default	change screen orientation	Allows the app to change the rotation of the screen at any time. Should never be needed for normal apps.	1,267	(I)
System tools	allow Wi-Fi Multicast reception	Allows the app to receive packets not directly addressed to your device. This can be useful when discovering services offered near by. It uses more power than the non-multicast mode.	1,203	(I)
Default	write call log	Allows the app to modify your tablet's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log. Allows the app to modify your phone's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log.	1,184	(I)
System tools	delete all app cache data	Allows the app to free tablet storage by deleting files in app cache directory. Access is very restricted usually to system process. Allows the app to free phone storage by deleting files in app cache directory. Access is very restricted usually to system process.	1,138	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
System tools	access USB storage filesystem access SD Card filesystem	Allows the app to mount and unmount filesystems for removable storage.	1,101	(I)
System tools	expand/collapse status bar	Allows the app to expand or collapse the status bar.	991	(I)
System tools	change/intercept network settings and traffic	Allows the app to change network settings and to intercept and inspect all network traffic, for example to change the proxy and port of any APN. Malicious apps may monitor, redirect, or modify network packets without your knowledge.	932	(N)
Default	disable or modify status bar	Allows the app to disable the status bar or add and remove system icons.	875	(I)
Your accounts	act as the AccountManagerService	Allows the app to make calls to AccountAuthenticators.	652	(S)
System tools	read sync statistics	Allows the app to read the sync stats; e.g., the history of syncs that have occurred.	652	(I)
Hardware controls	test hardware	Allows the app to control various peripherals for the purpose of hardware testing.	641	(I)
System tools	disable your screen lock	Allows the app to disable the keylock and any associated password security. For example, the phone disables the keylock when receiving an incoming phone call, then reenables the keylock when the call is finished.	639	(I)
System tools	make app always run	Allows the app to make parts of itself persistent, so the system can't use it for other apps.	626	(I)
System tools	change system display settings	Allows the app to change the current configuration, such as the locale or overall font size.	588	(I)
Default	delete other apps' data	Allows the app to clear user data.	579	(I)
Default	force tablet reboot force phone reboot	Allows the app to force the tablet to reboot. Allows the app to force the phone to reboot.	578	(I)
Default	delete other apps' caches	Allows the app to delete cache files.	548	(I)
Your personal information	choose widgets	Allows the app to tell the system which widgets can be used by which app. An app with this permission can give access to personal data to other apps. Not for use by normal apps.	515	(I)
System tools	measure app storage space	Allows the app to retrieve its code, data, and cache sizes	509	(I)
System tools	close other apps	Allows the app to end background processes of other apps. This may cause other apps to stop running.	471	(I)
System tools	draw over other apps	Allows the app to draw on top of other applications or parts of the user interface. They may interfere with your use of the interface in any application, or change what you think you are seeing in other applications.	461	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
System tools	set preferred apps	Allows the app to modify your preferred apps. Malicious apps may silently change the apps that are run, spoofing your existing apps to collect private data from you.	421	(I)
Default	press keys and control buttons	Allows the app to deliver its own input events (key presses, etc.) to other apps. Malicious apps may use this to take over the tablet. Allows the app to deliver its own input events (key presses, etc.) to other apps. Malicious apps may use this to take over the phone.	399	(I)
Default	read frame buffer	Allows the app to read the content of the frame buffer.	348	(I)
System tools	reorder running apps	Allows the app to move tasks to the foreground and background. Malicious apps may force themselves to the front without your control.	330	(I)
Your messages	send SMS-received broadcast	Allows the app to broadcast a notification that an SMS message has been received. Malicious apps may use this to forge incoming SMS messages.	328	(I)
Phone calls	reroute outgoing calls	Allows the app to process outgoing calls and change the number to be dialed. This permission allows the app to monitor, redirect, or prevent outgoing calls.	318	(S)
Network communication	make/receive Internet calls	Allows the app to use the SIP service to make/receive Internet calls.	318	(I)
Default	bind to a wallpaper	Allows the holder to bind to the top-level interface of a wallpaper. Should never be needed for normal apps.	311	(I)
Default	access SurfaceFlinger	Allows the app to use SurfaceFlinger low-level features.	305	(I)
Network communication	pair with Bluetooth devices	Allows the app to view the configuration of Bluetooth on the tablet, and to make and accept connections with paired devices. Allows the app to view the configuration of the Bluetooth on the phone, and to make and accept connections with paired devices.	299	(I)
Default	access checkin properties	Allows the app read/write access to properties uploaded by the checkin service. Not for use by normal apps.	292	(I)
Your personal information	set alarm in alarm clock	Allows the app to set an alarm in an installed alarm clock app. Some alarm clock apps may not implement this feature.	281	(I)
Default	permission to install a location provider	Create mock location sources for testing. Malicious apps may use this to override the location and/or status returned by real location sources such as GPS or Network providers or monitor and report your location to an external source.	275	(I)
Your personal information	read user-defined dictionary	Allows the app to read any private words, names and phrases that the user may have stored in the user dictionary.	268	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Development tools	enable app debugging	Allows the app to turn on debugging for another app. Malicious apps may use this to kill other apps.	257	(I)
Default	read your profile data	Allows the app to read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and send your profile information to others.	254	(S)
Your personal information	write to user-defined dictionary	Allows the app to write new words into the user dictionary.	254	(I)
Your accounts	use accounts on the device	Allows the app to request authentication tokens.	253	(I)
Default	display unauthorized windows	Allows the app to create windows that are intended to be used by the internal system user interface. Not for use by normal apps.	244	(I)
Your accounts	add or remove accounts	Allows the app to perform operations like adding and removing accounts, and deleting their password.	237	(S)
Your messages	read Gmail	Allows the app to read your Gmail.	236	(S)
System tools	adjust your wallpaper size	Allows the app to set the system wallpaper size hints.	235	(I)
System tools	force stop other apps	Allows the app to forcibly stop other apps.	210	(I)
Default	Access download manager.	Allows the app to access the BluetoothShare manager and use it to transfer files.	204	(I)
System tools	access Bluetooth settings	Allows the app to configure the local Bluetooth tablet, and to discover and pair with remote devices. Allows the app to configure the local Bluetooth phone, and to discover and pair with remote devices.	199	(I)
System tools	format external storage	Allows the app to format removable storage.	188	(I)
Storage	modify/delete internal media storage contents	Allows the app to modify the contents of the internal media storage.	177	(S)
Default	read battery statistics	Allows an application to read the current low-level battery use data. May allow the application to find out detailed information about which apps you use.	167	(I)
Your accounts	read Google service configuration	Allows this app to read Google service configuration data.	165	(I)
Your personal information	retrieve system internal state	Allows the app to retrieve internal state of the system. Malicious apps may retrieve a wide variety of private and secure information that they should never normally need.	153	(S)
System tools	set time zone	Allows the app to change the tablet's time zone. Allows the app to change the phone's time zone.	146	(I)
Default	record what you type and actions you take	Allows the app to watch the keys you press even when interacting with another app (such as typing a password). Should never be needed for normal apps.	136	(S)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Default	bind to an input method	Allows the holder to bind to the top-level interface of an input method. Should never be needed for normal apps.	125	(I)
Default	monitor and control all app launching	Allows the app to monitor and control how the system launches activities. Malicious apps may completely compromise the system. This permission is only needed for development, never for normal use.	115	(I)
Default	modify the Google services map	Allows the app to modify the Google services map. Not for use by normal apps.	110	(I)
Default	set time	Allows the app to change the tablet's clock time. Allows the app to change the phone's clock time.	108	(I)
Default	interact with a device admin	Allows the holder to send intents to a device administrator. Should never be needed for normal apps.	104	(I)
Development tools	make all background apps close	Allows the app to control whether activities are always finished as soon as they go to the background. Never needed for normal apps.	101	(I)
System tools	send package removed broadcast	Allows the app to broadcast a notification that an app package has been removed. Malicious apps may use this to kill any other running app.	101	(I)
Default	force app to close	Allows the app to force any activity that is in the foreground to close and go back. Should never be needed for normal apps.	95	(I)
System tools	read subscribed feeds	Allows the app to get details about the currently synced feeds.	93	(I)
Development tools	send Linux signals to apps	Allows the app to request that the supplied signal be sent to all persistent processes.	91	(I)
System tools	read/write to resources owned by diag	Allows the app to read and write to any resource owned by the diag group; for example, files in /dev. This could potentially affect system stability and security. This should be ONLY be used for hardware-specific diagnostics by the manufacturer or operator.	89	(I)
Default	View WiMAX state	Allows the app to view the information about the state of WiMAX.	87	(I)
Default	reset system to factory defaults	Allows the app to completely reset the system to its factory settings, erasing all data, configuration, and installed apps.	82	(I)
Your messages	send WAP-PUSH-received broadcast	Allows the app to broadcast a notification that a WAP PUSH message has been received. Malicious apps may use this to forge MMS message receipt or to silently replace the content of any webpage with malicious variants.	78	(I)
System tools	write subscribed feeds	Allows the app to modify your currently synced feeds. Malicious apps may change your synced feeds.	77	(I)
Network communication	Broadcast data messages to apps.	Can broadcast data messages received from the Internet to apps registered to listen for them.	76	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Default	Change WiMAX state	Allows the app to connect to and disconnect from WiMAX network.	71	(I)
Your accounts	create accounts and set passwords	Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.	69	(S)
Default	write to your profile data	Allows the app to change or add to personal profile information stored on your device, such as your name and contact information. This means other apps can identify you and send your profile information to others.	69	(I)
System tools	toggle sync on and off	Allows an app to modify the sync settings for an account. For example, this can be used to enable sync of the People app with an account.	68	(I)
Network communication	download files without notification	Allows the app to download files through the download manager without any notification being shown to the user.	65	(I)
System tools	modify global animation speed	Allows the app to change the global animation speed (faster or slower animations) at any time.	64	(I)
Default	Install DRM content.	Allows app to install DRM-protected content.	56	(I)
Development tools	limit number of running processes	Allows the app to control the maximum number of processes that will run. Never needed for normal apps.	53	(I)
Default	control system backup and restore	Allows the app to control the system's backup and restore mechanism. Not for use by normal apps.	51	(I)
Your accounts	YouTube	Allows apps to sign in to YouTube using the account(s) stored on this Android device.	45	(S)
Default	read your social stream	Allows the app to access and sync social updates from you and your friends. Malicious apps may use this to read private communications between you and your friends on social networks.	43	(S)
Default	manage app tokens	Allows the app to create and manage their own tokens, bypassing their normal Z-ordering. Should never be needed for normal apps.	43	(I)
Your accounts	Google mail	Allows apps to sign in to Google mail services using the account(s) stored on this Android device.	42	(S)
Your messages	modify Gmail	Allows the app to modify your Gmail, including sending and deleting mail.	42	(S)
Default	bind to a widget service	Allows the holder to bind to the top-level interface of a widget service. Should never be needed for normal apps.	40	(I)
Default	Send download notifications.	Allows the app to send notifications about completed downloads. Malicious apps can use this to confuse other apps that download files.	39	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Default	access mail information	Allows the app to access information about your mail.	36	(S)
Default	access the cache filesystem	Allows the app to read and write the cache filesystem.	35	(I)
Default	run in factory test mode	Run as a low-level manufacturer test, allowing complete access to the tablet hardware. Only available when a tablet is running in manufacturer test mode. Run as a low-level manufacturer test, allowing complete access to the phone hardware. Only available when a phone is running in manufacturer test mode.	35	(I)
Default	Access all system downloads	Allows the app to view and modify all downloads initiated by any app on the system.	34	(I)
System tools	change background data usage setting	Allows the app to change the background data usage setting.	32	(I)
Default	partial shutdown	Puts the activity manager into a shutdown state. Does not perform a complete shutdown.	31	(I)
Default	write to your social stream	Allows the app to display social updates from your friends. Malicious apps may use this to pretend to be a friend and trick you into revealing passwords or other confidential information.	29	(I)
Default	read your own contact card	Allows the app to read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.	28	(S)
Your messages	read instant messages	Allows apps to read data from the Google Talk content provider.	27	(S)
Default	permanently disable tablet permanently disable phone	Allows the app to disable the entire tablet permanently. This is very dangerous. Allows the app to disable the entire phone permanently. This is very dangerous.	26	(I)
Default	update component usage statistics	Allows the app to modify collected component usage statistics. Not for use by normal apps.	25	(I)
Default	prevent app switches	Prevents the user from switching to another app.	24	(I)
Default	Access DRM content.	Allows app to access DRM-protected content.	20	(I)
System tools	erase USB storage erase SD Card	Allows the app to format removable storage.	20	(I)
Your accounts	Google Docs	Allows apps to sign in to Google Docs using the account(s) stored on this Android device.	18	(S)
Your accounts	Google Spreadsheets	Allows apps to sign in to Google Spreadsheets using the account(s) stored on this Android device.	17	(S)
Default	move app resources	Allows the app to move app resources from internal to external media and vice versa.	15	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Default	Advanced download manager functions.	Allows the app to access the download manager's advanced functions. Malicious apps can use this to disrupt downloads and access private information.	13	(S)
Your messages	Send Gmail	Allows the app to send Gmail messages without opening the Gmail app.	13	(I)
Your accounts	Google Maps	Allows apps to sign in to Google Maps using the account(s) stored on this Android device.	11	(S)
Default	bind to a text service	Allows the holder to bind to the top-level interface of a text service(e.g. SpellCheckerService). Should never be needed for normal apps.	11	(I)
Default	manage preferences and permissions for USB devices	Allows the app to manage preferences and permissions for USB devices.	11	(I)
Default	add voicemail	Allows the app to add messages to your voicemail inbox.	10	(I)
Default	bind to a VPN service	Allows the holder to bind to the top-level interface of a Vpn service. Should never be needed for normal apps.	9	(I)
Default	change pointer speed	Allows the app to change the mouse or trackpad pointer speed at any time. Should never be needed for normal apps.	9	(I)
Your personal information	add words to user-defined dictionary	Allows the app to write new words into the user dictionary.	9	(I)
Your accounts	contacts data in Google accounts	Allows apps to access the contacts and profile information of account(s) stored on this Android device.	8	(S)
Your accounts	Google App Engine	Allows apps to sign in to Google App Engine using the account(s) stored on this Android device.	7	(S)
Your accounts	YouTube usernames	Allows apps to see the YouTube username(s) associated with the Google account(s) stored on this Android device.	5	(S)
Default	manage network policy	Allows the app to manage network policies and define app-specific rules.	5	(I)
Default	Recorded audio access	Can access the recorded audio utterances for notes to self, and for raw audio analysis.	4	(S)
Default	connect and disconnect from WiMAX	Allows the app to determine whether WiMAX is enabled and information about any WiMAX networks that are connected.	4	(I)
Default	Read Google settings	Allows this app to read Google settings.	4	(I)
Default	status bar	Allows the app to be the status bar.	4	(I)
Your messages	write instant messages	Allows apps to write data to the Google Talk content provider.	4	(I)
Your accounts	access all Google services	Allows apps to sign in to ALL Google services using the account(s) stored on this Android device.	3	(S)
Your accounts	Google Finance	Allows apps to sign in to Google Finance using the account(s) stored on this Android device.	3	(S)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	Label	Description	Frequency	Type
Your accounts	Picasa Web Albums	Allows apps to sign in to Picasa Web Albums using the account(s) stored on this Android device.	3	(S)
Default	bind to an accessibility service	Allows the holder to bind to the top-level interface of an accessibility service. Should never be needed for normal apps.	3	(I)
Default	directly start CDMA tablet setup directly start CDMA phone setup	Allows the app to start CDMA provisioning. Malicious apps may unnecessarily start CDMA provisioning.	3	(I)
Default	use any media decoder for playback	Allows the app to use any installed media decoder to decode for playback.	3	(I)
Default	access to passwords for Google accounts	Allows apps direct access to the passwords for the Google account(s) you have set up.	2	(S)
Default	full license to interact across users	Allows all possible interactions across users.	2	(I)
Default	Modify Google service configuration	Allows this app to modify Google service configuration data.	2	(I)
Default	Modify Google settings	Allows this app to modify Google settings.	2	(I)
Your accounts	Blogger	Allows apps to sign in to Blogger using the account(s) stored on this Android device.	1	(S)
Your accounts	Google Calendar	Allows apps to sign in to Google Calendar using the account(s) stored on this Android device.	1	(S)
Your accounts	Google Voice	Allows apps to sign in to Google Voice using the account(s) stored on this Android device.	1	(S)
Your messages	Exchanges messages and receives sync notifications from Google servers.	Used for server cloud to device messages and for sync notifications. Google Talk uses this service to exchange messages and to synchronize presence status. Malicious apps could use this service to transmit excess data.	1	(S)
Default	interact across users	Allows the app to perform actions across different users on the device. Malicious apps may use this to violate the protection between users.	1	(I)
Default	modify your own contact card	Allows the app to change or add to personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.	1	(I)
Default	select Gmail or Google Mail branding	Allows apps to switch the displayed name between "Gmail" and "Google Mail" branding.	1	(I)
Default	Send broadcasts to Google Play.	Can send broadcasts to Google Play requesting app installation and removal.	1	(I)
Default	Voice Search shortcuts	Can access the shortcuts created for voice searches.	1	(I)
Development tools	force background apps to close	Allows the app to control whether activities are always finished as soon as they go to the background. Never needed for normal apps.	1	(I)

Continued on next page

Table 9: Permissions' Information showing category, label, description, frequency and type. Permission's type is shown as sensitive (S), network (N) and functionality-based (indifferent) permissions (I).

Category	**Label**	**Description**	**Frequency**	**Type**
Network communication	Send heartbeat to Google Talk server	Can send a heartbeat packet to the Google Talk server to ensure the health of the connection.	1	(I)

Appendix B Example of Social Manager's permission requests

Table 10 below shows the name and description of permissions requested by *Social Manager* app by SmallBell on the 28th March 2013.

Tab. 10: Social Manager's permissions list

Permission Name	**Permission Description**
This application has access to the following sensitive permissions:	
Add or Remove accounts	Allows the app to perform operations like adding and removing accounts, and deleting their password.
Create accounts and set passwords	Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.
Receive text messages (SMS)	Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.
Receive text messages (MMS)	Allows the app to receive and process MMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.
Read your text messages (SMS OR MMS)	Allows the app to read SMS messages stored on your tablet or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality. Allows the app to read SMS messages stored on your phone or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality.
Read your contacts	Allows the app to read data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.
Add or modify calendar events and send email to guests without owners' knowledge	Allows the app to add, remove, change events that you can modify on your tablet, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge. Allows the app to add, remove, change events that you can modify on your phone, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge.
Read calendar events plus confidential information	Allows the app to read all calendar events stored on your tablet, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity. Allows the app to read all calendar events stored on your phone, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity.
Read phone status and identity	Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.
Reroute outgoing calls	Allows the app to process outgoing calls and change the number to be dialed. This permission allows the app to monitor, redirect, or prevent outgoing calls.
Find accounts on the device	Allows the app to get the list of accounts known by the tablet. This may include any accounts created by applications you have installed. Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed.
Read Call Log	Allows the app to read your tablet's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge. Allows the app to read your phone's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge.

Continued on next page

Table 10: Social Manager's permissions list – continued from previous page

Permission Name.	**Permission Description**
Modify your contacts	Allows the app to modify the data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data. Allows the app to modify the data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data.
This application has access to the following indifferent permissions:	
Prevent tablet from sleeping/Prevent phone from sleeping	Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.
Toggle sync on and off	Allows an app to modify the sync settings for an account. For example, this can be used to enable sync of the People app with an account.
Control vibration	Allows the app to control the vibrator.
Read sync settings	Allows the app to read the sync settings for an account. For example, this can determine whether the People app is synced with an account.
Run at startup	Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.
Write call log	Allows the app to modify your tablet's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log. Allows the app to modify your phone's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log.
This application has no Internet permission.	